Table of Contents

Research on the System Structure of IPV9 Based on TCP/IP/M

Wang Jianguo
[1.] State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control
Xi'an, China
[2.] School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: wjg_xit@126.com

Xie Jianping
[1.] Chinese Decimal Network Working Group
Shanghai, China
[2.] Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13386036170@189.cn

Wang Zhongsheng
[1.] School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
[2.] State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control
Xi'an, China
e-mail: wzhsh1681@163.com

Zhong Wei
[1.] Chinese Decimal Network Working Group
Shanghai, China
[2.] Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13331860961@189.cn

***Abstract*—Network system structure is the basis of network communication. The design of network model can change the network structure from the root, solve the deficiency of the original network system, and meet the new demand of the future network. TCP/IP as the core network technology is successful, it has shortcomings but is a reasonable existence, will continue to play a role. Considering the compatibility with the original network, the new network model needs to be compatible with the existing TCP/IP four-layer model, at the same time; it can provide a better technical system to implement the future network. Based on the Internet three-layer/four-layer hybrid architecture TCP/IP/M and ISO/IEC next-generation Internet standard solutions, this paper proposes the IPV9 system architecture, which can directly transmit audio and video data with three layers on the premise of not affecting the existing four-layer network transmission. The hybrid structure is a new transmission theory, which requires the establishment of a link before data transmission and the withdrawal of the link after the transmission is completed. It solves the problem of high-quality real-time media communication caused by the integration of three networks (communication network, broadcasting network and Internet) from the underlying structure of the network, realizes the long-distance and large-traffic data transmission of the future network, and lays a solid foundation for the digital currency and virtual currency of the Internet. The system framework is verified by practical application. It have been deployed to verify the compatibility and reliable transmission between IPV9 network and the existing network, under the independent, reliable, secure and controllable network architecture, a new generation of master root server and 13 root domain name servers.**

DOI: 10.21307/ijanmc-2019-054

Keywords-TCP/IP/M; Next Generation Internet; IPV9; Big Data Stream

I. NEW GENERATION NETWORK SYSTEM IPV9

IPv9 protocol as one of the future network concepts, IETF proposed some basic dreams of IPv9 in 1994, and looked forward to the idea of network in the 21st century. Such as: 1024-bit length address, direct routing and the 42 layer routing addressing method. However, due to the lack of research results of basic theories, address stratification technology, high research and development costs, intellectual property rights and other factors, the research publicly failed. In 1997, the IPv9 working group was disbanded and intellectual property and patent results were not obtained.

Inspired by IPv9, Chinese scholars have established a new generation of network work expert teams. Based on the patent "Method of Using Whole Digital Code to Assign Addresses for Computer", they have completed the development of a new generation of network system after more than 20 years of research and development. The development of the system, its theory and practice has reflected the novelty and originality. The decimal network has experienced the stages of assumption, theory, model, prototype, small-scale trial and demonstration project implementation. Since September 2001, the Ministry of Information Industry of China has decided to establish "Decimal Network Standard Working Group (also known as IPV9 Working Group)", "New-generation Security and Controllable Network Expert Working Group", and "Electronic Label Working Group Data", united domestic and foreign enterprises, research institutions and universities to develop the IPV9 protocol with independent intellectual property of the digital domain name and other technical standards. By June 2016, the Ministry of Industry and Information Technology announced the approval of the four standards of the IPV9 system. Through unremitting efforts in various aspects, the IPV9 system mother root server, the main root server, and 13 root name servers named after N-Z letter have been developed.

II. THE DESIGN OF IPV9 ARCHITECTURE

The conventional packet switching of TCP/IP protocol does not support real time application and circuit switching application, that is, the transmission of sound or image by circuit in the four-layer protocol. TCP/IP is a connectionless unreliable packet protocol with a maximum packet size of 1514 bytes. The main idea of IPV9 design is to combine the IP protocol of TCP/IP with circuit switching, and make use of routers compatible with both protocols and a series of protocols, so that the addresses of IPv4, IPv6 and IPV9 can be used simultaneously on the Internet.

A. The hierarchy of IPV9

IPV9 system adopts the mixed network architecture of three-layer circuit/four-layer grouping, adopts the rules of verify first and then communication, address encryption, the address length could alter from 16-bie to 2048-bit, resource reservation, and adopts character direct route transmission mode, which apply virtual and real circuit to ensure the transmission security. The architecture diagram is shown in Figure 1.

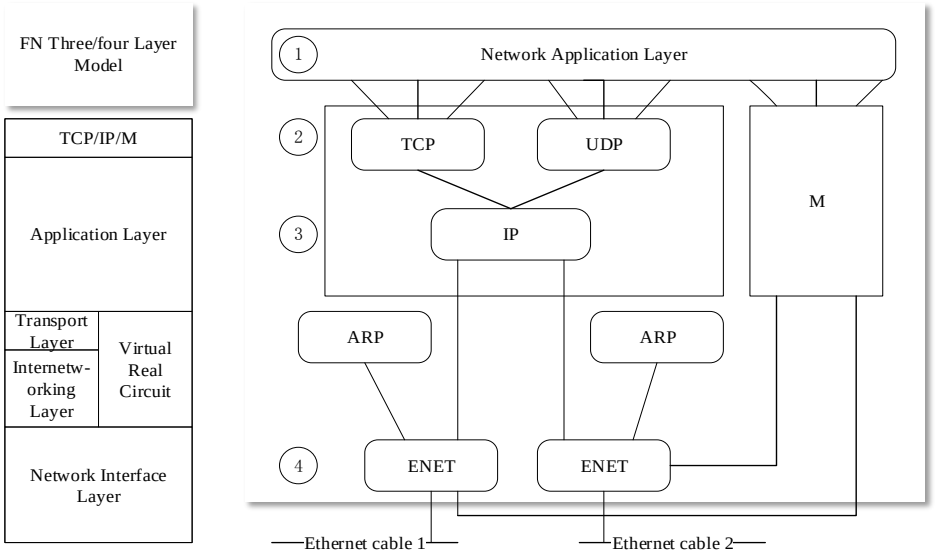


Figure 1. The Architecture Diagram

B. IPV9 connection method

TCP/IP/M protocol has developed absolute code stream and long stream code classes, a long packet can reach more than tens of megabytes. It can transmit telephone and cable TV data directly in three layers without affecting existing four-layer networks.

A four/three-layer transport protocol with a new transmit theory that is not removed connect link until finished the transmission.

The connection mode is shown in Figure 2.

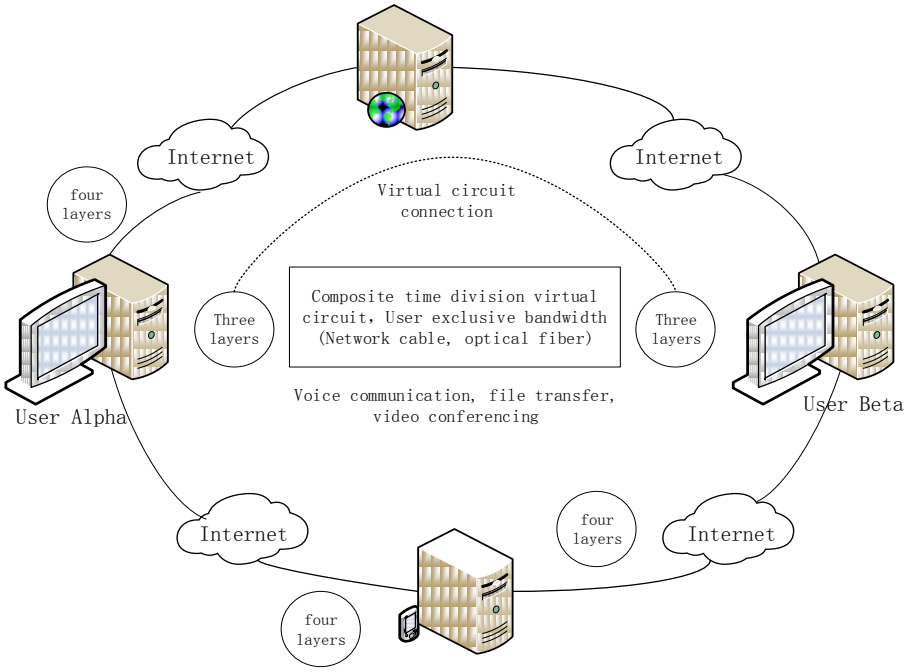


Figure 2. The connection mode

IPV9 automatic allocation access system, the system uses OpenVpn to set up virtual private network, uses IP TUNNEL for 9over4 data transmission, TR069 as the control protocol to push data to the terminal, to achieve the IPv4 subnet to subnet or IPV9 transmission. It can be a transmission between different individual routes or between the same enterprise routes, or between enterprise or individual routes to backbone routes. OpenVpn was adopted to penetrate the subnet to form the proprietary virtual network, and on the basis of the virtual network, IP TUNNEL was implemented to complete the data transmission of 9over4.In the virtual private network, the TR069 protocol is used to push the automatically assigned personal address or manually assigned business address, and at the same time, the 4to9 of the individual or business is automatically pushed to the device router.IPV9 network management system is a set of comprehensive network management system based on web interface that provides network monitoring and other functions. It can monitor various network parameters and server parameters to ensure the safe operation of server system. Both IPV4 and IPV9 protocols are supported and flexible notification mechanisms are provided for system administrators to quickly locate and resolve problems. IPV9 network and IPV9 /IPv4 hybrid network is constructed by using IPV9 design router, client, protocol conversion router and other devices. It includes IPV9 future network root domain name system, promoting technology integration, business integration and data integration, and realizing cross-level, cross-region, cross-system, cross-department and cross-business collaborative management and services. We will build an integrated national big data center and gateway bureau through data centralization and sharing, and build a secure and controllable information technology system.

C. Root domain name server

IPV9 root DNS server is mainly used to manage the Internet and decimal network home directory. IPV9 root name server system consists of a parent root server, primary root server, 13 root name servers named by N-Z, Top-level domain server named by • CHN, • USA, • HKG, • MAC and other three characters 239 countries and regions, routing management system, application server and 10 Gigabit backbone routers. The China Decimal Network Standards Working Group is responsible for management of the decimal network root name server, domain name system, and IP address.

The principle of root domain name server is that 13 root domain servers first read the primary root server, and then read the parent root server to obtain the data, and then spread to the whole network. The 13 root DNS servers are all equal. The system includes the parent root server and the primary root server. This hidden publishing host is accessed by only 13 root domain-name servers, which are read by mirror servers. The IPV9 root name server system is shown in Figure 3.

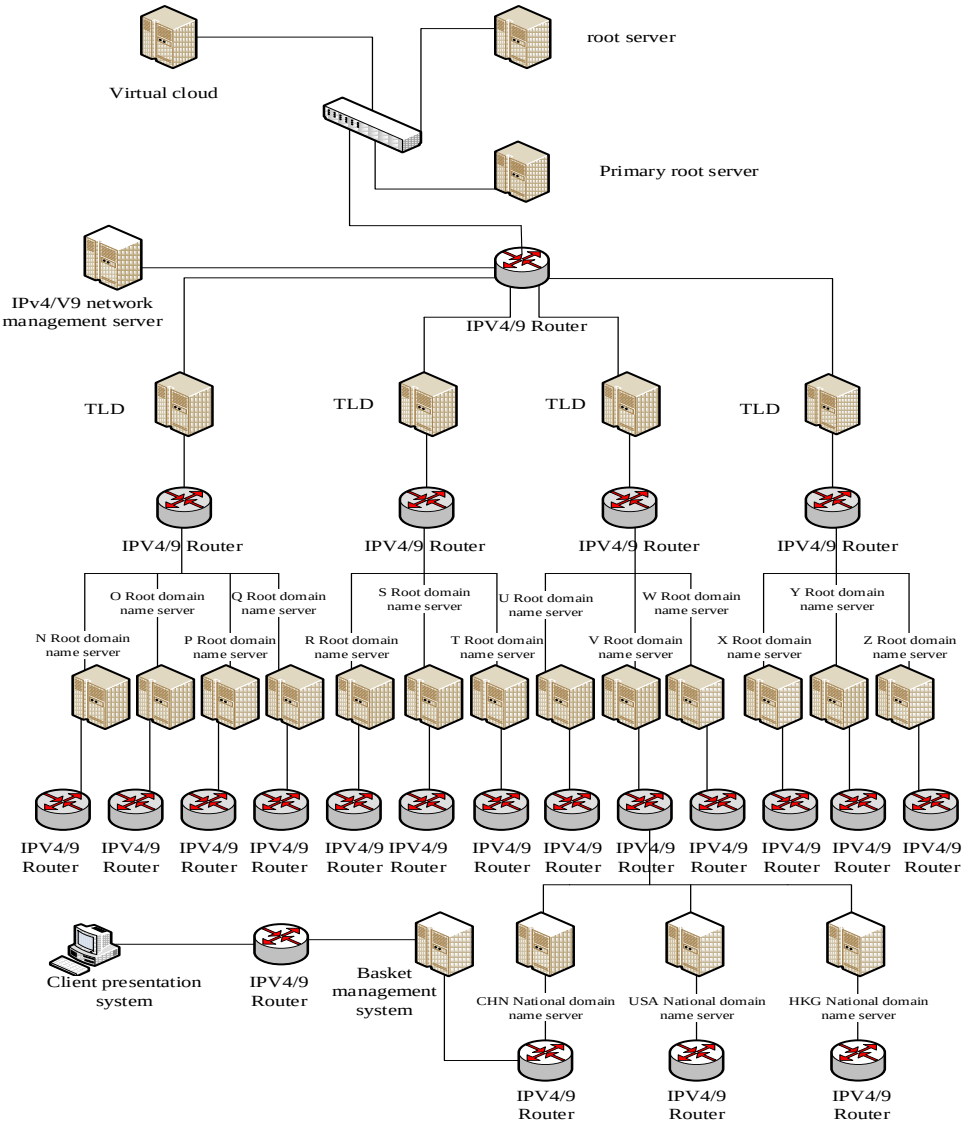


Figure 3. The IPV9 root name server system

The root name server is the highest level domain name server in DNS (Domain Name System) and is responsible for providing the authorized domain name server address for resolving the TLD (Top Level Domain). At present, the root DNS server and the gTLD (general top-level domain) and the ccTLD (country/region top-level domain) are managed and controlled by ICANN (Internet Corporation for Assigned Names and Numbers). The domain name system is the basic service of the Internet, and the root server is the foundation of the whole domain name system.

The IPV9-based root domain name resolution system can adapt to the IPv4 network, IPv6 network, IPV9 network. IPv9 resolution system can resolve the Internet user's domain name through the domain name server to obtain the corresponding access object IP address, and can send the request of non-digital domain name to the corresponding English domain name server or Chinese domain name server and domain name server in various languages, compatible with the current various domain name services.

III. THE TEXT REPRESENTATION OF IPV9 ADDRESS

The text representation of IPV9 address include "square brackets decimal" notation, "curly brackets decimal" notation, and " round brackets decimal" notation.

A. Square brackets decimal

The bracket decimal can be expressed in the following two ways:

1) 2048 bits are represented by "[]". The 2048 bits in the "[]" symbol are expressed in decimal notation and can be written in indefinite length.

2) IPV9 address representation with a length of 256 bits is in the form of " y[y[y[y[y[y[y[y", where each y represents a 32-bit part of the address and is expressed in decimal. 232 =4294967296, so y is a decimal number of ten digits. For example: 0003625410[0000030201]0000000000[0000000000]0000000000[00008701]0000000562.

In address representation, multiple consecutive zeros to the left of each decimal number can be omitted, but a decimal number that is completely zero needs to be represented by a zero. The contiguous all-0 field in the address is replaced by a pair of square brackets "[X]" (X is the number of segments in the all-0 field).The above address may be written as 3625410[30201[4] [508701[562.

B. Curly brackets decimal

This method divides the 256-bit address into four 64-bit decimal numbers represented by curly braces separating them. The representation method is in the form of "Z}Z}Z}Z", where each Z represents a 64-bit portion and is represented in decimal notation. It usage is exactly the same as Y, and it is compatible with Y. This greatly facilitates the current compatibility of these IPv4 addresses in IPV9.

C. Round brackets decimal

Since the address length of IPV9 defaults to 256 bits, there will still be many bits in each segment regardless of whether 4 or 8 segments are used. For example, each segment still has 32 bits with an 8-segment representation. In this way, the following situation will appear in the paragraph: ...] 00000000000000000000000000101101 0]...Such a situation is not only cumbersome to input, but also easy to make mistakes. For convenience, the parenthesis notation -- (K/L) is introduced, where "K" means 0 or 1 and "L" means the number of 0 or 1. The above example can be abbreviated as :...](0/25) of 1011010]....

D. A text representation of the address prefix

The IPV9 address scheme is similar to the supernetting and CIDR (Classless Inter-Domain Routing) schemes of IPv4, which all use the address prefix to represent the network hierarchy. The IPV9 address prefix is represented by a CIDR like representation in the form IPV9 address/address prefix length.

IPV9 addresses are written in IPV9 address notation, and the length of the address prefix is the length of the contiguous bits that form the address prefix from the leftmost part of the address. For example, the address prefix 1502[0] [0[0]390820[4027] for 210 bits can be expressed as: 1502[0] [0] [0]390820[4027] [0] [0] [0]390820[0] [0] [0]/210, short for: 1502[3]390820[4027]/210.

The ping implementation of the decimal network IPV9 address is shown in Figure 4.

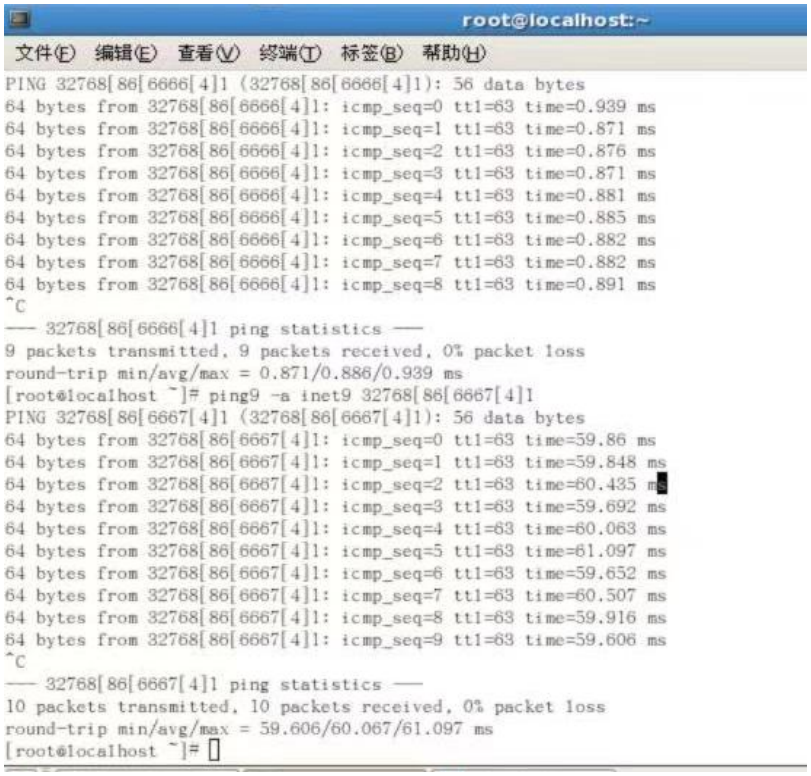


Figure 4. The ping implementation of the decimal network IPV9 address

IV. IMPLEMENTATION OF IPV9 SYSTEM

The IPV9 protocol implements the assumption that the address length is extended by the current 32-bit 1024-bit address and direct routing, and the original router class address addressing method is extended to the 42-layer route addressing method. According to the deficiency of the real network and the actual demand of future network, the new address, domain name system and routing addressing theory are studied to solve the problem of network resources and engineering implementation technology.

In order to be compatible with the existing Internet, dual stack technology is adopted. Dual stack technology refers to enabling both IPv4 stack and IPV9 stack on a single device. In this way, the device can communicate with both the IPv4 and IPV9 networks. If the device is a router, the interfaces of router are configured with IPv4 addresses and IPV9 addresses, and can connect to the IPv4 and IPV9 networks. If the device is a computer, it would have both an IPv4 address and an IPV9 address, and the ability to handle both. The IPV9 dual protocol stack is shown in Figure 5.

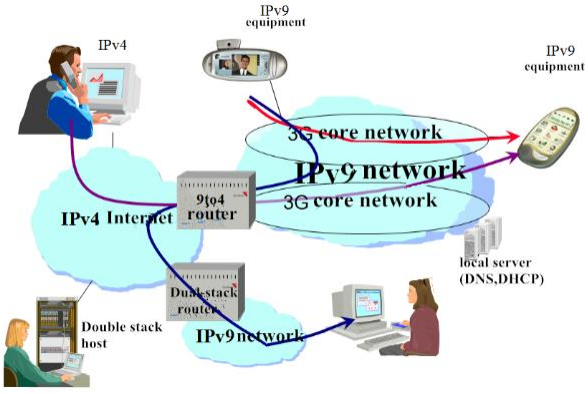


Figure 5. The IPV9 dual protocol stack

A. *Hardware component*

IPV9 system hardware devices are composed as follows:

1) Core router

Core routers, also known as "backbone routers", are routers located in the center of the network. Routers located on the edge of the network are called access routers. Core routers and edge routers are relative concepts. They all belong to the router, but they come in different sizes and capacities. The core router of one layer is the edge router of the other layer. It is used for IPv9 core network environment to realize large capacity data exchange.

2) Edge router

Edge routers, also known as "access routers", are routers located on the periphery of a network. Edge routers and core routers both belong to routers, but they have different sizes and capacities. The core router of one layer is the edge router of another layer.

3) IPV9-IPv4 protocol conversion router

IPV9-IPv4 protocol conversion router is used for mutual conversion between IPV9 and IPv4 protocols. IPv4 protocol data is converted to IPV9 protocol data by using preset mapping rules through 4to9 network interface devices.IPV9 protocol data is converted to IPv4 protocol data using preset mapping rules through the 9to4 network interface device.

4) Embedded router

Embedded router is low-cost user side access router. It can be easily deployed in the case of access to IPV9 network and the Internet.

5) Client

System support Centos5.5 32bit, Centos7 64bit client, and support mainstream Linux release later. IPv9 virtual machine that supports VMware allows customers to quickly deploy with existing hardware devices. Windows7, 9, 10 based on Windows IPv9 protocol stack client.

6) Beidou /GPS timing server

System Support Beidou, GPS satellite signal, and provide IPv4, IPV9 protocol NTP Server. User devices can be timed over IPv4 or IPV9 protocols.

B. Software system

1) IPv9 network management system

IPV9 network management system is a set of comprehensive network management system based on web interface that provides network monitoring and other functions. It can monitor various network parameters and server parameters to ensure the secure operation of server system. Both IPv4 and IPV9 protocols are supported and flexible notification mechanisms are provided for system administrators to quickly locate and resolve problems.

2) IPv9 automatic allocation access system

The system set up a virtual private network with OpenVpn, IP TUNNEL for 9over4 data transmission, and TR069 as the control protocol to push data to the terminal, and finally the IPv4 subnet to subnet or IPv9 transmission was realized. IPv4 subnet to subnet or IPv9 transmission can be implemented in different personal routing, the same enterprise routing, or between enterprise and personal routers to backbone routes.

OpenVpn is adopted to penetrate the subnet to form the proprietary virtual network; IP TUNNEL is implemented to complete the data transmission of 9over4 on the basis of the virtual network. In the virtual private network, the TR069 protocol is used to push the automatically assigned personal address and manually assigned enterprise address, and at the same time, the 4to9 of the individual or enterprise is automatically pushed to the device router.

3) IPv9 Windows protocol stack

Based on the original IPv4 and IPv6 protocols of the Windows operating system, the IPV9 protocol is added to realize the dual stack working access.

V. APPLICATION OF IPV9 SYSTEM

We designed the following scenarios to more fully reflect the features and advantages of the IPV9 network system.

A. Application 1—Pure IPV9 Network Architecture

This application implements a pure IPV9 network architecture. The simplest system includes IPV9 client/server A, IPV9 client/server B, 10G IPV9 routers C, D. The network topology is shown in Figure 6.

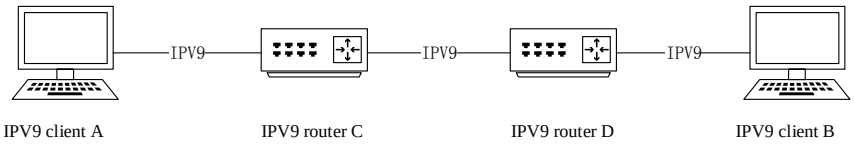


Figure 6. Pure IPV9 client-server test topology

The pure IPV9 network architecture is suitable for building a pure IPV9 network in one area and establishing an independent IPV9 network system.

B. Application 2—IPv4 network applications are connected via pure IPV9 network.

This application implements IPv4 network application to communicate through pure IPV9 network. The simplest system includes IPv4 client/server A, IPv4 client/server B, IPV9 10G routers C and D. The network topology is shown in figure 7.

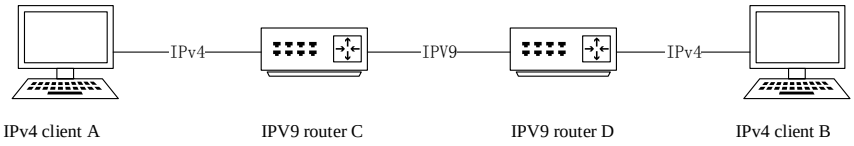


Figure 7. IPv4 network application test topology through pure IPV9 network connection

This scenario is suitable for several IPv4 networks in different regions connected through the IPV9 core network to achieve penetration access between different IPv4 networks. A main feature is that other areas are using the IPV9 protocol transmission in addition to the existing IPv4 network, which requires the different IPv4 network between the need for a private network connection (such as optical fiber, DDN line, etc.).

C. Application 3—IPv4 network is connected through 9over4 tunnel

This application implements IPv4 network application communication through 9over4 tunnel. The simplest system includes IPv4 client/server A, IPv4 client/server B, IPV9 10G router C, D. The biggest difference between scenario 3 and scenario 2 is that the IPv4 public network address between routers C and D is based on 9over4 tunnel communication. This scenario simulates that IPV9 uses the existing IPv4 public network to achieve IPV9 network connectivity in different geographic regions, and has the ability to build a national network. The network topology is shown in Figure 8.

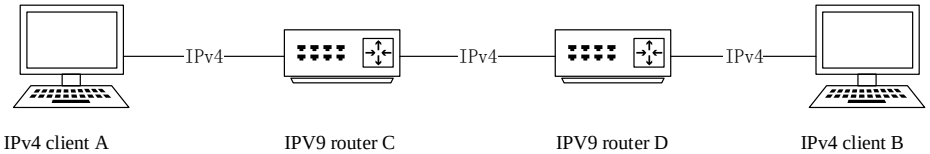


Figure 8. IPv4 network test topology through 9over4 tunnel connection

IPv4 networks in different areas are connected through the IPV9 over IPv4 core network to achieve transparent access between different IPv9 networks. A major feature is that system uses existing IPv4 networks between core networks, communicates via 9over4 tunnel mode. It uses the existing IPv4 public network to quickly establish connections between different regional IPv4 networks and achieve penetration access.

D. Application 4—IPV9 network connected through 9over4 tunnel

This application implements IPV9 network application communication through 9over4 tunnel. The simplest system includes IPV9 client/server A, IPV9 client/server B, IPV9 10G router C, D. The network topology is shown in Figure 9.

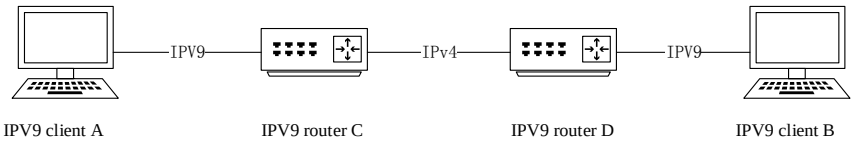


Figure 9. IPv9 network test topology through 9over4 tunnel connection

The application implements the IPV9 network to connect through the IPV9 over IPv4 core network to achieve transparent access between different IPV9 networks. A major feature is the use of existing IPv4 networks between core networks, communicating via 9over4 tunnel mode.

E. Application 5—Hybrid Network Architecture

In this application, the client side of the IPV9 access router accesses the IPv4 network and the IPV9 network. The network side of multiple IPV9 access routers accesses the user side of the same core router, and the network side of the core router accesses the IPV9 network and IPv4 network (including public network). The application can achieve the following functions: (1) IPv4 client penetrates private network to access the IPv4 client of other subnets; (2) IPv4 client accesses the Internet normally; (3) IPV9 client accesses the IPV9 client of other autonomous domains; (4) OSPFv9 dynamic router protocol is used between access routers to establish network; (5) IPV9 core routers can choose to use 9over4 network to access Shanghai node IPV9 network, or use pure IPV9 protocol to access Beijing node IPV9 network. The network topology is shown in Figure 10.

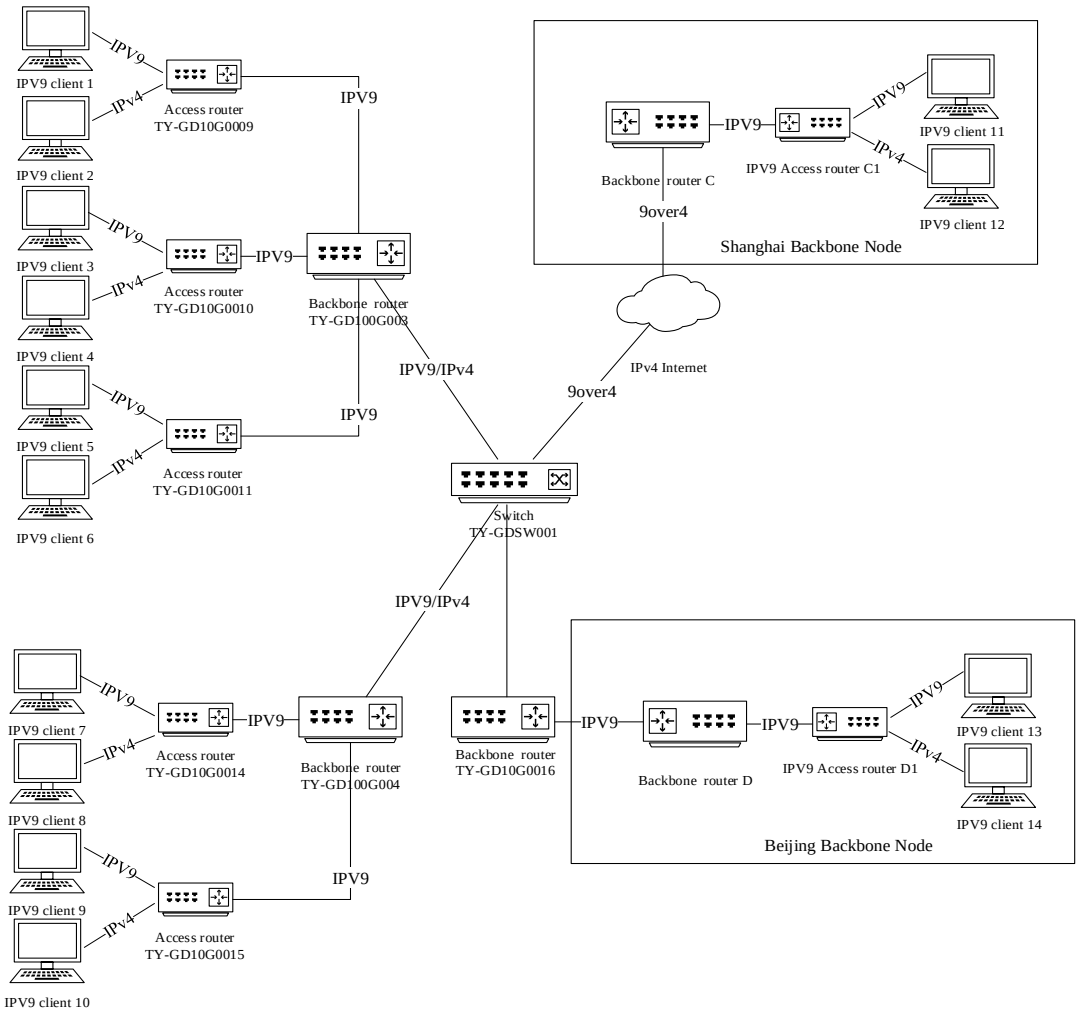


Figure 10. IPV9 hybrid network architecture test topology

This application scenario is mainly used to build an IPV9 network environment and seamlessly integrate IPv4 networks and IPV9 networks. All IPv4 and IPV9 network islands are connected using the IPV9 protocol or the existing IPv4 public network. It is convenient and fast to connect independent networks in different regions to form a national unified network by using the IPV9 network system.

F. Application 6--IPV9 Root Domain Name Agent System

IPV9 root domain name system provides the system expansion support capability compatible with the RFC1035 protocol under the support of a powerful database, and forms a symbiotic relationship with the existing IPv4 domain name system. At the same time, it provides an independent and controllable application guarantee for the IPV9 domain name.

The system network includes three parts: IPV9 domain name back-end support system, routing and network add service system, and application system. IPV9 domain name back-end support system can be deployed in a grid, deployed in Shanghai and Beijing to establish a root domain extension support environment that is both organic and relatively independent. The routing and network service system can choose IPv4, IPv6 networks or IPV9 network. The application system includes mobile terminal and

desktop platform support system. The network topology is shown in Figure 11.

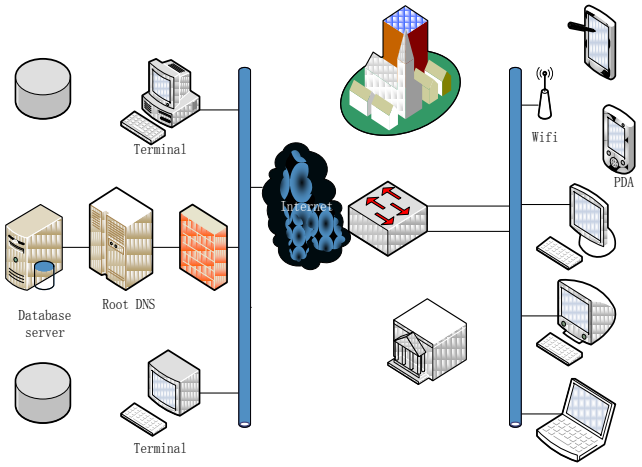


Figure 11. IPV9 root domain name proxy system topology

```
xtiger@ubuntu:~$ dig9 +trace -x 202.170.218.91 +noedns +nodnssec

; <<>> DiG 9.12.0b2 <<>> +trace -x 202.170.218.91 +noedns +nodnssec
;; global options: +cmd
.                       84400   IN      NS      n.root-servers.chn.
.                       84400   IN      NS      o.root-servers.chn.
.                       84400   IN      NS      p.root-servers.chn.
.                       84400   IN      NS      q.root-servers.chn.
.                       84400   IN      NS      r.root-servers.chn.
.                       84400   IN      NS      s.root-servers.chn.
.                       84400   IN      NS      t.root-servers.chn.
.                       84400   IN      NS      u.root-servers.chn.
.                       84400   IN      NS      v.root-servers.chn.
.                       84400   IN      NS      w.root-servers.chn.
.                       84400   IN      NS      x.root-servers.chn.
.                       84400   IN      NS      y.root-servers.chn.
.                       84400   IN      NS      z.root-servers.chn.
;; Received 506 bytes from 32768[86[21[4]3232239457#53(32768[86[21[4]3232239457)
 in 471 ms

202.in-addr.arpa.       86400   IN      NS      a.arpa-servers.chn.
;; Received 109 bytes from 32768[86[10[3[3]2#53(q.root-servers.chn) in 29 ms

91.218.170.202.in-addr.arpa. 120 IN     PTR     em777.chn.
218.170.202.in-addr.arpa. 86400 IN      NS      a.arpa-servers.chn.
218.170.202.in-addr.arpa. 86400 IN      NS      a.gtld-servers.chn.
218.170.202.in-addr.arpa. 86400 IN      NS      b.gtld-servers.chn.
;; Received 182 bytes from 172.16.3.2#53(a.arpa-servers.chn) in 187 ms

xtiger@ubuntu:~$
```

Figure 12. IPV9 root domain name proxy system analysis results

VI. SUMMARY

The main technical features and innovations of IPV9 system are as follows.

1) Independent address text format

Decimal network technology can be independent of the original IPv4 and IPv6 network networking. The IPV9 address text representation of decimal network uses the Arabic numerals of 0-9 and "[" as a separator, which is compatible with IPv4 and IPv6.

2) Infinite IP address space

The length of IPV9 address is 2256, can be up to 21024. It conforms to assumptions of ISO future networks 66N13376, 66N13488, 6N13947 and RFC1606, RFC1607. The address resources are very rich. End-to-end transmission can be achieved according to the requirements, which have high efficiency and economy. The IPV9 address uses a technique of two-sided compression and a number of brackets in the compression section, which is simple and convenient to use.

3) Safe and controllable

IPV9 USES a specific encryption mechanism for the address to achieve point-to-point transmission to enhance the privacy of users. In order to ensure the healthy and orderly development of information services, the means of verification before communication can be temporarily closed to businesses with incomplete or unqualified security measures.

IPV9 is independent of IPv4 and IPv6 Internet networking. It can effectively manage and control network security and information security. According to the actual needs, users can choose valuable information download, methods to avoid intrusion of bad information and unexpected attacks.

4) Unified coding

The domain name and the IP address synthesize, may cause the telephone, the handset, the domain name and the IP address, IPTV, the IP telephone and so on to combine into one number. This method saves the translation time between the domain name and the IP address, makes the network communication fast and convenient, and improves the communication capability of the existing network switching equipment.

At present, electronic labels and bar codes are used and managed separately. IPV9 has developed more superior and more viable RFID electronic tags, barcode unified data format and application standard

system. It can make the electronic label and barcode unified into a code, so that a commodity code has three ways of identification: one-dimensional barcode, two-dimensional code and electronic label, the three represents are global unique code, and also are the IP address of the IPV9 domain name. This feature enables barcodes and electronic tags have the same Internet access capabilities, which will greatly reduce the management costs of the global manufacturing and logistics industries.

ACKNOWLEDGMENT

This paper is sponsored by the Xi'an Decimal Network Technology Co., Ltd..

REFERENCE

[1] Xie Jianping etc. Method of using whole digital code to assign address for computer [P].US: 8082365, 2011.12.

[2] RFC - Internet Standard. Internet Protocol, DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791, 1981.09.

[3] S. Deering, R. Hinden, Network Working Group. Internet Protocol Version 6 (IPv6) Specification, RFC-1883, 1995.12.

[4] M. Crawford. Network Working Group. Transmission of IPv6 Packets over Ethernet Networks. RFC-2464, 1998.12.

[5] J. Onions, Network Working Group. A Historical Perspective on the usage of IP version 9. RFC1606. 1994.04.

[6] V. Cerf, Network Working Group. A VIEW FROM THE 21ST CENTURY, RFC1607. 1994.04.

[7] Xie Jianping, Xu Dongmei, etc.Digital domain name specification. SJ/T11271-2002, 2002.07.

[8] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.

[9] Wenfeng, Xie Jianping, etc. Product and service digital identification format for information procession. SJ/T11603-2016, 2016. 06.

[10] Radio frequency identification tag information query service network architecture technical specification. SJ/T11606-2016, 2016. 06.

Design and Research of Healthy Ecology System Framework Based on IPV9

Li Qinyu
Tai'an Finance Health Medical Information Technology Co., LTD
Shandong Radio, Television and Network Co., LTD. Tai'an Branch.
639 Leigushi Street, Tai'an 271000, Shandong Province
e-mail: 13720517562@163.com

Geng An
Shandong Radio, Television and Network Co., LTD. Tai 'an Branch.
639 Leigushi Street, Tai'an 271000, Shandong Province
e-mail: 398705156@qq.com

Zhao Hongwen
Shandong Radio, Television and Network Co., LTD. Tai 'an Branch.
639 Leigushi Street, Tai'an 271000, Shandong Province
e-mail: tagdglcs@qq.com

Han Lei
Shandong Radio, Television and Network Co., LTD. Tai 'an Branch.
639 Leigushi Street, Tai'an 271000, Shandong Province
e-mail: 2839437805@qq.com

***Abstract*—With the improvement of living standard and the change of life, people's health awareness has been enhanced as a whole, and the health demand has changed from single medical service to multiple services such as disease prevention, health promotion, healthcare and rehabilitation. The wisdom medical system, Internet + medical service mode and digital hospital have become the direction of medical development. In order to build Tai'an healthy big data ecological domain, accelerate the traditional medical process informatization reform, and improve the application level of information service, we build a medical system with the support of new generation network IPV9 technology. The system is based on the medical institutions in Tai'an city, Shandong province, and has researched and implementation of the health ecosystem business structure, core technology, network architecture, system software and hardware, and system security. The system was put into trial operation in the medical institutions of the whole city and has achieved perfect results.**

Keywords-IPV9; Internet +; Healthy Ecology; Health Platform

I. THE CURRENT STATUS OF HEALTH CARE

A. Medical health background

A new round of scientific and technological revolution and industrial changes are accelerating. Life science technologies continuously made new breakthroughs, and major technologies such as genetic engineering, molecular diagnostics, stem cell therapy, and 3D printing are accelerating applications. The new generation information biology and engineering technologies such as big data, cloud computing, Internet, artificial and intelligence are increasingly integrated into the medical and health fields. The rapid

DOI: 10.21307/ijanmc-2019-055

development of telemedicine, mobile medical care, precision medical care, smart medical care and other technologies have promoted the vigorous development of new formats and models of health industry, such as health management, health care, health tourism, leisure and health care, and “Internet + health”.

“13th Five-Year Plan for National Population Health Informatization Development” pointed out: We should strengthen population health informatization and health care big data service system construction, promote integration of government health care information system and public health medical data fusion, and eliminate information barriers, focus on improving the ability and level of population health information governance, vigorously promote the development of health care big data applications, and explore new models and new formats of innovative "Internet + health" services. We will build a unified, authoritative and interconnected platform for population health information, standardize and promote "Internet+ health care" services, and create new models of Internet health care services. Data collection, integration and sharing and business coordination of applied information systems such as public health, family planning, medical services, medical security, drug supply and comprehensive management are realized.

In recent years, the aging population in Shandong province is characterized by large base, rapid growth and empty nest. On the one hand, the needs of elder's life care and medical health care are superimposed, and the consumption demand in the field of medical care, health care are strong, with huge space for the development of related industries. On the other hand, the health care industry in Shandong province is still in its infancy, with relatively insufficient supply-side capacity, structural contradictions and policy barriers, lack of high-quality resources, narrow coverage of medical care, and insufficient professional personnel, making it difficult to meet the needs of the elderly for different levels of health care services.

B. Tai'an health care platform

In 2016, Tai'an City proposed in the of “Tai'an City transformation and upgrading of medical and health service industry implementation plan” to accelerate the construction of "smart medical" system, explore the "Internet + medical" service mode, and build a digital hospital. We will build a sound healthy Tai'an big data ecological domain, accelerate the informatization reform of traditional medical treatment process, and improve the application level of informatization services. The government encourages medical and health institutions to make full use of the advantages of Internet development.

The design and research of this system is based on the medical informatization of Tai'an City, Shandong Province, which is led by Tai’an Central Hospital of Tai'an City, Tai'an Central Hospital and Tai'an City Hospital of Traditional Chinese Medicine. The district and county people's hospitals are the main force, and the informatization development of the hospital is relatively perfect. However, some secondary hospitals, primary health care institutions, medical associations, medical communities, Internet hospitals, regional medical and health platforms and other information systems are not perfect, and they are unable to meet the growing needs of medical information development. Take the construction of medical and health information in Feicheng City as an example.

With the rapid development of IT technology, SOA technology, SaaS application, wireless network and other new technologies, the price of IT equipment is getting lower and lower, which makes the construction of smart city feasible technically and economically. Meanwhile, with the continuous application of cloud computing technology in the practice of medical informatization, the construction of regional medical informatization can achieve better results on this basis.

In August 2007, the Ministry of Information Industry Officially defined IPv9 as a new generation Internet to distinguish IPv6 next-generation Internet. The Internet based on TCP/IP protocol has been unable to meet the needs of future development by increasing bandwidth and gradual improvement. In order to break through the future network basic theory and support a new generation of Internet experiment. It is necessary to build test facilities include: original network equipment system, resource monitoring management system, covering cloud computing services, Internet of Things applications, spatial information network simulation, network information security.

On November 20, 2018, the General Staff Department of the People's Liberation Army organized the IPv9 Technology Project Application Seminar at the No. 9 Dacheng Road in Beijing. They discussed and demonstrated the application of the healthy Tai'an Big Data Ecological Domain as an IPv9 technology application. It is required to speed up construction of the Tai'an big data ecological domain and rapidly increase the scale of the IPv9 network, and strive to build an IPv9 network technology demonstration zone through healthy Tai'an big data ecological domain.

Tai'an City "smart medicine" was achieved through the establishment of a unified data standard for health information in Tai'an City, public health information resources sharing, and electronic two-way referral and inspection results in the city mutual recognition and health card application in the city. With the healthy Tai'an big data ecological domain as the core, it realizes information interconnection and sharing, as well as comprehensive business collaboration. It promotes the development of a large health industry, achieves a more scientific management, smarter business, and benefits more residents, and promotes the openness of the health and family planning business in Tai'an City. Through the construction of this platform, the informatization construction of health and family planning in Tai'an City has reached the national first-class level.

II. ECOLOGICAL DOMAIN SYSTEM

Tai'an big data ecological domain can provide personalized health management and health care for residents, improve residents' satisfaction. It can provide life-cycle health information for residents, and provide residents with network and information health services and health management. It enables residents to obtain continuous, comprehensive and high-quality health care services. It improves the efficiency of health services and reduces the waiting time of residents. We will support the rational use of high-quality regional health resources; effectively resolve the rational division of labor and allocation between primary and secondary large hospitals.

A. System business architecture

The health Tai'an big data ecosystem consists of five parts: business system layer, IT basic service layer, data layer (data warehouse), application layer and service layer (Internet + convenient service platform).

The business systems layer includes the business systems of medical institutions, health management centers, public health institutions, and other administrative agencies. Through the IPv9 service private network, network equipment, servers and storage equipment in the IT basic service layer, data such as electronic medical records, health files, population, and health resources are stored in the data layer. We divide the platform business system into three categories according to the different roles of data usage. The first category is the Internet + service platform for residents (including health Tai'an website, health Tai'an APP, Internet hospital, etc.). The second category is the medical collaborative service system for medical and health personnel (including hierarchical diagnosis and treatment platform, health identity card management system, telemedicine, health Tai'an imaging/ECG/inspection/pathology, etc.). The third

category is the medical and health supervision system which serving the medical and health administrative institutions (including the medical and health supervision platform, medical reform monitoring system, third-party regional evaluation system, etc.). Meanwhile, business intelligence in data warehouse can be used to support the development of big data analysis and artificial intelligence.

The entire platform architecture conforms to the international and national information standard management system and information security protection framework to ensure the consistency and security of the exchange of data. Meanwhile, the remote disaster recovery and backup mode in line with international requirements is specially used to ensure the safe storage of data from natural or man-made disasters.

Figure 1. Business architecture of health Tai'an big data ecological domain

B. Overall technical architecture

The health Tai'an big data ecological domain database uses relational databases such as MySQL, Oracle, SQL Server, and the development language uses JAVA and .net.

The platform service is built with ESB bus and SOA architecture, which provides perfect technical support for big data, and realizes rapid access to massive data. The flat platform provides complete functions such as collaborative support services and configuration management, and provides a comprehensive monitoring mechanism for the operating environment, which facilitates the rapid positioning and troubleshooting of problems. The overall technical framework of the platform conforms to the national standard and standard system, and adopts the data exchange standard of the industry standard, and adopts a variety of security mechanisms and security technologies to ensure the stable operation of the platform.

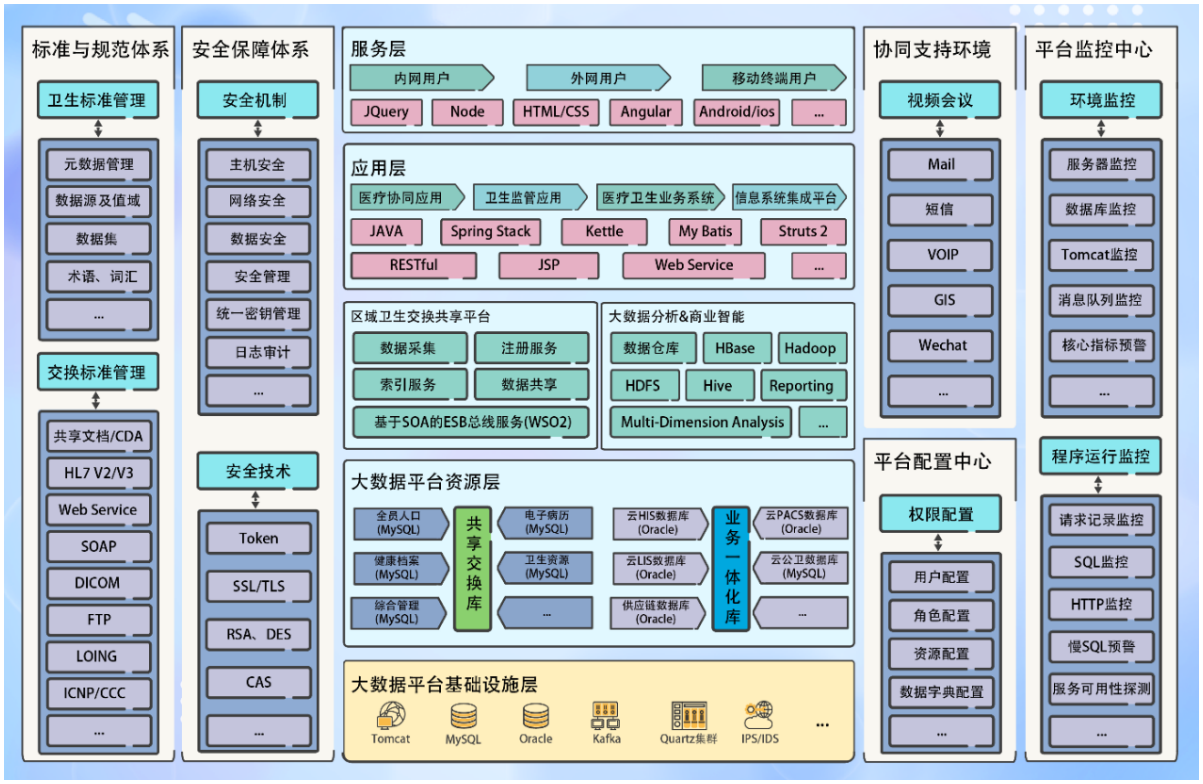


Figure 2. Technical architecture of health Tai'an big data ecological domain

1) SOA architecture support

The platform adopts the Micro services architectural mode. Micro services are an updated version of the traditional SOA architectural pattern that supports for fine-grained control. Each system accessed in healthy Tai'an big data ecological domain is equivalent to micro services component, which dynamically realizes service scheduling and balance through registration and discovery mechanism. In addition, each service component can deploy multiple instances, effectively improving the overall stability of the platform.

A service component is a mineralized project with distributed deployment and invocation that provides a type of interface services. In terms of interface granularity division of service components, appropriate granularity should be adopted to split the interfaces to ensure the flexibility of top-level application calls and reduce the number of calls between different components to avoid complex business logic dependencies between components.

2) ESB bus technology

ESB (Enterprise Service Bus) is the combination of traditional middleware technology and XML, Web Service technology. The ESB provides the most basic connectivity hub in a network and is an essential element in building an enterprise nervous system. The enterprise service bus is the latest way to provide reliable, guaranteed messaging technology.ESB middleware products leverage Web services standards and interfaces with recognized reliable messaging protocols. Common features of ESB products include: connecting heterogeneous MOM, encapsulating the MOM protocol using the Web services description language interface, and the ability to transport Simple Object Application Protocol (SOAP) transport streams on the MOM transport layer.

The ESB uses the "bus" model to manage and simplify the integration topology between applications, based on open standards to support dynamic interconnectivity between applications at the level of messages, events, and services.

The platform adopts B/S architecture and SaaS deployment mode, which is different from traditional medical information platform manufacturers and the overall architecture design, is more advanced and efficient.

C. Overall standard architecture of the platform

Following the unified standard, unified code, unified interface, under the principle of combing and standardized data through canonical business definition, strictly in accordance with established standards and technical route, so as to realize multiple departments, multiple system, information technology, as well as heterogeneous platform environment, interconnection, make sure that the maturity of the whole system, expansibility and adaptability, to evade the risk of system construction.

Under the principle of "unified specification, unified code, and unified interface", the system strictly abides by established standards and technical routes, thereby achieving information interconnection in multi-sector, multi-system, multi-technology, and heterogeneous platform environments.

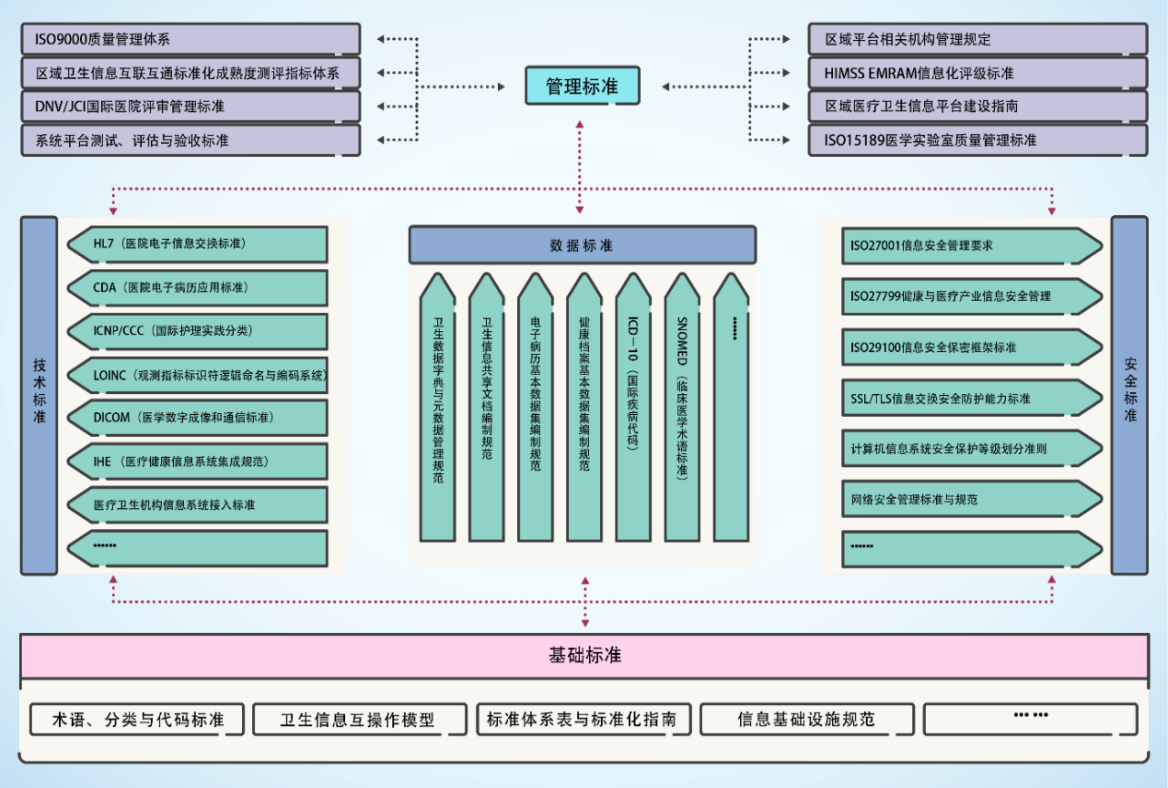


Figure 3. The standard architecture health Tai'an big data ecological domain

D. Platform security architecture

The platform security architecture refers to ISO-27001 and the third level of the national information security level protection system requirements. From the aspects of technology, operation and maintenance, management system and infrastructure, it is divided into security technology system, operation and maintenance security system, information security management system, security infrastructure and other parts.

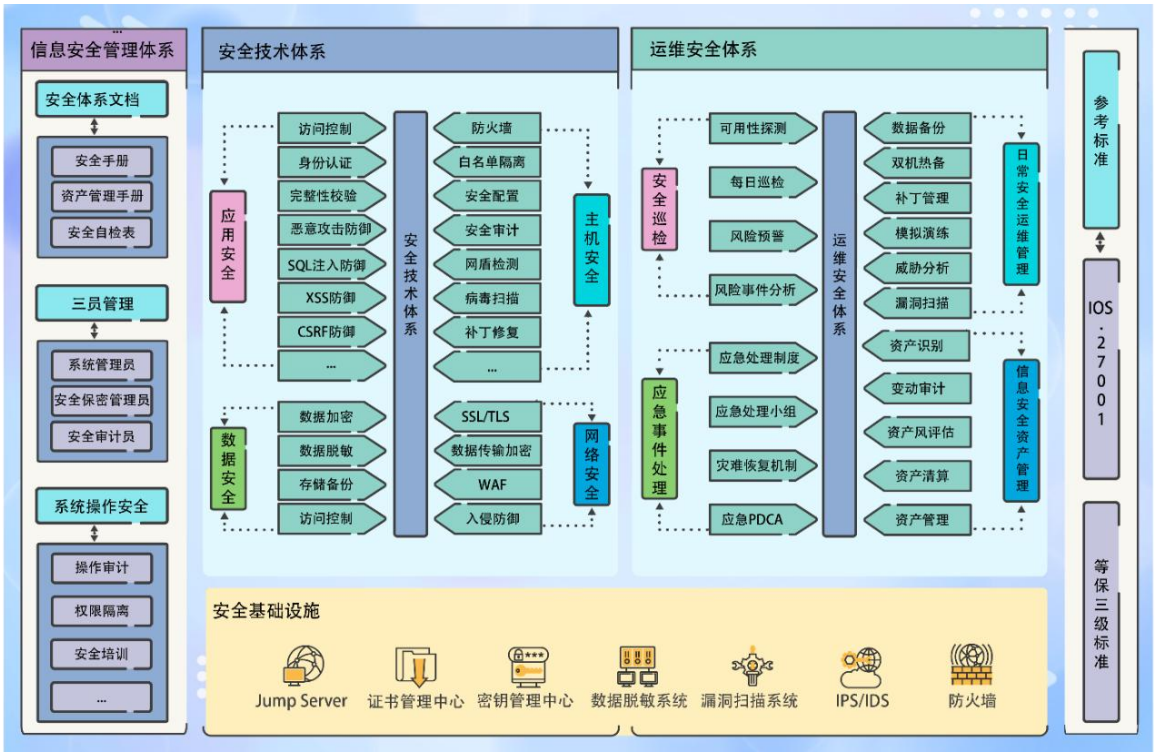


Figure 4. The security architecture health Tai'an big data ecological domain

The security technology system is mainly divided into application security, data security, network security and host security.

1) Application security. Application security mainly against common WEB security vulnerabilities published by OWASP. It mainly includes SQL injection, invalid authentication and authentication management, XSS attacks, invalid access control, sensitive information disclosure, CSRF, use of known vulnerability components, unprotected API, insufficient logging and monitoring and other WEB vulnerabilities.

2) Data security. Database security relies on various technologies and management measures to ensure data security, availability, integrity and confidentiality through data encryption, data desensitization, data storage backup, and access control.

3) Network security. Network security is mainly to ensure the integrity, confidentiality and non-repudiation of data in the process of network transmission. Through data transmission process encryption, intrusion prevention guarantees network security.

4) Host security. Host security solves the main security risks faced by the server, builds a server security protection system to prevent information leakage and risk by firewalls, white list isolation, security configuration, etc.

III. SYSTEM NETWORK ARCHITECTURE

The system is divided into six areas, and the core area is two Huawei S2710 data center level switch clusters. The core area is connected to all other areas using dual gigabit connections. The network topology is shown in figure 5.

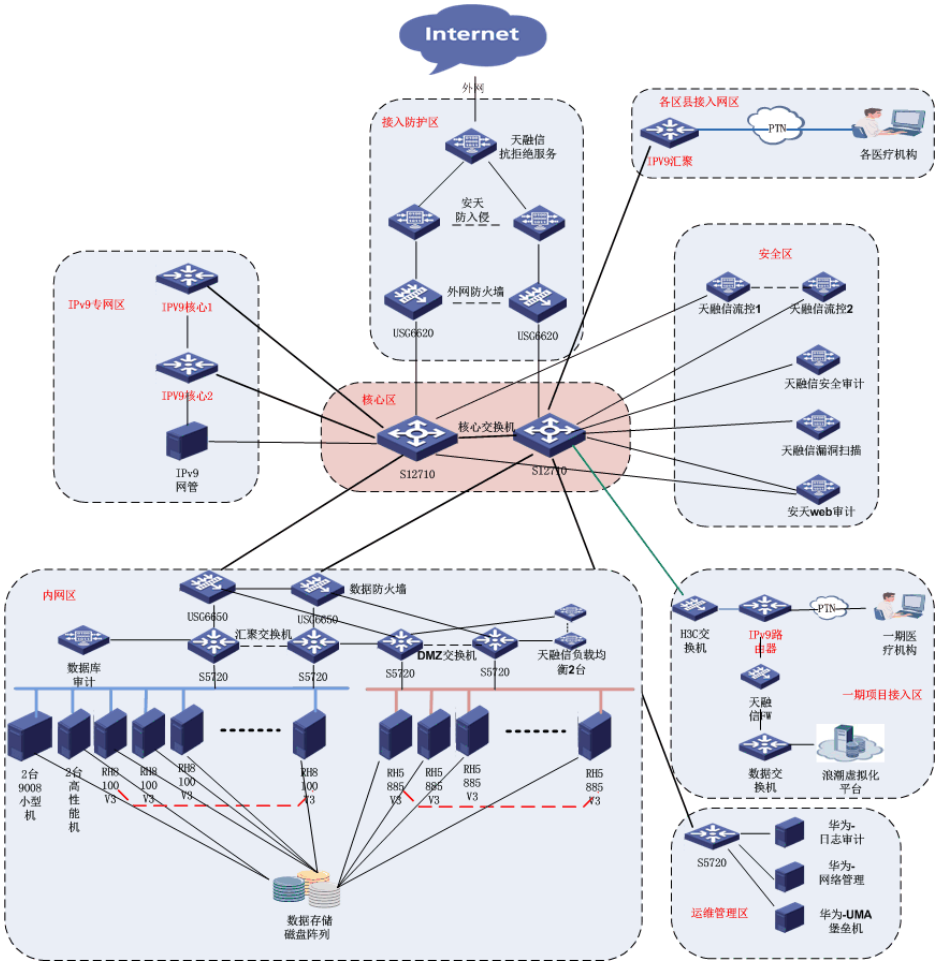


Figure 5. Topology architecture of healthy Tai'an big data ecological domain network

The access area is the area where all health cares institutions access. Two Huawei 10 Gigabit firewalls are used for isolation and aggregation. The business volume in the early stage is limited, and each of the two firewalls uses a 10 Gigabit connection, which can be expanded at any time with the business development in the future.

The internal network area is centered on two IPv9 backbone routers and Huawei 6650 data firewall. The data firewall isolates the internal network from the core switch 12710 to protect it. The establishment of virtual servers and storage devices in the internal network area is completed through optical fiber switches. The IPv9 router backbone router encrypts the address of the core data area of the internal network for higher security.

The external network deployment has the external network firewall. The anti-attack device is deployed to further increase the security protection of the external network. Platform logging, auditing, monitoring and IPv9 management are deployed in the management area. The security zone is used to deploy TOPSEC vulnerability scanning, network auditing, and flow

control devices, which mainly provide security auditing and vulnerability scanning andother protection functions for the network.

IV. DESIGN OF SYSTEM HARDWARE ARCHITECTURE

The system is equipped with Huawei key business server minicomputer, which is mainly used in HIS system. It gives full play to the characteristics of strong processing capacity and high reliability of the minicomputer to ensure the normal operation of the hospital's daily business for 24 hours. The system is equipped with Huawei high-performance data server, which serves as the city's population health records database to ensure the security of these important data.

The high-performance generic server runs the LIS system, supply chain system, PACS system, medical business collaboration, Internet applications, and other applications. The cloud mode dynamically adjusts the computing resources of the server according to the running status of the service. Each virtual machine can be used as a backup. If a hardware server fails, the service will not be affected.

The hardware architecture of the system is shown in figure 6.

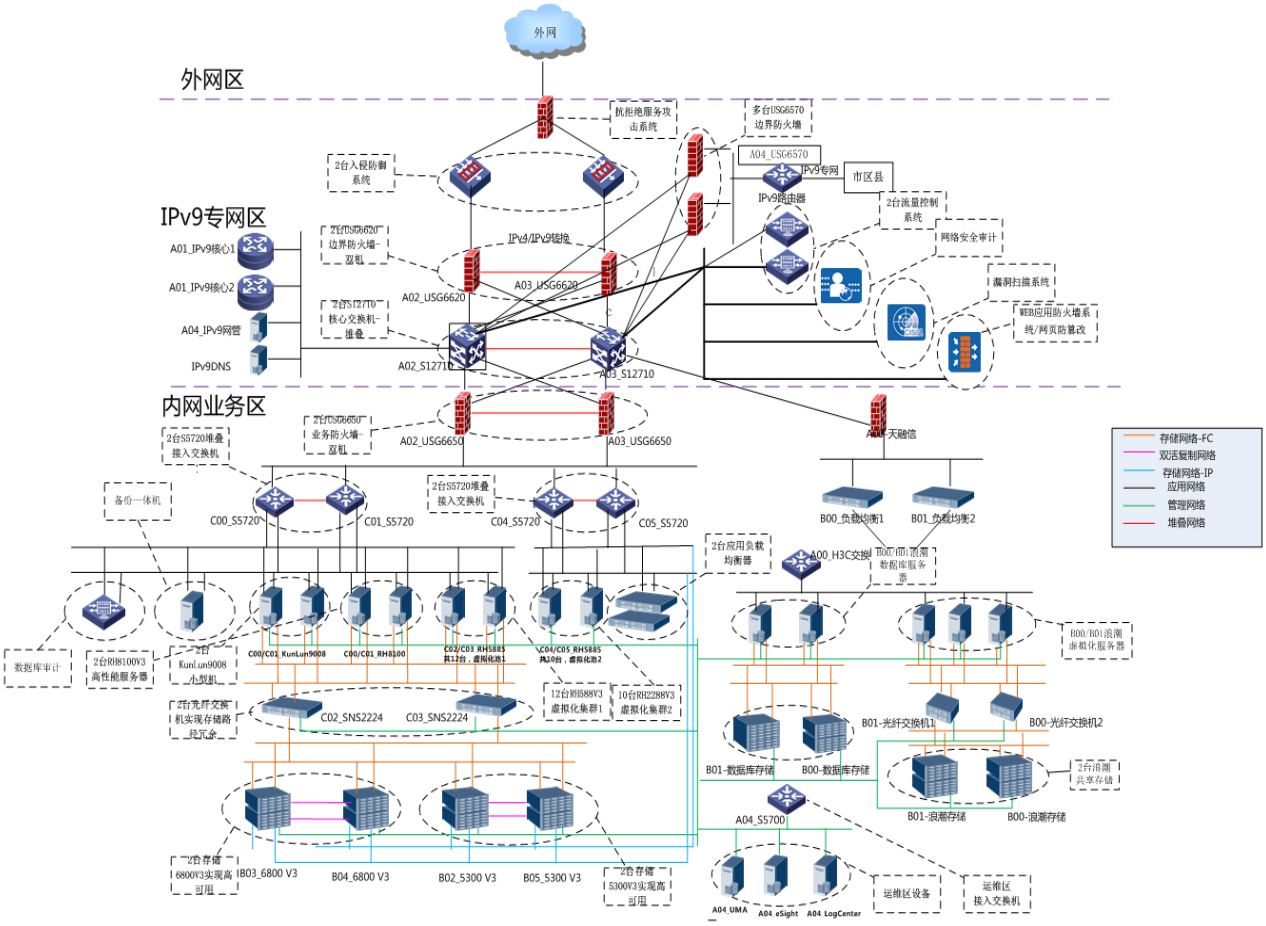


Figure 6. Topology diagram of health Tai'an big data ecological domain equipment.

According to the outpatient volume of all levels of hospitals within Tai'an region, the available storage capacity of healthy Tai'an big data ecological domain is 202.5T, which can meet the business needs in the next 3 to 5 years. The storage portion consists of Huawei OceanStor6800 V3 and Huawei

OceanStor5300 V3 virtualized Shared storage disk array.

The system plans HUAWEIRH2288HV3, (CPU E5-2620V4, 16G memory 600G hard disk) server, as a silver enterprise server, deploys two independent physical machine servers. System antivirus virus database upgrade server, and system antivirus virus database requires independent physical server.

V. SYSTEM IMPLEMENTATION

Tai'an City health big data ecological domain designed in accordance with the above framework system, it has completed the overall planning of nearly 300 platforms and products in 8 categories, including basic platform, medical service, health service, healthy family, business system, benefit people service, business supervision, emerging technology since its construction in 2017. The system has completed the construction of all basic platforms, including platform standard management system, platform basic service, data exchange service, data resource service, information system integration platform, platform operation and maintenance system, platform security system. It has completed the construction of the information system of all primary medical institutions, including cloud HIS, cloud LIS, cloud PACS, cloud EMR and so on. Some health services have been completed, including basic public health services and family doctor services. It has completed the construction of some business collaboration systems, including medical group/medical association/medical community/specialist alliance system, health ID card management system, health record access system, two-way referral system, remote consultation system, imaging center system. It has completed the construction of some beneficial services, including health Tai'an website/app, Internet hospital, prescription sharing platform, pharmacy purchasing, sales and storage management system, online drug purchase management system, etc. It has completed the construction of some business supervision system, including medical and health supervision system, financial fund supervision system, medical insurance control system, etc. The detail is as follows:

Figure 7. Application system module map

In the above system, the financial capital clearing platform has been used in various medical and health unit in the whole city. The Fourth People's Hospital of Tai'an City, Tai'an Traditional Chinese Medicine Hospital, and Wangzhuang Town Health Center of Feicheng City of medical informatization and Internet + application have been comprehensively. It has been fully launched and stable, and has been highly praised by visiting experts. The Fourth People's Hospital of Tai'an City, the Wangzhuang Town Health Center of Feicheng City is applying for a typical case of the national universal medical health information platform.

The overall platform has achieved good application results, and the operation based on IPV9 network platform is stable and reliable.

REFERENCE

[1] Xie Jianping etc. Method of using whole digital code to assign address for computer [P].US: 8082365, 2011.12.

[2] Xie Jianping, Xu Dongmei, etc.Digital domain name specification. SJ/T11271-2002, 2002.07.

[3] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.

[4] Radio frequency identification tag information query service network architecture technical specification. SJ/T11606-2016, 2016. 06

[5] J. Onions, Network Working Group. A Historical Perspective on the usage of IP version 9. RFC1606. 1994.04.

[6] Notice of the Shandong provincial government on printing and distributing the work plan for the promotion of the construction of medical complex in Shandong province, issued by Shandong administrative office. No.51 [2017]

[7] Notice on printing and distributing the implementation plan for promoting the construction of Tai'an City medical consortium, issued by Thailand administrative office. No.14 [2017]

[8] Opinions of the Shandong provincial government on the implementation of document. No.47 [2016] of The State Council on promoting and standardizing the development of the application of big data in health care. No.55 [2017]. Issued by the Council of Shandong province.

[9] Notice of the national health and family planning commission on printing and distributing guidelines on the application of hospital information platform. No. 1110 of the planning letter of the national health office [2016]

[10] Notice of Shandong provincial health and family planning commission on the implementation of contract service for family doctors. No.6 [2018]

[11] Notice on the 100-day action of Internet + medical and health care for the benefit of the people. No. 2019 [2018]

[12] Notice of the State Council on printing and distributing the implementation and assessment program of healthy China action organization. No. 32 [2019]

Crawler Technology Based on Scrapy Framework

Wu Hejing
East University of Heilongjiang
Heilongjiang, China
e-mail: 499917928@qq.com

Abstract—With the development of the times and the popularization of scientific and technological products, the Internet has become inseparable from our lives, and search engines have become a daily necessity of people.In view of the growing needs。 **This topic requires the design of a prototype crawler system based on Scrapy framework. The specific requirements and contents are as follows: analyzing the structure and rules of the target website, looking for data items that need to be crawled. Based on Scrappy framework, a crawler prototype program is implemented by customizing crawling rules.Select the appropriate database for data access and analysis.**

Keywords-Creeper; Scrapy; framework; Python; Cookie

I. INTRODUCTION

With the development of the times and the popularization of scientific and technological products, the Internet has become inseparable from our lives, and search engines have become a daily necessity of people. Users can search information by inputting keywords into search engines to find information related to keywords. But with the explosive growth of network information, it becomes more difficult to find the desired information accurately.

In order to meet the growing needs, this paper chooses Scrapy, an open-source crawler framework based on Python, to crawl the "knowledge", and to learn and analyze the principle and running process of the crawler. On this basis, a prototype program of web crawler is implemented, and data crawling and storage are completed.

Firstly, this paper introduces the development process of the crawler, the working principle and classification of the crawler and the grasping strategy, and focuses on the current popular Cookie and its corresponding Session and Robots protocol.

Secondly, the use of Scrapy framework is introduced in detail. Using Scrapy framework to develop crawlers, the process and implementation details of developing crawlers by Scrapy are introduced in detail.

Finally, the crawler is tested and the results of crawling are shown.

II. WORKING PRINCIPLE

In a word, a crawler is a script or program that can get information and save it. The first step is to send a request to the target web page or website, and then get the response from the server.

Universal crawler is an important part of search engine. Its main function is to collect web pages on the Internet, then save them and process them.

Focus on crawlers, crawlers for specific needs. When it crawls a web page, it filters the first content and grabs the web page information related to the requirements.

DOI: 10.21307/ijanmc-2019-056

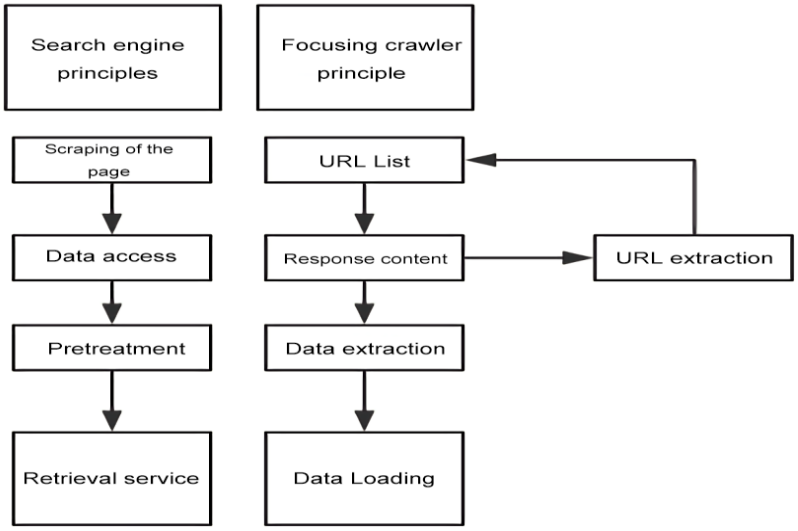


Figure 1. The Difference between Universal and Focused Reptiles

The crawler workflow is similar to the principle of ordinary users accessing web pages. When a user opens a web page, the browser will send a request to the server visiting the site, and the server will respond to the request and return it to the browser Response. The browser will parse the Response to display the web page[9]. The general crawler framework is shown in Fig. 2below.

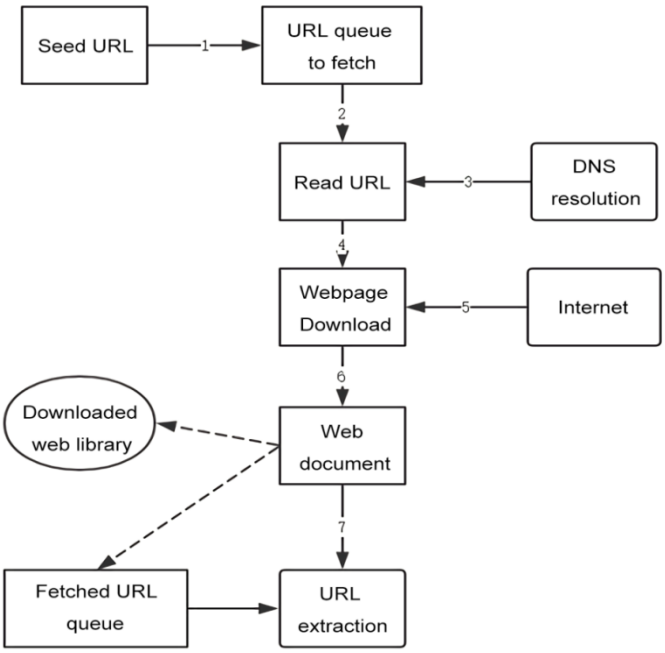


Figure 2. Universal crawler framework process

First of all, select some sites in the Internet, and take it as a starting point.Put these starting points into the queue to be grabbed, perform the queue out operation, and read out the queue elements.Resolve the URL of the target site through DNS.DNS will convert the domain name to the corresponding IP. The Downloader Downloads the target page through the server.The URL of the download page will be extracted.Reduplicate the crawl URL queue.The URL of the crawl URL queue continues to loop until the waiting URL queue is empty.

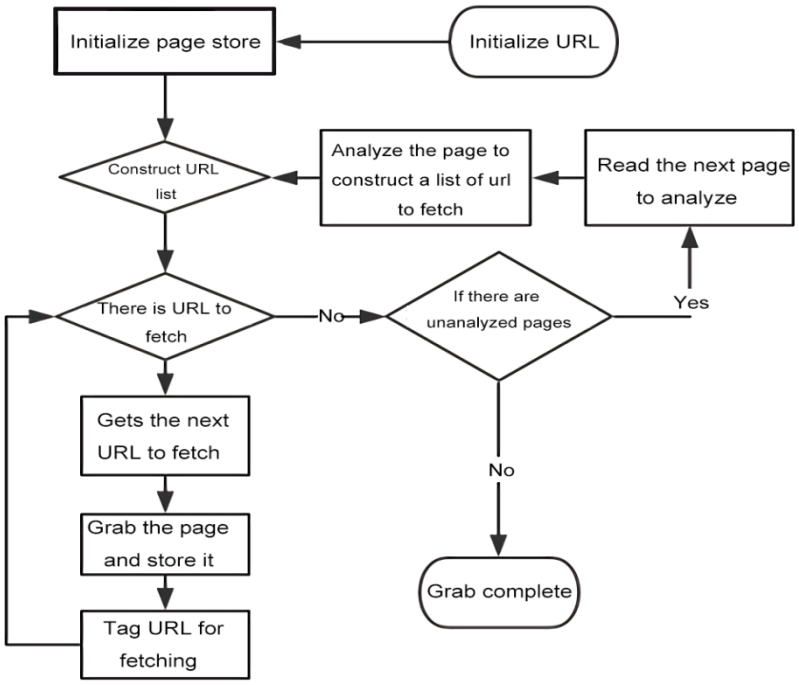


Figure 3. Network crawler flow chart

III. DETAILS OF CRAWLER IMPLEMENT

Data items are obtained by debugging web pages that know the user interface.The fieldin Python can accept almost any data type.

Follower_info_parse has two functions: first, it can initiate requests for user information through the attention list; second, it has the function of turning over pages. By parsing the response, it can obtain all users of the current target attention list and obtain detailed information of users. There is also the function of page scheduling to get the list of concerns on the next page. Further requests are then retrieved recursively for circular crawling. Followee_info_parse, which can request user's detailed information through fan list, also has the function of turning pages. Its implementation logic is exactly the same as follower_info_parse, except that the object of the request is different. One is to request detailed information from the person concerned, the other is to request detailed information from the person concerned with the current user.

```
class UserItem(Item):
    name = Field()
    avatar_url = Field()
    headline = Field()
    description = Field()
    url = Field()
    url_token = Field()
    cover_url = Field()
    answer_count = Field()
    articles_count = Field()
    commercial_question_count = Field()
    favorited_count = Field()
    follower_count = Field()
    following_columns_count = Field()
    following_count = Field()
    pins_count = Field()
    question_count = Field()
    thanked_count = Field()
    vote_from_count = Field()
    following_question_count = Field()
    following_topic_count = Field()
    hosted_live_count = Field()
```

Figure 4. Field definitions in item.py file

```
def followee_info_parse(self, response):
    result = json.loads(response.text)
    if 'data' in result.keys():
        for user in result.get('data'):
            yield Request(self.user_info_url.format(user=user.get('url_token'),
include=self.followee_query),
                          callback=self.user_info_parse)
    if 'paging' in result.keys() and result.get('paging').get('is_end') == False:
        next_url = result.get('paging').get('next')
        yield Request(next_url, callback=self.followee_info_parse)
```

Figure 5. Followee_info_parse method

Spiders.py is the core of web crawling module and an important part of the whole project. It defines the core business logic. Followee_info_parse, which can request user's detailed information through fan list, also has the function of turning pages. Its implementation logic is exactly the same as follower_info_parse, except that the object of the request is different. One is to request detailed information from the person concerned, the other is to request detailed information from the person concerned with the current user.

```
class ZhihuSpider(Spider):
    name = 'zhihu'
    allowed_domains = ['www.zhihu.com']
    start_urls = ['http://www.zhihu.com/']
    start_user = 'india'
    user_info_url = 'https://www.zhihu.com/api/v4/members/{user}?include={include}'

    user_query = :...
    follower_url = :...
    follower_query = :...
    followee_url = :...
    followee_query = :...
```

Figure 6. ZhihuSpider

IV. RUNNING STATUS AND TESTING

After testing, the crawler capture data of a single host can reach 400,000 users per day. The crawling speed can be artificially controlled by setting it in the code.

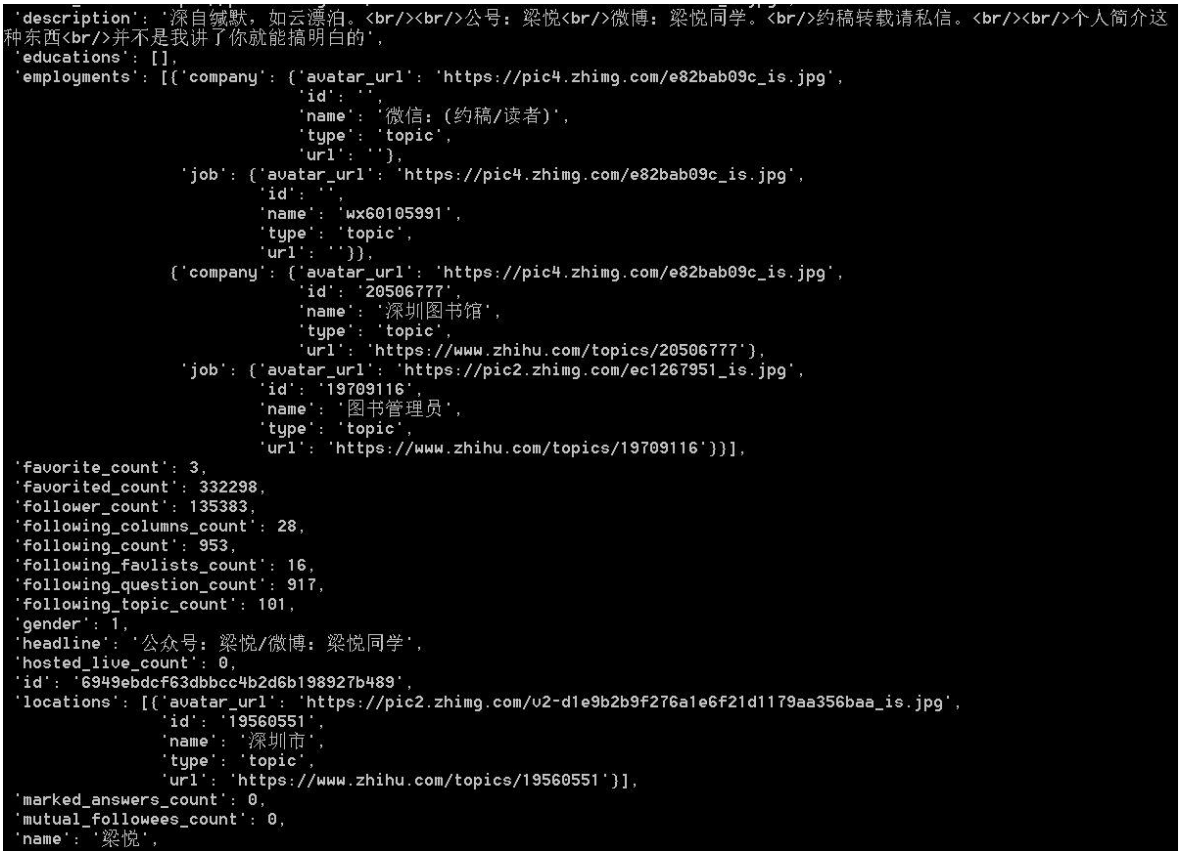


Figure 7. Screenshots of crawling 1

Figure 8. Screenshots of crawling 2

After the program runs, it gets a database named "zhihu" and stores all the information in the user table.

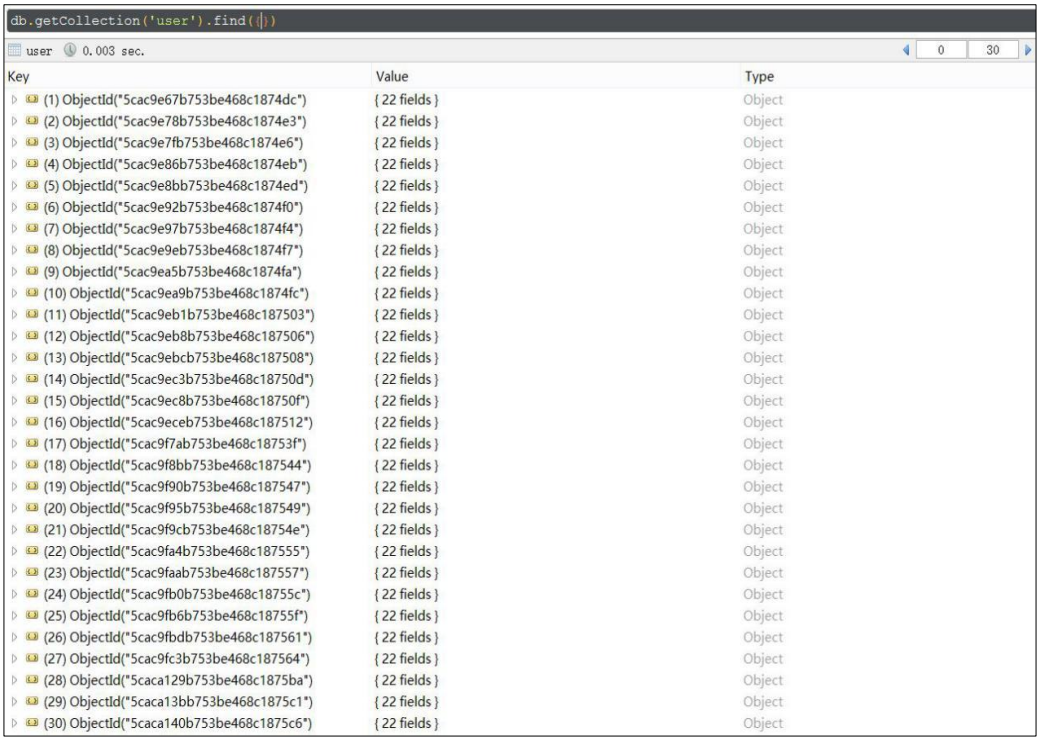


Figure 9. Database screenshots

V. CONCLUSION

When the crawler development is completed, it should be tested. Testing is a very important step. First of all, we need to know the performance of the crawler through testing, check whether the crawler has problems, and whether it can crawl the required data. Secondly, we should explore the anti-crawler strategy of the target website and improve the crawler. Finally, check the data that has been crawled to see if it achieves the expected goal of the project.The crawler system can also be extended, there are many technologies not added to it, and then added to it is the requirements of the enterprise level. In the process of writing this system, I consulted a lot of information about Scrapy. Scrapy framework is a new thing for me. New APIs and libraries. Fortunately, I have done some crawler projects before, which is not particularly difficult for me.

ACKNOWLEDGMENT

This paper is about the scientific research project of Heilongjiang Oriental University in 2019, "Implementation of Reptiles Based on Python Scrapy Framework", project number HDFKY190109.

REFERENCE

[1] Jing Wang,YuchunGuo. Scrapy-Based Crawling and User-Behavior Characteristics Analysison Taobao[P]. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on,2012.

[2] James W. McGuffee. Non-profit geographically constrained locator[J]. ACM SIGCASComputers and Society,2015,45(2).

[3] Yuhao Fan. Design and Implementation of Distributed Crawler System Based on Scrapy[J].IOP Conference Series: Earth and Environmental Science,2018,108(4).

[4] Shen Jie, Li Yifan. Application of Web crawler system in cloud media [J]. China Cable Television, 2018 (05): 595-597.

[5] Zhang Jin. Research on Web crawler technology based on Hadoop platform [D].Nanjing University of Posts and Telecommunications, 2017.

[6] Zhao Fen, Lei Zhenzhen, Yang Xiaoyun, Su Pengju and Wang Shunye.Based on Baidu Tieba College Students'Network Public Opinion Analysis [J]. Computer Knowledge and Technology, 2018, 14 (28): 227-229.

[7] Ding Zhongxiang, Yang Yanhong, DuYanming. Design and implementation of video information crawling based on Scrappy framework [J]. Journal of Beijing Printing Institute, 2018, 26 (09): 92-97.

[8] Xie Zhu. Emotional Tendency Analysis for Chinese Short Texts [D].Hunan University, 2018.

[9] Wei Chengcheng. Data Information Crawler Technology Based on Python [J]. Electronic World, 2018 (11): 208-209.

[10] Ye Xiqiezhong. Research and Implementation of Tibetan Text Automatic Classification Based on Web [D]. Qinghai University for Nationalities, 2014.

[11] ZhongJiajun. Research on Copyright Infringement Recognition of News Aggregation Platform [D].Lanzhou University, 2018.

Global Internet Come into a New DNS Era

Mou Chengjin
Research Center of International Strategic, China Mobile Communication Federation
Software Evaluation Center of National Information Center
e-mail: Mcjzp139@139.com

***Abstract*—DNS, short for Domain Name System, is an analytic central system, which transfers domain names into IP addresses that can be identified by the Internet. DNS has internal traits within it to conduct commands and regulations in network communication, as well as centralized ones that are inherently political. Unlike other Internet protocols, DNS protocols penetrate the Application Layer, the Internet Layer, the Transport Layer, and provide even more complicated, tailored low-level software that are feasible to the DNS, ranging from authorized Domain Name Servers to Recursive Domain Name Servers, a domain system based Content Distribution Network (DN-CDN), whether private or public, inside or outside the network, it must be dependent on the service provided by Domain Name System (DNS). DNS includes the increase in Client Subnet in DNS Extension Mechanism (EDNS) to conduct more accurate matches to push service.**

Keyword-DNS; EDNS; SDN; IPv6; TLD

I. IMPORTANT LANDMARK EVENTS

A. DNS "Execution Day"

Knowledge of obsolescent, wrong, or inappropriate methods to conduct software work around is required when we need to go on DNS software updating or programming. Some workarounds pertain to DNS software have made it a deeper and refined situation for the US to control and inaugurate Domain Name System, unavoidably there are functional declination and an increase in unpredictable errors and safety risks. Consequently, reinforcement in Domain Name System becomes inevitable.

The Internet Engineering Task Force (IETF) proposed the implementation of DNS Domain Name System Extension Mechanism (EDNS) in 1999. In March 2016, the US Department of Commerce's National Telecommunications and Information Administration (NTIA), Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign, a company that provides intelligent information infrastructure services which was established in the United States, led to the completion of the domain name root zone key (KSK) replacement plan as domain name root zone managers.

On October 12, 2018, ICANN finished the first global domain name root zone key (KSK) rollover in the history of the Internet and announced there will be rollover every year. Professionals claimed that KSK is a unified "re-keying", followed by "DNS Execution Day" being unified "lock and hinge updating", they interlock with each other, laying codes systematically.

In May 2018, the Internet's worldwide regional regulatory agencies (RIR) announced officially that February 1, 2019would be the "DNS Flag Day". According to the official notifications from regional Internet authorities and the joint alert of the Internet community, non-compliant domain name servers will identified as "Dead" from the "Execution Day" and beyond, which will make inroads on the access of related websites.

Domain name servers are mainly authoritative domain name servers and recursive domain name

DOI: 10.21307/ijanmc-2019-057

servers oriented. Compliance is a "workaround" to dispense with or delete DNS software by updating software version, and to identify or support the Domain Name System Extension Mechanism (EDNS) by Software Defined Interconnection (SDN). EDNS is implemented by the standard RFC 6891 released by the Internet Engineering Task Force (IETF) in 2013.

The application of DNS protocols on the Internet has a history of more than 30 years. It is the first time in the history of the Internet of the "Execution Day" to maintain DNS protocols and update DNS software versions together globally, indicating the DNS into a new beginning, a new phase, and a new generation in control community. The Asia Pacific Network Information Center (APNIC) state: "We hope that all operators of authoritative DNSSEC (DNS Security Extension) servers will be able to successfully update their DNS system software and seamlessly transfer to the next 30 years of DNS era."

The London School of Economics and Political Science (LSE) published an article entitled "China and the Domain Name System" in March 2009stating,"In terms of Information and Communication Technology (ICT), DNS is an 'inherently political' technology. Because of its ability to allocate, store, and resolve Internet addresses, it is undoubtedly an important fountain of political power; and DNS is mainly for the assurance of the latent capacity to conduct successful communication between standardized technologies and system and the avoidance of duplicate allocation of a same network address. 'Inherently political' technologies also characterized by the high concentration of DNS technology itself. Therefore, these who possess the centralized technology of DNS will seize the power and dominance in cyberspace."

B. To dispense with the "next Internet IPNG"

The United States has released a series of planned preparations and foreshadows for the implementation of the "next 30-year DNS era", including the deployment of "recognition" for the Internet development.

1) To Abandon IPv6 as "next generation Internet protocols", this lasts for nearly 20 years

On July 14, 2017, the US Internet Engineering Task Force (IETF) released Document RFC 8200, announcing the latest official standard for the sixth edition of the Internet Protocol (IPv6) (Code: STD 86).The Document RFC 2460 (the draft IPv6 specification) proposed in December 1998 and the "Next Generation Internet Protocol IPNG" which was originally for the transition to IPv6 abandoned and removed.

The US Internet Regional Working Group pointed out: "In the past few years, the widespread implementation of new data protection regulations around the world is beginning to make inroads on technology companies and consumers worldwide, resulting the change to bad practices of some formerly established best methods required by IETF procedures and regulations." That is to say, the dramatic changes in the global network application environment have caused dramatic changes in the network technology frames and user needs, "which led to the inevitability and necessity of abolishing drafts (protocols) and transitional measures (plans) with IPv6 in the "next generation of Internet ", showing that the Document RFC No. 8200 is based not only on the objective summary and generalization of the history and status of the Internet but the adherence to the principle of "US first" and the maintenance of "the supremacy of US interests", the aim of cyberspace strategy and the security bottom line.

In the United States, the transition to IPv6 proposed with a pretext of the "insufficient number of IPv4 addresses"; the "IPv6 draft specification" and "next generation Internet IPNG" transition plan now abandoned based on the same principles. The reason being not simply in the design of network technology architecture; nor in the strategic error of network

deployment, but a major deployment to deepen and refine the US network hegemony, and a fundamental decision to reaffirm the “inherently political” trait of the Internet.

Correspondingly, the KSK and DNS Domain Name System Extension Mechanism (EDNS), which controls the DNS Domain Name System Security Extension (DNSSEC), are the premise and the foundation for establishing and consolidating the core role and status of DNS in the "next generation Internet ".

2) The release of three basic principles advocated by IETF intellectual property rights

In May 2017, the US Internet Engineering Task Force (IETF) issued the official document RFC8179 (BCP79), the “Intellectual Property Rights in IETF Technology”, providing three basic principles in handling Internet intellectual property problems and discarding document RFC3979 and RFC4879. TheRFC8179 document stipulates:

a) The IETF will make no determination about the validity of any particular IPR claim.

b) The IETF, following normal processes, can decide to use technology for which IPR disclosures been made if it decides that such a use is warranted.

c) In order for a working group and the rest of the IETF have the information needed to make an informed decision about the use of particular technology. All those contributing to the working group’s discussions must disclose the existence of any IPR the Contributor or any other IETF Participant believes Covers or may ultimately cover the technology under discussion. This applies to both Contributors and other Participants, and applies whether they contribute in person, via email, or by other means. The requirement applies to all IPR of the Participant, the Participant’s employer, sponsor, or others represented by the Participant that reasonably and personally known to the Participant. No patent search is required.

That is to say, “The Internet is mine, and the rules are made by me.” IETF is legitimate to choose technology that has not intellectual property rights claimed yet, or freely licensed intellectual property technology; IETF can adopt any technology with no promise of any technology license. Indicating that technology adopted by the IETF in Internet engineering applications is free from the restriction of intellectual property rights and ownership owners. It only determined by the IETF whether the technology adopted by the Internet is “compliant”; technology and any application of intellectual property rights are invalid and non-compliant without the consent of the IETF, and the IETF will not admit it. It is commonplace for the IETF to enforce the utterance of security technology in its technical specifications. The release of the three principles of intellectual property rights is only a public announcement of the “removing the burning brands from under the boiling cauldron”, “overweening” and “getting my own way” strategies.

Until November 2018, the US Patent and Trademark Office (USPTO) granted 19,296 patents for IPv6 related technologies, and the European Patent Office (EPO) granted 2,180. The abrogation of IETF for IPv6 as the "Next Generation Internet Protocol" and its decision to implement a global “DNS Execution Day” and the practice of arbitrarily shutting down the best servers of other countries (such as Iraq and Libya, disconnecting the network and services. No matter how powerful the intellectual property rights are, no matter who grants intellectual property rights to them and who's intellectual property rights are, the three principles of intellectual property rights of IETF, the US civil society organization, are placed on the authority of the government to protect intellectual property rights and the authority of the regulatory agencies. They are absolute dominate and the only "compliance" to the Internet.

The principle of “US priority” and “US interest first” and the bottom line always placed beyond

everything else, too is the cyberspace hegemony to maintain the Internet "one network for all" policy.

II. LEGAL COMPETITION FOR DATA SOVEREIGNTY

The three basic dimensions that make up cyberspace are the infrastructure-centered physical dimension, the data-centric information dimension, and the cognitive dimension centered on human behavior. For more than half a century, irreversible evolution have taken place, from industrialization to socialization, from commercialization to customization, and the quality-quantity evolution from technology-driven to data-driven, especially the dominance and influence of marginal politic power have become increasingly prominent.

The United Nations Internet Governance (IGF) organization has approved the Global Internet and Jurisdiction Policy Network (I&J) as an "open forum" with more than 200 key entities from different stakeholders around the world participated, including governments and networks enterprises, technical groups, civil organizations, academic institutions and international institutions (for some reason, no Chinese organization participated), with the focus of research and discussion being "the jurisdiction of data" for three consecutive I & J annual meetings (including the upcoming annual meeting in June 2019) .

In October 2015, the European Court of Justice (ECJ) made a landmark ruling that overturned the "safe harbor "mechanism proposed by the European Commission at the beginning of this century and has utilized by more than 4,000 companies, including IBM, Google and Ericsson. According to the European Court of Justice, the "safe harbor" mechanism does not provide adequate protection for the personal data of EU citizens, because the United States often violates the privacy protection measures established by the mechanism in the name of national security, public interest and law enforcement needs.

UK is the one with the highest penetration rate of the Internet economy in the G20 countries. The goal of the UK government is to make UK the safest country to conduct online business activities, and the government holds that the level and duration of protection for personal data should be improve simultaneously when the amount of personal data is keeping increased by the development of digital economy. On August 7, 2017, the UK Department of Digital, Cultural Media and Sports issued a report titled "New Data Protection Act: Our Reforms", which passed the new Data Protection Law to update and enforce the personal data protection in the digital economy era and to replace the 1998 Data Protection Act.

The General Data Protection Regulations (GDPR) adopted by the European Parliament came into effect on May 25, 2018. The regulation extends the data protection from subordinates to owners, refines the classification of personal private data, clarifies the "consent" requirements of the data subject, and guarantees the individual's access to the data, the right to restrict processing and the right to refuse data using, and "portable rights" (obtaining a copy of personal data processing), "erasing rights" (also known as the right to be forgotten). Severe high-limit penalties have been imposed for data managers and processors who violate the law to negate data owner rights, to restrict data processing, to interrupt data transmission or to prohibit data access.

Trump is in a tit for tat, and signed the Clarify Lawful Overseas Use of Data (CLOUD) on March 23, 2018; two months in advance of the European Union, requiring the US Federal Bureau of Investigation (FBI) and other law enforcement agencies have the right to get access to Internet data worldwide. The bill holds that timely access to electronic data provided by communication service providers is the key to the US governments for protecting public safety and combating major crimes, including terrorism; the

communication service providers that regulate, control or own such data should subject to the US law. The bill also allows other countries to store personal data of non-US citizens in the United States. According to professionals, the bill gives US law enforcement agencies infinite priority for administrating any data controlled by the service provider, regardless of where the data is stored and where it created.

In other words, the Clarify Lawful Overseas Use of Data holds that the US government, USA companies and institutions are legal and legitimate in accessing any data in the world to be prosecuted and punished against the EU General Data Protection Regulations. .

The year 2018, it called the "first world data protection year".

Undoubtedly, the protection of data sovereignty and security has risen to the battle for national sovereignty and security. What we have seen is still the battle for cyberspace data that dominated by "US priority", "US interest first". "DNS Execution Day" indicates that the cyberspace data battle has penetrated into the control and command system of the Internet in all directions.

Nomine, one of the world's three largest network information centers, is one of the world's first professional CCTLD (Country Code Top Level Domain) operators. The UK's .UK domain name management and registration agency founded in May 1996. Nomine believes that DNS plays a vital role in every network – it sets the technical standard for translating human-readable domain names into machine-aware Internet Protocol (IP) addresses.

In other words, DNS is the underlying backbone platform of network data operations, applications, services, and security. The dispute between data sovereignty and security must first involve the dispute over the control, command, standard, and initiative and discourse power of the DNS.

The "DNS Execution Day" is the inevitable result of data sovereignty competition. The United States yields none in cyberspace data, not only in technology but also in the performance and implementation at the legal level.

III. China's Network Data Has Major Security Risks

A. Servers generally hosted outside the country

When observing reversely, China is obviously lagging behind in maintaining data sovereignty and security, protecting data, paying attention to and using data. In the form of insufficient emphasis on law, owner management, and governance of data, many institutions and officials who rely on data and contact with data all day are ignorant of the principles, bottom lines, key points, methods, and approaches of data protection. They are politically confused; formality adhered, technically exaggerated, and lazy in management.

According to National Information Center's continuous real-time monitoring based on DNS open source information, there is a top-down tendency in China's party and government organs, state-owned enterprises, well-known websites (service providers) and other servers with their servers indirectly or directly hosted outside the country. In recent years, there is a large number of data leakages in citizens' personal data, corporate data, national data, and other data involving important economic, political, social, cultural, military and other sensitive industries. Some enterprises provide exclusive services of domestic servers hosting to overseas, and Content Delivery Network (CDN) services, without any scruples and hesitation.

In 2017, China ranked first in the top 10 countries of data leaking. The main member including Baidu with 2 billion user phone numbers, names and addresses; Notecase's 1.222 billion email addresses and user passwords sold on the Internet; Shanghai Chonju's 268 million email addresses and phone numbers; Ten cent's 130 million Email address and

user password sold on the network and the like. So far, how do did they reflect and rectify, and how did the government regulatory department investigate and handle with they remain unknown. However, the online articles that disclosed the truth of the leaked data were quickly delete, and the websites that published the articles were under great pressure. Not only are the rights of the individuals and units that have leaked data at least not respected and protected, but the national data security issue is actually “turned to domestic sales” after being discovered and alerted by the outside world. It is really a strange thing.

On October 11, 2018, Wiki Leaks published Amazon’s “highly confidential” internal file "Amazon Atlas." The document lists the address and operational details of more than 100 Amazon data centers in 15 cities across nine countries, among them nine data centers are in China with six in Beijing. In 2013, Amazon signed a contract with the US Central Intelligence Agency (CIA) to build a “cloud” for intelligence agencies to integrate and provide information classified as “top secret”. Amazon also operates a special Gov Cloud area (government cloud) for the US government. Amazon's government cloud center in China is located in Ningxia Province. Many local development zones and high-tech zones have numbly invited Amazon to set up data centers in the region to publicize and provide “business” training for free servers hosting.

On November 20, 2017, Amazon publicly announced that it would provide a "cloud" service to the CIA and its intelligence system (IC) members, known as the "Amazon Secret Service" (AWS Secret Region). Amazon called the service “the first and the only commercial cloud providing the government with a comprehensive data classification service, including non-confidential, sensitive, confidential, top secret data”. Amazon is the only company required to certify confidential data in the "cloud". The Net Ease mail server hosted on Amazon's AWS service platform.

The server is hosted outside the country, on Amazon,, meaning that the path and system relying on the DNS domain name address translation and resolution depend ocean penetrate (leap) China's “firewall”, with no need to go through the “mirror” in China (With no traces left).It avoid the various monitoring and supervision in China, and the big data managed by the host can be selectively filtered and then “pushed” back to the “Cloud” operated b China.

B. Revolving Doors Abound

In the early years, some college elites in the United States changed their status and became national politicians. Some senior generals retired as multinational entrepreneurs or scientific research leaders. They considered the "revolving doors" of identity conversion, which provided the possibility for the realization of the American dream.

Over the years, the concept and manipulation of the "revolving door" has applied to the Internet. Based on the situational awareness of DNS real-time monitoring, the “revolving door” problem found in the servers and “cloud” centers of publicly known websites.

The “vest effect” led by the domestic company and jointly produces the data flow to the outside is called the "inner revolving door", otherwise it is called the "outer revolving door". The original source data conducted in China hosted overseas, and the data pushed from overseas is the data being filtered (backup), and cached domestic. Data leakage or malicious utilization are only in the moment of "revolving door", and we are often asking and arguing for whether the data is leaked, how much data leaked, "towing the library" or "collision library".....

Please note that in recent years, the US Department of Justice, the Federal Bureau of Investigation, and other public evidences of criminal prosecution of Chinese citizens (including my national security officials, international students, researchers, entrepreneurs and the like) are mainly obtain through

the "revolving door"-- Open source data, information, and intelligence.

The CDN Cache Server is an important technical model supporting “revolving doors”. It is the source to provide data (content) to the territory, and also the node that receives data (content) from outside the country. Its open custom port potentially interacts with other countries. Network intrusions and attacks often utilize custom port penetration.

Among Ten cent’s 16 mail servers (IPv4 addresses), 12 of them belong to Los Angeles, with an autonomous system AS 7939, the owner being owner Hurricane Electric (HE, Hurricane Electronics); and the rest 4 in Shenzhen, with an autonomous system AS 132203/132591, with the owner being Ten cent itself. All servers have a "revolving door" function.

Apple has four major domain names in China. The “Guizhou-Cloud Big Data” page is www.colasoft.com.cnicloud.com.cn, and the other three addresses displayed on Apple's official website. The "Canonical Name" of “Guizhou-Cloud Big Data” is www.icloud.com.cn.edgekey.net, the website in China is 47.96.193.19 (www.icloud.com.cn), and the owner is AS37963 (Alibaba Cloud). The IPv4 address 104.100.56.123 mapped to the IPv4 address 23.38.201.117, and the owner is Akamai Corporation of the United States (a service provider with more than one-third of the CDN market in the world). The function of “Guizhou-Cloud Big Data” and the “revolving door” is very obvious and typical, and may involve deeper and broader cyberspace sovereignty and security issues.

The alias of China Railway 12306’s main website is www.12306.cn.lxdns.com, the website in China is 58.216.109.187, the owner is AS4134 (China Telecom), and the five DNSs bound to the alias are all in the United States (AS54994).It is a typical DNS-based content push network (DN-CDN); the domain name of the customer service center dynamic.12306.cn is hosted by the host’s IP address 210.61.207.156 (AS3462), the territory is actually Taiwan (Taipei) and the owner is incredibly the official network operator of Taiwan, Data Communication Business Group.

TABLE I. SOME OF CHINA RAILWAY’S SUB DOMAIN HOSTED IN TAIWAN [210.61.207.156]

Sub-domain name (alias)	Standardize domain name	IP address visible in the territory (A record)	Business (reference)
dynamic.12306.cn	dynamic.12306.cn.lxdns.com	110.18.246.12	customer service
ad.12306.cn	ad.12306.cn.wscdns.com	110.18.246.12	advertisement
travel.12306.cn	travel.12306.cn.wsglb0.com	110.18.246.12	go out
hotel.12306.cn	hotel.12306.cn.wsglb0.com	110.18.246.12	hotel
wifi.12306.cn	wifi.12306.cn.wsglb0.com	110.18.246.12	Radio communication
test.wifi.12306.cn	test.wifi.12306.cn.wscdns.com	110.18.246.12	test
eximages.12306.cn	eximages.12306.cn.wsglb0.com	110.18.246.12	picture
epay.12306.cn	epay.12306.cn.lxdns.com	110.18.246.12	electronic payment
expay.12306.cn	expay.12306.cn.wsglb0.com	110.18.246.12	
epay-hy.12306.cn	epay-hy.12306.cn.lxdns.com	110.18.246.12	
exservice.12306.cn	exservice.12306.cn.wsglb0.com	110.18.246.12	
hyfw.12306.cn	hyfw.12306.cn.lxdns.com	110.18.246.12	

China Railways Member Service's domain name cx.12306.cn managed by the host's IP address 163.171.129.134 (AS 54994), belonging to the United States (California), and the owner is QUANTIL NETWORKS.

TABLE II. SOME OF CHINA RAILWAY'S SUB DOMAIN HOSTED IN TAIWAN [163.171.129.134]

Sub-domain name (alias)	Standardize domain name	IP address visible in the territory (A record)	Business (reference)
cx.12306.cn	cx.12306.cn.wsglb0.com	110.18.246.11	Member Services
video.12306.cn	video.12306.cn.lxdns.com	110.18.246.11	video

The above-mentioned hosting servers had opened and used the "Tor the onion router" port 81 defined by the Internet Assigned Numbers Authority (IANA) specification. "Onion routing" is an anonymity-orient, self-contained domain name system and proxy mechanism, mostly used for "dark net" and hackers. Using Tor the onion router to highlight the hosted mainframe will definitely increase risk of severe data leaking. According to the news released by the Ministry of Public Security of China on January 25, there are 406 million passengers during the National Railway Spring Festival in 2019, which far exceeds the US population (326 million). The amount of data and information is considerable, and the value of open source intelligence is difficult to assess. If the United States and Taiwan use this path to launch a network attack or hacker intrusion, it will be able to accurately locate and track any target, and the consequences are unimaginable.

Important note: IANA was formerly managed by the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce. The establishment of ICANN is to fulfill the duties of the IANA. The functions of the two are different and mutually reinforcing, and must be implemented in accordance with the no-cost agreement signed with the Ministry of Commerce and they work well with each other. IANA's functions are developed as part of the ARPANET's deployment of the US department of advanced defense research projects agency, including: 1) coordinating the allocation of Internet Protocol's technical parameters; 2) fulfilling duties related to Internet DNS root zone management; 3) Assign an Internet IP address.

IV. THE IMPORTANT INSPIRATION PROVIDED BY "DNS IMPLEMENTATION DAY"

A. The Bankruptcy of the "Snowman Plan" Lie

The "Snowman Plan" proposed and announced by ICANN in 2015, its English name is "the Yeti DNS Project", i.e. the "Snowman DNS Plan".

ICANN's best-known responsibilities and missions are to coordinate the global Internet's unique identifier system as a technical coordinator for the Internet Domain Name System (DNS) to ensure the stable and secure operation of the unique identifier system.

The "Snowman DNS Program" website hosted by ICANN clearly states that the "Snowman DNS" system is a test platform for root domain name services and some experiments and will do not add/delete delegates in the IANA root zone, and all resource records (Resets) are identified by the "Yeti" security extensions (DNSSEC) key, no alternate domain space is provided.

Paul Dixie, proclaimed himself as the "father of domain names", one of the founders of the Snowman DNS Program, stressed and warned in 2016 that if the "Snowman Plan" is considered to be a domain name expansion, anyone in addition to IANA will be able to effectively edit the top-level domain space, such as adding a new top-level domain (TLD) or changing the ownership of an existing top-level domain (TLD). The

answer is definitely not; if you touch it (to instead the root domain name service), you will die; and if a certain country wants to create its own Internet DNS system, independence will be unhealthy, vulgar and short-lived.

Paul's "Snowman DNS" working mode:

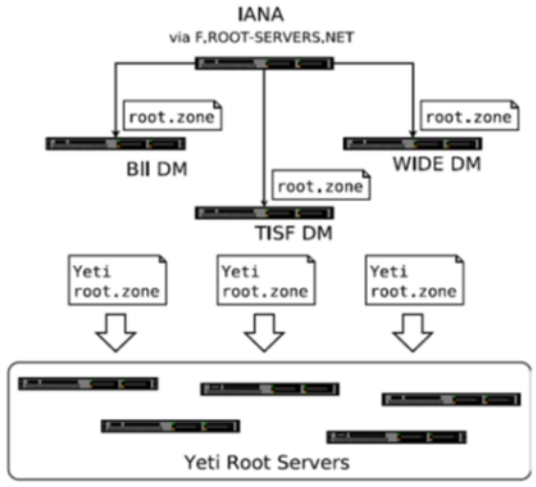


Figure 1. Snowman DNS working mode

For a long time some professionals and government officials in China spare no effort to advocate that the "Snowman Plan" is led by Chin, represented by Beijing Tinder Interconnect Information Technology Co. Ltd. (BII Group), and claimed that China had "Built a global IPv6 root server network and demonstrating a new IPv6 root server capabilities", "China deployed four IPv6-based root servers, breaking the predicament of China with no root servers in the past." and the like.

Ruthlessly, the "DNS Execution Day" returned the "Snowman Plan" back to reality. The result of DNS's compliance announced the impeachment of the "Snowman Plan" in the beginning of the Internet's "the next 30 years of the DNS era"; or it was a "slapstick" exploited by someone. The practice makes "alternative routes for the domain name" unsustainable, as well as the melting of invest and foundation of the "snowman" (deceitful publicity and fake amounts) which lasts for more than three years.

Beijing Tandy Interconnect Information Technology Co. Ltd. (BII Group)'s IPV6 domain name server compliance testing result

IPv6 address: 240c:f:6644:2:0:276a:c70

Test result: Fatal error detected

dns=timeout
edns=timeout
edns1=timeout
edns@512=timeout
ednsopt=timeout
edns1opt=timeout
do=timeout
ednsflags=timeout
docookie=timeout
edns512tcp=timeout
Optlist=timeout

All 11 tests are out of order

Figure 2. Result of IPV6 DNS Compliance Testing

It is worth pondering that the DNS Extension Mechanism (EDNS) was proposed by Paul in 1999 (RFC 2671) and became a standard in 2013 (RFC 6891). However, Paul turned a blind eye to "snowman" deceitful technology, its non-compliant application and self-deprecating in the Internet community (that is, the flexible workaround of the claimed "one world, one Internet, one domain name system"). So where does the reason lie? Is Paul fooling the experts of the BII Group or vice versa? Or is there a tacit agreement between the two?

The above facts also clearly reveal that the Internet vitality based on IPv4 technology is still vigorous. For the United States, the "DNS era of the next 30 years" is still the IPV4 era.

According to the "USG v6 status statistics" collected by the National Institute of Standards and Technology (NIST) until December 22, 2018, only 2% of the US-supported IPv6 industries are still in operation in spite of the US government's nearly 20-year IPv6 transition plan,98% of them have transitions or no progress; only 3% of US universities use IPv6 domain name operations, 97% of them have

transitions or no progress, which is an abnormal dynamic that cannot be ignored. According to the APNIC statistics, until October 31, 2018, the rate of US IPv6 users has dropped from the first to the third worldwide, and China ranked 71st. According to Google's monitoring, the adoption rate of IPv6 in the United States is actually a mere 36.31%.

The Asia Pacific Network Information Center (APNIC) report pointed out that from the second half of 2017 to August 2018, the IPv6 deployment status had declined. Operators who are under higher pressure of an IPv4 addresses shortage have a low IPv6 deployment rate, which does mean that there is no urgency to deploy IPv6 in a client/server (C/S) environment in many areas of the Internet. In other words, the pressure of address shortage is not a sufficient and necessary prerequisite for deploying IPv6 on a large scale.

Entrusted by the Office of the Chief Technology Officer (OCTO) of the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Projects Group (IGP) of the Institute of Public Policy at the Georgia Institute of Technology published a survey report entitled “latent standard war” in February 2019, the research analysis found that it’s not a “transition” issue that makes sense between IPv4 and IPv6, but economic disputes between the two routes in technological evolution; and the current lopsided IPv6 deployment rate and the relevant data violates a simple or predictable pattern.

According to “Supporting China's IPv6 Scale Deployment - China's IPv6 Service End-to-End User Experience Monitoring Report” released by China's “National Next Generation Internet Industry Technology Innovation Strategic Alliance” on November 1, 2018, there are 7.18 million IPv6 Active Users (IPv6 Allocated and with IPv6 Internet history records within one year) with mobile broadband and 2.33 million with fixed broadband, 9.51 million in total. According to the “promoting the scale of IPv6deployment” requirements to reach a 200 million at the end of 2018, the current number is still far behind.

IPv6 subverts the situation of IPv4 network application architecture, and it is difficult to solve a large number of known and unknown security traps and security barriers.: huge investment and operation and maintenance costs, and the economic benefit in the future is distant no matter whether it is market economy or planned economy; the balance of trade-offs. It is imperative to re-adjust the strategy of deploying IPv6 in a realistic manner. Our country must make an early decision.

In the face of well-known and irrefutable facts, what will the Beijing Tandy Interconnect Information Technology Co. Ltd. (BII Group)’s experts say? Self-defense or explanation? Should the administrative, law enforcement, auditing, and supervision departments of the state and governments at all levels seriously perform their duties?

B. BIND is the Key and Crucial Part

The US Defense Advanced Research Projects Agency (DARPA) funded the development of BIND in 1980 and BIND, which was taken over by the US Internet Systems Alliance (ISC) after 1984, is the most important core step and strategic deployment of the Internet. It is for not only the "kidnapping" of the DNS hub platform, but also for the close integration in the "soft and hard" aspects, firmly grasping and controlling the ownership, command, control and decision-making power of the DNS. BIND has embedded in the DNS and has become the “de facto standard” for DNS bundled applications. The global software market, which dominates DNS applications, is not only a “traffic light” rule that guides the flow of Internet data, but also a baton that conducts compulsory obedience if you have “bad Behavior”; you will be in violation of the law, get lost, embarrassed, and chaotic or hit the wall.

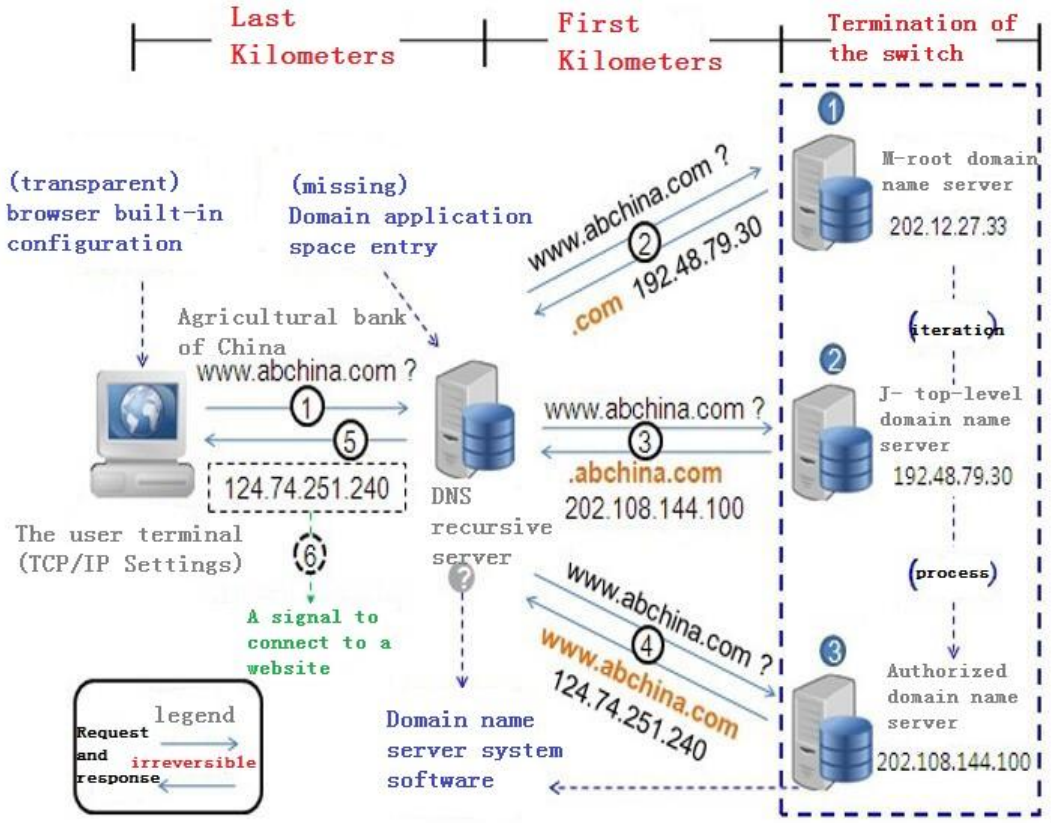


Figure 3. Structure of BIND

The picture above shows that under the role of BIND (control command guiding software interconnection and interoperability), the DNS application drives the recursive server, the recursive domain name server and the domain name resolution system perform conduct three irreversible domain name resolution iterations by "right to left" interaction process. However, any of these links may be eavesdropped, stolen, tampered with or transferred. It may also be a "safe information exchange" after being "legally mirrored" by the hierarchical service providers. It is “sifter-type” vulnerability that professionals must have knowledge of it.

The US Department of Defense uses the domain name system to set the Internet logical boundary, and the US Department of Defense Network Information Center (DOD Network Information Center) operates and manages the military-specific network NIPR net. BIND (developed by the US Department of Defense), which is solidified in DNS, was targeted to the data flow to the US Department of Defense Network Information Center firstly and then to other network information center nodes such as intelligence departments.

We must pay attention that the process DNS request data (and information) is identical during the parsing interaction. Some experts explained that: “The content stored in the root server is very few. Usually, ordinary users will not access the root server when they surf the internet.” If it is not an ignorant mistake, it must be intentionally misleading.

Given the information on May 12, 2017, when the “WandaCry” ransom ware incident spread rapidly in

more than 150 countries and regions around the world. A British engineer stumbled upon the "want to cry" virus through domain name to conduct command and control (C&C), and used the "Kill Switch" method to effectively curb the “WandaCry” virus, which was praised by the industry and the media as an “Accidental Hero”. At the same time, the world has realized the BIND solidified” end switch” function of the DNS.

“Termination switch” is a new Internet term or a network hot word involving data sovereignty, network security, and Internet governance. The exact definition of Internet Kills which is: a control mechanism designed to be activated as a countermeasure to shut down all or part of the Internet traffic.

US Senator Joe Lieberman and other people submitted a legislative proposal “Protecting Cyberspace as a Nationalization Act Asset Act of 2010)” (S. 3480) at the 111th Congress on June 19, 2010, was called by the media as the Internet Termination Switch Act.

The Electronic Privacy Information Center (EPIC) of the American Civil Human Rights Organization began to track the US government's Standard Operating Procedure 303 secret plan document in 2011. The 30-page “Emergency Radio Protocols” drafted by the National Telecommunications Coordination Center (NCC) and approved by the National Communications System (NCS), proposes the process to “close and restore commercial and private wireless network when the country is in crisis.” It represents the policy of the US government and is also called the "Internet Kill Switch" by the industry and the media.

ICANN's official website published a passage entitled “What is the Internet termination switch? Who has the key?”On July 22, 2016, clarifying that the Internet "termination switch" is in the domain name root zone and ICANN holds the key. Russian experts call it the “red button of the Internet.”

Europe, Russia and other countries have been highly vigilant against the US control and command to solidify BIND's DNS. The NSD developed by NLnet Lab in the Netherlands based on BIND standards. Although the technology research and the support are relatively independent, it has not yet to form a mainstream. But at least, from the perspective of DNS application, it is possible to avoid “all eggs in one basket” and reduce risks; and from the perspective of open cooperation, research and development of controllable technologies and products can lead to the balance of different companies and seek a balances; in the long run, it is beneficial to the Internet domain “building” to balance of DNS control. Russia recently announced that it will take the test out of the global Internet in the near future (April 1). The focus and purpose is to check the content blocked by the traffic, to ensure that the traffic between Russian users (more than 90%) remains in the country, and it can only be the necessary countermeasures about research and development to control parallel DNS.

Our country should catch up. While drawing on and utilizing BIND in the United States and NSD in Europe, we can encourage the reference to the boundary and frontier security defense measures of the "Einstein 3" plan, and cut into the situational awareness based on real-time monitoring of DNS open source data information to accumulate experience, and re-recognize and explore the source of governance and control of the Internet, strive to develop the DNS system software that is self-controllable and compatible (check and balance) for both BIND and NSD.

C. Data Sovereignty and Security are the Key Point

In summary, Data Sovereignty has become the consensus and action of the United States, the European Union, and many countries (including the legislation and governance), especially after the “Prism Gate”, it becomes the important “topflight” Without the principle of data sovereignty, not only is data

security and privacy at risk, but national data assets are inevitably threatened. In particular, it should be pointed out that the "interconnection" of the Internet today is conditional and bordered! For example, China's IP address is used as a "blacklist" by some professional websites outside the country, and the access to it is prohibited (404, no access authorization).

The general identification of data sovereignty is: the government's control over the collection of data in the country, including data residency (the location where data is forced to store), data retention (the compulsory reservation of data trade records).

The United States is the initiator of the Internet. At first, it was introduced from the military APA network to the European Internet in order to transmit open source data (information, intelligence). For more than half a century, the United States has built and developed the Internet; the technological innovation is always about data sovereignty, data security and data utilization (acquiring intelligence)--all for data. Even from this perspective, we must re-recognize and deepen our understanding of the relationship between United States and the Internet, the world and the Internet, China and the Internet in all ways. We are obviously seriously lagging behind when we continue to follow the understanding, and thinking of the Internet 20 or 30 years ago in the United States and the situation even becomes more and more serious, ruthlessly ignoring our innovation and entrepreneurship in cyberspace, making us just wait and see again and again. Being completely marginalized, the scientific advancement of the future network is gradually drifting away.

Today, any network technology carries data. Network applications generate data; interconnections exchange data; network services face data; network innovation development (such as artificial intelligence) relies on data; network security (national security) protects data, Data has been integrated into the driving force of human social development, building the collective assets, culture and language of the community. Data, whether territorial or affiliated, has been transformed and applied in different degrees and at different levels "genetically modified". The "face-changing" of data has become the norm and has become a subversive factor for maintaining or shaking the fundamentals of cyberspace sovereignty and security.

Most Chinese citizens and officials are not sensitive enough to network data. They know nothing about cloud computing, big data, small probability events, open source information, and always think that there is no bearing between themselves and the unit, not to mention the full use of data, the urgent need to build and develop data centers, and the great importance of it. The DBS Group study believes that the overall utilization rate of China's data centers is less than 50%, and the utilization rate of data centers in the lower cities is only a 20%. In the next 3-5 years, the demand for data centers will not be transferred to the data centers of the lower rate cities on a large scale. Because of this, Amazon, Apple, Microsoft, IBM, etc. have come to China to build data centers in the past few years, called China services, which are actually American services. Ten cent, Net Ease, Baidu, 360, Railway 12306 and even party and government agencies have also been "managed" to overseas hosting servers in exchange for "free" advanced technology services and individual business interests in China. DNS-based CDN (and SDN) technology has formed the mainstream and technology trends of the Internet for years to come.

In most network environments of national key information infrastructure, gatekeepers, firewalls, intrusion detection systems, anti-virus software are usually configured to control the data traffic of TCP/IP and other network protocols, and to implement the physical isolation (PNI) between internal networks (private networks) and public Internet.

However, the rather universal stipulation and phenomenon deviate from the facts. Cyber security threat exploits this cognitive misunderstanding and the blind spot of supervision, DNS is used as a carrier to bypass the network security protection mechanism and transmit sensitive data from inside the enterprise to the outside of the enterprise. Even the ""physically isolated" private network still relies on DNS requests and responses to form an interaction between internal and external network (connection de facto). Usually it is "unblocked" (such as firewall port 53) and the commonly-held blind area (such as DNS abuse, misuse), so that the abnormal behavior of intranet DNS applications and information leakage through DNS is basically out of control.

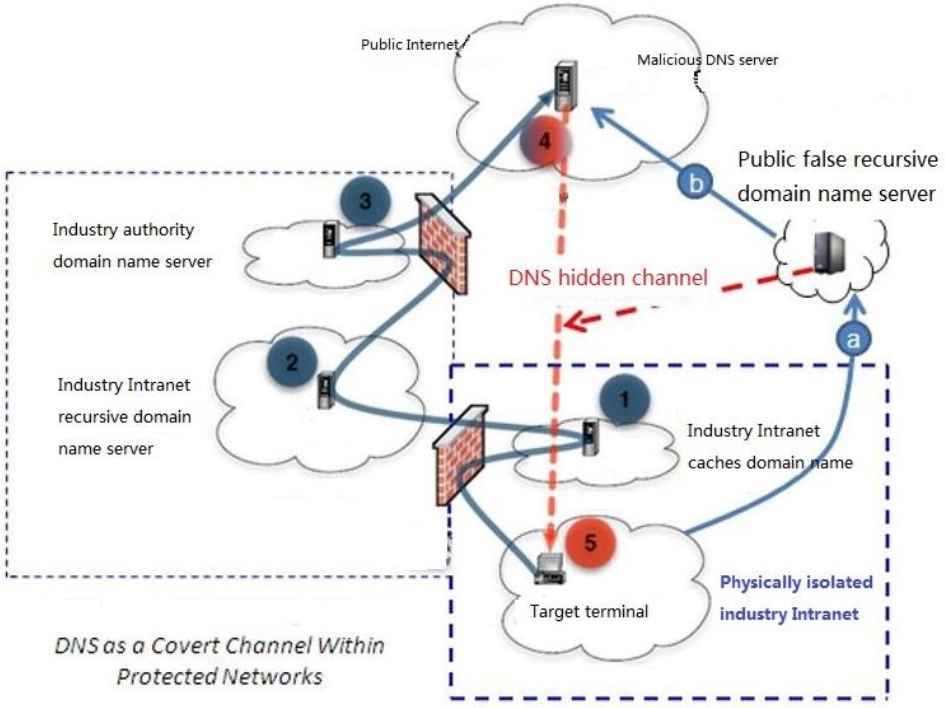


Figure 4. DNS as a Covert Channel Within Protected Networks

In the diagram above of the US Department of Energy (DOE), the "channels" of (1)-(2)-(3) are inherent to the industry intranet and industry extranets, that is, part of the network system; (a)-(b) "channel" is caused by DNS abuse or the existence of a loophole in the target terminal, that is, the application of chaos out of control (such as random use of Google public DNS service, 8.8.8.8, etc.); (4)-(5) forms the hidden channel of DNS that can be used not only as a transmission carrier for leaking data, but also as a means of command and control (C2) (such as APT).

Johnson from US Secretary of Homeland Security reported in January 2016 that the Einstein Plan for the National Cyber Security System (NCPS) began in 2010 and entered the third phase (called E3A) in April 2013. It not only monitors cyber attacks, but also has the ability to intercept and handle the confidential information; it can also effectively protect the government network's security and respond to the most advanced network attack opponents. Simultaneously E3A provides a platform for new technology research and development, and cooperates with advanced technology and expertise of government departments and private industries to discover unknown network attacks. The US Congress has mandated that all federal

administrations join the E3A program by the end of 2016.

"Einstein-3" (E3A) provides four main functions: 1) defense: real-time mitigation of already known or suspected cyber security threats; 2) screening: identification of invaded information systems, system components or host terminals, as an immediate response to security incidents; 3) perception: customized development, maintenance, and service for the network security status of the federal government information system, based on "Security is Normal Monitoring". 4) Discovery: monitoring and identifying new or emerging cyber security threats targeting federal government information systems to enhance cyber security defenses.

It is recommended that the state should formulate and launch China's network sovereignty and security strategic plan based on "Einstein-3" (E3A), using the existing network infrastructure to build an autonomous and controllable DNS situational awareness system, and build China's data sovereignty, data security, and data utilized for the new cyberspace Great Wall.

V. CONCLUSION

Today's Internet is facing a number of major changes. All countries are trying to grasp the latest technology for this revolution. As the United States announces the abandonment of the "next-generation Internet IPNG", it marks the entrance to a new era for the Internet. Based on the current status of worldwide Internet domain name system research, this paper analyzes the international research level of this technology, discusses Internet security and data security problems we are now facing, and puts forward the importance of independent research and development of Internet domain name system. At present, most of the servers in China are still hosted in foreign countries, which pose considerable, latent danger to data security. Under the current environment of Internet innovation, it is necessary to grasp the immediate opportunities and conduct research and development of the Internet domain name system to ensure China's data sovereignty and information security, and keep pace with the Internet development era.

VI. ACKNOWLEDGEMENT

This passage is written by the Director of International Strategic Research Center of China Mobile Communication Federation; the Chairman of Nanjing Huadao Network Technology Co. Ltd.

Street View House Number Identification Based on Deep Learning

Yang Haoqi
School of computer science and engineering
Xi'an Technological University
Xi'an, China
e-mail: curioyhq@gmail.com

Yao Hongge
School of computer science and engineering
Xi'an Technological University
Xi'an, China
e-mail: 835092445@qq.com

***Abstract*—In this paper, the difficult problem of character recognition in natural scenes caused by many factors such as variability of light in the natural scene, background clutter and inaccurate viewing angle, and inconsistent resolution. Based on the deep learning framework PyTorch, a convolutional neural network is implemented. Based on the classic LeNet-5 network, the network optimizes the input layer to accept three-channel images, changes the pooling method to maximum pooling to simplify parameters, and the activation function is replaced by Rectified Linear Unit with faster convergence. The cross-entropy loss is used instead of the minimum mean square error to mitigate the slow learning. Furthermore, we also enroll the gradient descent optimization algorithm RMSprop and L2 regularization to improve the accuracy, speed up the convergence and suppress the over-fitting. The experiment results show that our model achieved an accuracy of 92.32% after training for 7h24min on the street view house number(SVHN) dataset, effectively improving the performance of LeNet-5.**

Keywords-House Number Identification; Convolutional Neural Network; Lenet-5

I. INTRODUCTION

The traditional method of classifying house numbers from natural scene images is usually to use manual feature extraction[1-2] and template matching[3-4]. In order to identify the house number of the corridor environment, Zhang Shuai et al. used the combination of Robert edge detection and morphological operation to locate the position of the house number image, and then divide the house number by horizontal and vertical projection method, tilt correction, etc., and finally use pattern recognition to identify the house number [5]. Ma Liling et al. used the linear discriminant linear local tangent space alignment algorithm (ODLLTSA) and the support vector machine (SVM) method to identify the house number, use the extracted features to train the SVM classifier, and use the SVM classifier to the new house number classification [6].

For these traditional methods, the key to determining their performance is to have a good classifier, and the features in the classifier are mostly designed manually (such as SIFT, SURF, HOG, etc.), and the features of the artificial design are well interpreted. However, in the face of complex backgrounds, changing fonts and various deformations, it is rather troublesome and difficult to extract more general features[7].

The Convolutional Neural Network (CNN) is a multi-layered supervised learning neural network. Although the training process requires a large amount of data compared with the traditional method, the convolutional neural network can automatically summarize the target feature from these data. Features do not require human intervention. Overcome the shortcomings of manual design features that are time-consuming and labor-intensive, have poor general use and require high experience in the designer field. It is precise because of these advantages of convolutional neural networks that a large number of researchers have begun to apply it to solve character recognition problems.

In response to this situation, we implemented a LeNet-5-based neural network based on the deep learning framework PyTorch and achieved an accuracy of 92.32% on the SVHN dataset at a time of 6 hours and 17 minutes.

II. RELATED WORK

A. Network structure

The network used in this experiment is modified by LeNet-5 as shown in Figure 1. LeNet-5 appeared to solve the problem of recognition of handwritten characters. The data set used in the training process is the MNIST. The samples in the data set are single-

DOI: 10.21307/ijanmc-2019-058

channel grayscale images, and the street view dataset is The three-channel color picture, to improve the robustness of the model, minimize the intervention on the original data set, we do not pre-process it, such as grayscale, but choose to adjust the input layer of LeNet-5 to three channels.

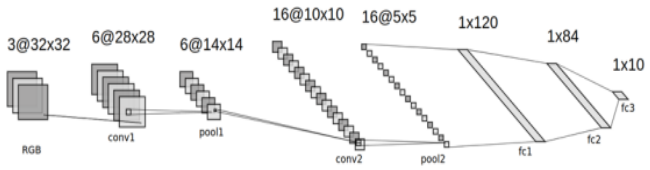


Figure 1. Network structure

The pooling layer in the original LeNet-5 network is very different from the currently recognized pooling layer operation, so we replace it directly with the max-pooling layer, which on the other hand reduces the number of trainable parameters of the network. It is conducive to controlling the scale of the network and speeding up the training. In terms of the activation function, the activation function in the original LeNet-5 is Sigmoid or TanH. Here we use a Rectified Linear Unit (ReLU) with faster convergence speed and no significant impact on the generalization accuracy of the model. LeNet-5's loss function is Minimum Mean Squared Error:

$$MSE = \frac{1}{n}\sum_{i}^{n}(\hat{y}_i - y_i)^2 \# \quad (1)$$

Where n is the number of samples， $\hat{y}_i$ represents the predicted value of the ith sample, and y_i is the labelof the ith sample. In the case of back-propagation by the gradient descent method, the minimum mean square error is easy to occur when the neuron output is close to '1' and the gradient is too small to learn slow. We use the cross-entropy loss function here:

$$L = -\sum_{i=1}^{n} y_i \, log(\hat{y}_i) \# \quad (2)$$

In addition to the above improvements, we will introduce four optimization algorithms, SGD (with momentum), Adam, Adamax, and RMSprop.

B. Comparison effects of different optimizers

The package 'torch.optim' in PyTorch encapsulates a large number of optimization algorithms, which are often referred to as optimizers. In Figure 2, we take the more common SGD, Adam, Adamax and RMSprop optimizers according to the parameters listed in Table 1.After 90 epochs training, compare their optimization effects on the SVHN dataset used in the improved LeNet-5 network proposed in this paper. It can be seen from Figure 2 that the network using the SGD optimizer has almost no improvement in the test set accuracy in the first 14 epoch, and the 14th epoch only starts to rise significantly; the network using the other three optimizers is in the toptenepochs, a good test set accuracy rate is obtained, and the test set accuracy of the network using the RMSprop optimizer is the fastest. So in the next experiment, we will use RMSprop as the default optimizer.

TABLE I. OPTIMIZER PARAMETER SETTING

Optimizer	parameter
SGD	lr=0.001,
Adam	lr=0.001,
Adamax	lr=0.002,
RMSprop	lr=0.001,

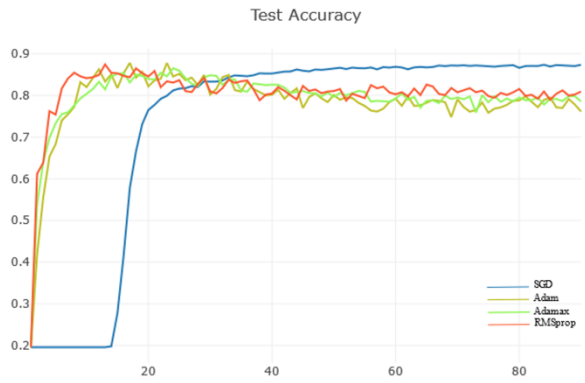


Figure 2. Optimizer effect

It can be observed from Figure 2 that the accuracy of the test set except the SGD optimizer is not improved much in the later stage of training, and the accuracy of the test set of the other three networks even shows a small downward trend. Table 2 shows the statistics in Figure 2. The data of test sets with high accuracy rate, the difference ofhighest accuracy rate on the SVHN test set is only 1.793816%, which can be considered as the optimization effect of the four optimizers on the accuracy rate; From the position of the highest test set accuracy, only the 7th epoch appears in the network using the SGD optimizer. The highest test set accuracy of the network using the other three optimizers is relatively high, indicating that theperformanceofthese three optimizers in the latter part of the trainingdecreased. It may be that the

network has been over-fitting, and it is necessary to introduce evaluation and avoid over-fitting.

TABLE II. OPTIMIZERS TRAINING RESULTS

optimizer	Top Accuracy/%
SGD	87.350184
Adam	89.090000
Adamax	88.955900
RMSprop	88.676000

C. Comparison of the application of L2 regularization with the appropriate weight attenuation coefficient

In the face of possible over-fitting, one possible inhibitory measure is the introduction of regularization. We first use the L2 regularization and introduce the training set accuracy rate, training set loss, test set loss three indicators to enrich the evaluation results of the experimental results. The experimental design is shown in Table 3. The default optimizer is RMSprop (lr=0.001, alpha=0.9), the maximum iteration number is still set to 90epoch, and the L2 pooling corresponding weight attenuation coefficient (weight_decay) is the best and the best. The resulting position is shown in Table 3, and the corresponding accuracy and loss curves are shown in Figure 2-6.

It can be seen from Table 3 and Figure 4 that the training set loss curves show a smooth downward trend under the four values of the weight attenuation coefficient. Comparing the training set accuracy rate of Figure 3 with the test set accuracy rate of Figure 5, it can be seen that the accuracy rate under the corresponding weight attenuation coefficient is about 5% up and down, within an acceptable range, but the weight attenuation coefficient in Figure 6 is The loss curve of the test set at 0.001 is firstly decreased and then increased. This indicates that the over-fitting phenomenon appears under this parameter, which indicates that the improved LeNet-5 network proposed in this paper is attenuated by the weight of 0.001 when training on the SVHN dataset. The coefficient can not suppress the over-fitting, we should choose a higher weight attenuation coefficient; from Table 3, we can see that the data with the weight attenuation coefficient of 0.0025 is better than the weight attenuation coefficient of 0.005 and 0.01. On the accuracy curve of the test set in Figure 5, the curve with the weight attenuation coefficient of 0.0025 is higher than the curve with the weight attenuation coefficient of 0.005 and 0.01, and the weight attenuation coefficient is 0.0025 in the later stage of the training process. More obvious and less shocking. The above analysis shows that among the selected four sets of weight attenuation coefficients, the weight attenuation coefficient of 0.0025 can avoid over-fitting and achieve better training results.

TABLE III. RESULT OF DIFFERENT WEIGHT DECAY

weight_decay	Train Acc%(e)	Test Acc%(e)
0.01	89.01538(85)	87.14659(85)
0.005	91.59397(57)	88.95590(57)
0.0025	94.51470(88)	90.01229(88)
0.001	97.21119(90)	89.70498(24)

Figure 3. Training Accuracy of different regularization

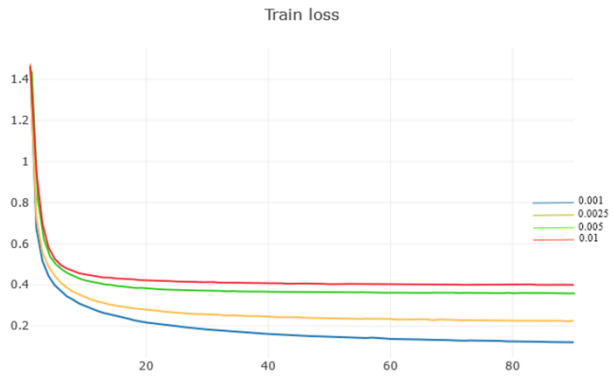


Figure 4. Training Loss of different regularization

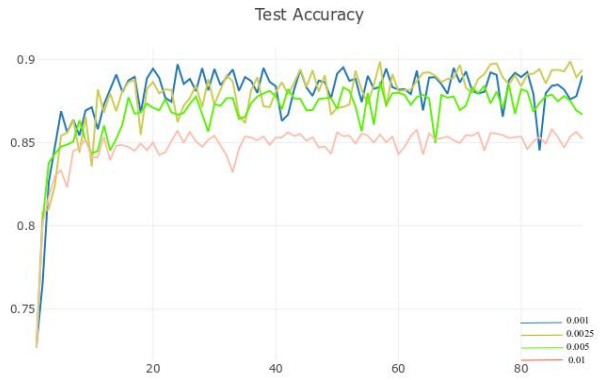


Figure 5. Test Accuracy of different regularization

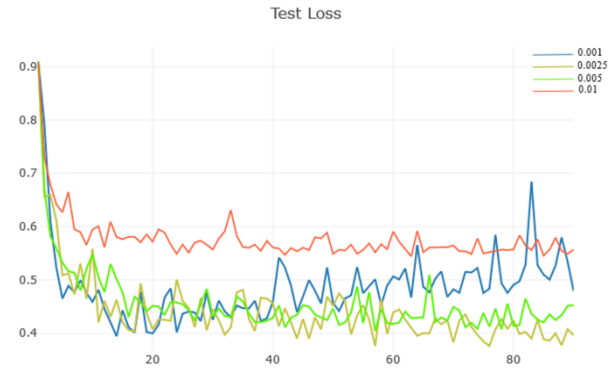


Figure 6. Tetst Loss of different regularization

III. EXPERIMENT AND ANALYSIS

A. *SVHN(The Street View House Numbers)*

Currently, for the identification task of the street view number, the better public data set is the SVHN data set. The SVHN dataset is a real-world image dataset focused on the development of machine learning and target detection algorithms with minimal need for data preprocessing and format conversion. There are ten types of labels in the dataset. Each class represents 1 number. For example, the category label of the number "1" is 1, and so on. The label of "9" is 9, and the label of "0" is 10. In general, the SVHN dataset contains three subsets: training set, test set, and extended set; the data set is divided into two formats based on the difficulty of recognition: a character-level bounding box containing the entire house number and a small number of wall backgrounds. The full resolution image (Figure 7); a 32x32 pixel centered on a single number similar to the MNIST dataset format image (Figure 8). The latter style is highly similar to the classic MNIST dataset, but is larger and more difficult to identify: the training set consists of 73,257 hard-to-recognize digital images, and the test set consists of 26,032 digital images, with an additional set of 531131. A simpler digital image that can be used to extend the test set. Unless otherwise stated, the SVHNdataset mentioned later in this article refers to the dataset in the format after cropping.

Figure 7. SVHN-Complete house number

Figure 8. SVHN-Part number

B. *Data augmentation*

Augmenting the data set is also an effective means to improve the accuracy of the model. The size of each subset of the SVHN dataset is shown in Table 4, where the extension set official mentions that it can be used to extend the training data. Figure 9-11 shows a small number of samples and their labels in each subset. It

can be seen that the resolution and brightness of the extended set are high and the background interference is small. The human eye recognition is indeed higher than the training set and test set, that is, It is said that the recognition of the extended set is relatively difficult, but the addition of the extended set can make the training set expand to 8.25 times, which is still expected to improve the accuracy of the model. Figure 12 shows the distribution of the original training set, extension set and test set ("1" for the number 1, "2" for the number 2, ..., "10" for the number 0), which can be seen in the three sub-categories The proportional distribution of each category is approximated, so the distribution of the new training set incorporating the extended set is similar to the distribution of the original training set. This correlation helps to suppress the disadvantages brought by the introduction of the extended set to the model training. influences.

TABLE IV. AUGMENTATION RESULT

Subset category	Number of samples
Training set	73257
Extra set	531131
Test set	26032

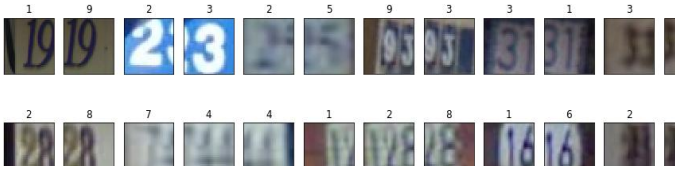


Figure 9. Example of train set

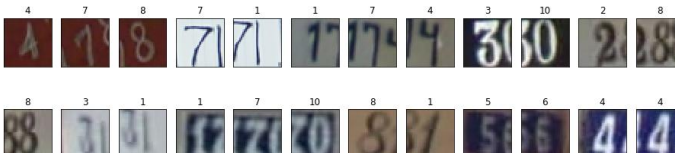


Figure 10. Example of extra set

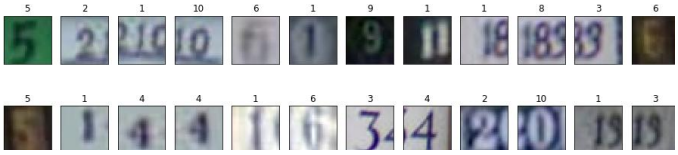


Figure 11. Example of test set

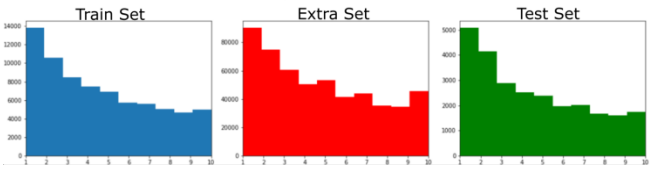


Figure 12. Category distribution of SVHN

The effect of 90 epoch training before and after the introduction of the extended set is shown in Table 5 and Figure 13. One point that needs to be specially stated is that the visualization tool Visdom we use has an automatic zoom function when drawing, which automatically hides the blank area of auto-hide the chart. Therefore, the different training sets in Figure 13 correspond to the vertical axis starting position and scaling of the chart. It's the same. The accuracy of the training set is lower than 95% and the loss curve of the test set shows a downward trend, indicating that there is no over-fitting phenomenon after expanding the data set; the accuracy of the test set is gradually reduced in the later period. The small description model tends to converge, and it can be seen that the model after the extended training set is higher than the extended training set. From Table 5, it can be seen that the training time after the expansion of the training set is 4 hours and 53 minutes, and the best accuracy rate is increased by 2.31254% compared with the expansion.

TABLE V. RESULT AFTER DATA AUGMENTATION

Train sample number	test sample number	Best test accuracy	time
73257	26032	90.01229	1h24min
604388	26032	92.32483	6h17min

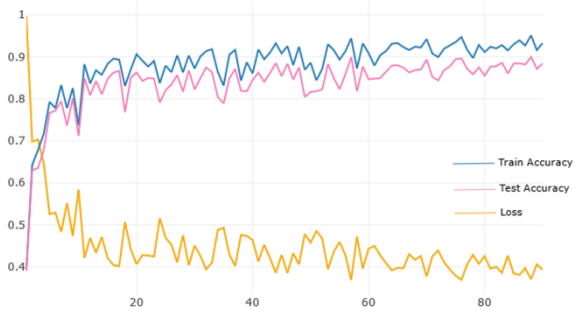


Figure 13. Training of the model after adding data augmentation

Figure 14. Figure 1 Test result

IV. CONCLUSION

The convolutional neural network applied in the SVHN dataset to improve the classic LeNet-5 network is: (1) modify the input layer to accept three-channel images; (2) switch to the more commonly used maximum pooling and Activation function, loss function; (3) introduction of gradient descent optimization algorithm RMSprop; (4) use L2 regularization. The seven-layer convolutional neural network implemented in this paper achieves direct processing of color pictures without complicated preprocessing, which improves the versatility of the model, speeds up the training and effectively avoids over-fitting. In the end, both the training speed and the prediction accuracy are better than the domestic Ma Miao and others based on the experimental results of the improved LeNet-5. After expanding the dataset, I tried to run a maximum of 170 epoch, and there was no obvious improvement in the test accuracy. Therefore, the future improvement direction should still be based on the principle. We can consider deepening the network level to obtain more abundant features.

REFERENCES

[1] Mori S, Suen C Y, Yamamoto K. Historical review of OCR research and development. Proceedings of the IEEE, 1992, 80(7): 1029-1058.

[2] Plamondon R, Srihari S N. Online and off-line handwriting recognition: a comprehensive survey. IEEE Transactions on pattern analysis and machine intelligence, 2000, 22(1): 63-84.

[3] De Campos T E, Babu B R, Varma M. Character recognition in natural images. VISAPP (2), 2009, 7.

[4] Yamaguchi T, Nakano Y, Maruyama M, et al. Digit classification on signboards for telephone number recognitio. IEEE, 2003: 359.

[5] ZHANG Shuai, SU Shi-tao. Doorplate Identification for Mobile Robot in Hallway Based on Morphological. Modern Electronics Technique, 2011, 34(14): 7-9+12.

[6] MA Li-ling. An algorithm based on ODLLTSA and SVM classier for door plate number recognition. Journal of Central South University (Science and Technology), 2011, 42: 789.

[7] ZHOU Cheng-wei. Recognition of Numbers in Natural Scene with Convolutional Neural Network.Computer Technology and Development, 2017.

Assessment of a Non-Optical Water Quality Property Using Space-based Imagery in Egyptian Coastal Lake

Hala O. Abayazid and Ahmed El-Adawy

Coastal Research Institute
National Water Research Center
Ministry of Water Resources and Irrigation

Hala Osman Moukhtar Abayazid:
e-mail: halazid@yahoo.com
address: 89 Al-Essawy street, Sidi Beshr
Alexandria-Egypt

Abstract*—Progressive anthropogenic intrusion and increasing water demand necessitate frequent water quality monitoring for sustainability management. Unlike laborious, time consuming field-based measurements, remote sensing-based water quality retrieval proved promising to overcome difficulties with temporal and spatial coverage. However, remotely estimated water quality parameters are mostly related to visibility characteristic and optically active property of water. This study presents results of an investigated approach to derive oxygen –related water quality parameter, namely Dissolved Oxygen (DO), in a shallow inland water body from satellite imagery. The approach deduces DO levels based on interrelated optical properties that dictate oxygen consumption and release in waters. Comparative analysis of multiple regression algorithms was carried out, using various combinations of parameters; namely, Turbidity, Total Suspended Solids (TSS), Chlorophyll-a, and Temperature. To cover the wide range of conditions that is experienced by Edku coastal lake, ground truth measurements covering the four seasons were used with corresponding satellite imageries. While results show successful statistically significant correlation in certain combinations considered, yet optimal results were concluded with Turbidity and natural logarithm of temperature. The algorithm model was developed with summer and fall data (R2 0.79), then validated with winter and spring data (R2 0.67). Retrieved DO concentrations highlighted the variability in pollution degree and zonation nature within that coastal lake, as related to boundary interactions and irregularity in flow dynamics within. The approach presented in this study encourages expanded applications with space-based earth observation products for exploring non-detectable water quality parameters that are interlinked with optically active properties in water.

Keywords-Remote Sensing; Algorithm Model; Coastal lake; Dissolved Oxygen

I. INTRODUCTION

Increasing demands and progressive development process have compromised sustainability potential of the coastal lakes in Egypt. The quality of water resources dictates beneficial uses offered as well as functionality of the aquatic ecosystem, especially with the alarming pollution level associated with the anthropogenic activities. Thus, continuous monitoring and frequent update of water resources status are required for sound management planning and corrective measure scenarios. However, such tasks require comprehensive data collection with adequate temporal and spatial coverage. Remote sensing is an advancing field that has the potential in reducing field work difficulties, and increasingly considered an essential planning tool.

A. Remote Sensing-based Water Quality Retrieval

Several studies in literature have addressed retrieval of water quality parameters using remote sensing techniques. Significant correlations have been found between specific water quality parameters and reflectance measured with satellite sensors. These parameters cause change to the spectral properties of reflected light and, hence, are remotely detectable (Gholizadeh et al., 2016). Recent research by Swain and Sahoo (2017) argued that certain conservative pollutants can be distinctively detected with different reflectance received in the electromagnetic spectrum because no biochemical reactions or ionic exchange are experienced.

Retrieving properties such as water clarity; turbidity, and Total Suspended Solids (TSS) concentrations

DOI: 10.21307/ijanmc-2019-059

using earth observation imageries have been tackled in applied research studies worldwide (Kloiber et al. 2002; Zhang, 2002; Bilge et al., 2003; He et al., 2008; Sravanthi et al., 2013; Dona et al., 2014; Dorji and Fearns 2016; Abayazid and El-Gamal 2017). In 2008, He et al. presented water quality retrieval models with proven successful results for optical nitrogenous and phosphorous components. Other parameters such as chlorophyll-a (chl-a) and Colored Dissolved Organic Matter (CDOM)) have also been covered in various studies (i.e. Brezonik et al., 2005; Thiemann and Kaufmann, 2000; Li et al., 2002; Dona et al., 2014).

Remotely deriving weak and/or non- optical water quality characteristics, that have no directly-detectable reflection, is challenging. Consequently, early studies are mostly focused on water physical and biogeochemical components that are considered optically active (Giardino et al., 2014). However, limitation to water quality characteristics that are related to Inherent Optical Property (IOP) narrows down the parameters that can be assessed by remote sensing techniques.

The Dissolved Oxygen (DO) concentration is considered a crucial indicator of water system healthiness, and governs recovery capability (UNESCO, 2005). Yet, being a non-optically active parameter, DO levels cannot be directly retrieved using remote sensing technique. This research study aims to present an approach to detect Dissolved Oxygen concentrations in an inland shallow coastal lake, using space-based imageries.

Based on grounds of early DO modeling theories, as well as regional conditions, the study investigates the potentiality of deducing DO levels from optically detectable water quality parameters that affect, and be affected by, Oxygen presences in water.

B. Study Area

With growing population and development activities, the Nile Delta of Egypt experience challenging conditions. Lake Edku is located within the active Northwestern coastal zone of the Delta, between longitudes 30°8' & 30°23'E and latitudes 31°10' & 31°18'N (Fig. 1). The lake is characterized of having systematically shrinking free open water, altered ecosystem and deteriorating water quality state (Abayazid, 2015). Edku lake serves an active agri-urban basin, and bordered by dense aquaculture practices. Accordingly, the lake receives wastewaters with different pollution degree from fish farming therapeutic drugs, nutrient flux from agricultural drainage network (e.g. Edku, El-Boussili, Khairy and Bearsik drains), in addition to effluents from municipal WasteWater Treatment Plants (WWTPs) and industrial facilities (Siam and Ghobrial, 2000). The lake is connected to the Mediterranean Sea with single opening "Boghaz Al-Maadia", which allows temporal tidal inflows and localized saline water interaction. Discharges with heavy nutrient levels, as well as the deceased salinity inputs, have encouraged excessive unwanted aquatic vegetation. That, in turn, disturbed natural circulation; flow dynamic and sediment transport, and hence self –purification within the lake (Hossen and Negm, 2017).

II. MATERIALS AND METHODS

This section addresses the basis of DO modeling that dictated selection process to the parameters included in this study application. Also, the ground truth data and corresponding satellite imageries considered are presented, and then followed by the approach adopted for algorithm development.

A. Theory: Grounds for DO Modeling

Modeling of Dissolved Oxygen in water bodies has been initiated in 1925 by Streeter and Phelps through an application in the Ohio River of the United States of America (Chapra, 1997). Simulation studies were based on the fact that the rate at which DO fluctuates in waters reflect the rate of Oxygen demand and release. Their modified model set foundation of DO sinks and sources through inclusion of factors proved affecting the Dissolved Oxygen depletion and recovery in a water body. Beside the initially considered coefficients that represent reaeration as well as settling/ decay processes, the model extension added representative components of aquatic flora role in the Oxygen production and exhaustion with photosynthetic activity. Furthermore, sediment consumption of DO has been added as an effective factor to be employed in the modified model for DO prediction. Equations 1 and 2 state the early model and modefied version; respectively. More details can be found in the text book of Chapra (1997)

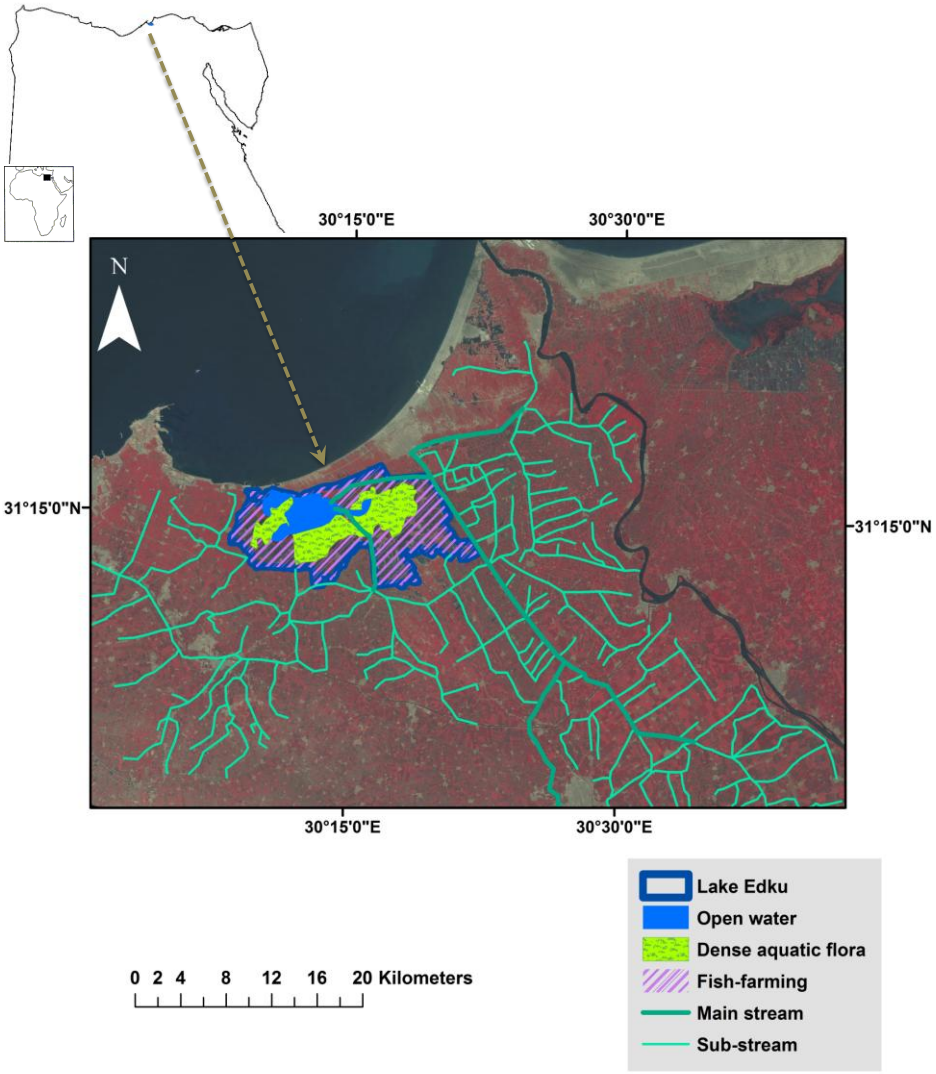


Figure 1. Edku Lake

$$\text{Dt} = \text{Do EXP}\left(-K_a t\right) + \left[\frac{K_d L_o}{K_a - K_c} \times \left\{EXP\left(-K_c t\right) - EXP\left(-K_a t\right)\right\}\right] \quad (1)$$

Where; Dt is the predicted dissolved oxygen deficit concentration, t is the travel time, L is the BOD level at point of interest, Lo is the ultimate BOD level, Ka is the reaeration rate, Kd is the decomposition rate, Ks is the settling removal rate, Kc is the CBOD decay coefficient, and Do is the initial value of the oxygen deficit.

$$D_t = \frac{K_c L_o\left(e^{-K_c t} - e^{-K_a t}\right)}{K_a - K_c} + \frac{K_n N_o\left(e^{-K_n t} - e^{-K t_a}\right)}{K_a - K_n} - \frac{P\left(1 - e^{-K_a t}\right)}{K_a} + \frac{R\left(1 - e^{-K_a t}\right)}{K_a} + \frac{S_b\left(1 - e^{-K_a t}\right)}{K_a} + D_o e^{-K_a t} \quad (2)$$

The modified model has added factors as; P the photosynthetic oxygen production rate, R the algal respiration rate, Sb the sediment oxygen demand rate, No the initial Nitrogenous BOD (NBOD), and Kn the NBOD decay coefficient.

B. Field Measurements

Ground truth data used were obtained from published research study by Okbah et al. (2017). Authors presented data collected in ten sampling locations distributed throughout the Edku Lake. Spatial distribution of field measurement locations reflects variability in the lake water quality, with regard to boundary interaction as well as flow movements within the lake (Fig. 2). Further, sampling campaigns have been carried out during four seasons; spring, summer, fall and winter of year 2016, which reflected the variable conditions that the coastal lake experince. Statistics of the field measurements show that in summer time DO levels reach the lowest concentrations, ranging from 1.6 to 9.4 mg/L, and experience wide variability within the lake with standard deviation of 3 among the ten investigated locations. Meanwhile, the highest DO levels occur in winter, ranging from11.3 to 18.1 mg/L, with standard deviation of 2.3. The lake water DO range from 7.5 to 14.0 mg/L in spring, whereas the fall season has slightly less concentrations, ranging from 5.0 to 13.1 mg/L. Maximum measured DO concentrations were mostly found in zones "C" and "D", as illustrated in figure (3). On the other hand, minimum levels occur in locations within the eastern zone "A", where most of direct wastewater discharges reach the lake water, especially in summer season.

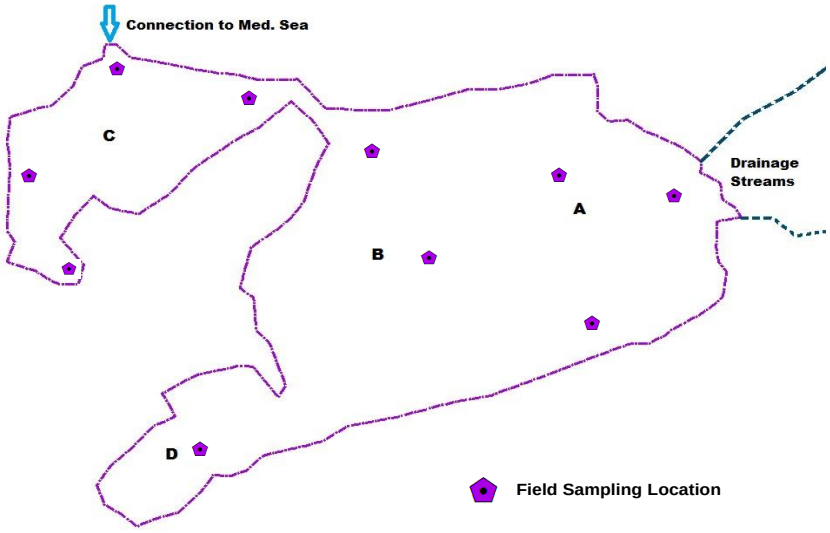


Figure 2. Field measurement locations in Lake Edku zones A, B, C, and D

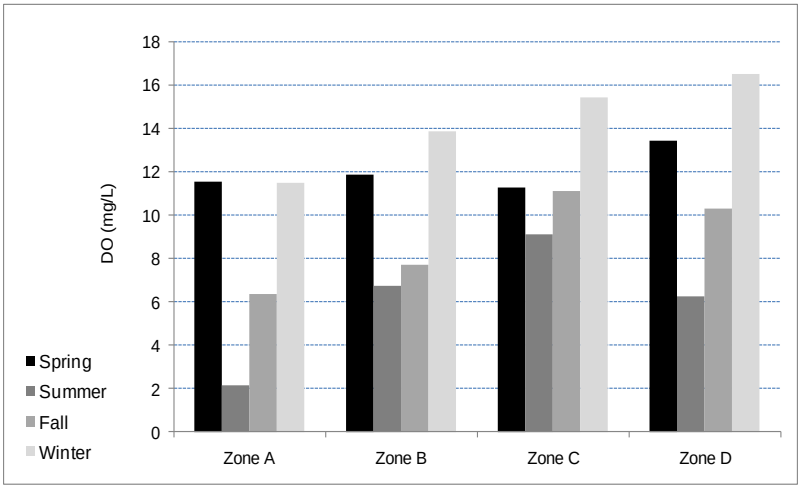


Figure 3. Observed DO data during four seasons in Lake Edku zones

C. Remote Sensing Data

In 2013, Ganoe and DeYoung presented theoretical basis for DO retrieval with the use of air-borne Raman spectroscopy instead of ship-based technology that customary required direct contact with the waterbody. Authors argued the advantages of air-based technique in measuring DO when compared to time consuming as well as limitation in detecting variability in changing water conditions during field trips. The research concluded promising success of remote sensing retrieval of the temporal and spatial dynamics of dissolved gas distributions in coastal ecosystems. Yet aerial arrangements are costly and not always readily available, while space-borne sensors can have more frequent revisits and reasonably spatial coverage with advancing spectral resolution.

The imageries used in this study are the freely available Landsat 8 Operational Land Imager (OLI) from the Unitd States Geological Survey (USGS) Earth- Explorer website. The Landsat 8 (OLI/TIRS) is the most recent satellite that was launched in 2013 under the Landsat program, with swath width of 170 km and 16 days' revisit interval. Since the in situ DO data have been collected during spring, summer, fall and winter of year 2016, images used in this study were acquired on nearest corresponding overpass dates to match the sampling data timing Table (1). Table (2) states the spectral range considered in this study, covering visible and Near-Infrared as well as Thermal Infrared bands. The necessary image processing and result analysis were carries out in Geographic Information System (GIS) environment.

TABLE I. USED LANDSAT 8 (OLI) SCENES AND DATES OF ACQUISITION

Scene ID (path177/row38)	**Date Acquired**
"LC81770382016071LGN01"	11-Mar-2016
"LC81770382016151LGN01"	30-May-2016
"LC81770382016231LGN01"	18-Aug-2016
"LC81770382016343LGN01"	8-Dec-2016

TABLE II. LANDSAT 8 (OLI) SPECTRAL BANDS CONSIDERED IN THIS STUDY

Landsat 8 (OLI) bands	**Spectral range (μm)**
Band 2 (Visible)	0.450 - 0.51
Band 3 (Visible)	0.53 - 0.59
Band 4 (Visible)	0.64 - 0.67
Band 5 (Near-Infrared)	0.85 - 0.88
Thermal Infrared Sensor (TIRS)	
Thermal Infrared (Band 10)	10.6 - 11.19
Thermal Infrared (Band 11)	11.5 - 12.51

D. Algorithm Development

Satellite imageries were processed for carrying out multiple regression technique and reaching best algoritm model for DO retrival in Lake Edku. Analysis have been performed with the spatially distributed field measurements of Dissolved Oxygen as related to the spectral reflectance values derived from Landsat images at corresponding dates in year 2016. The available field data were divided into two groups for building algorithm models. Then performance has been tested with the reserved second group of data for validation process.

Based on the previously mentioned grounds of Streeter and Phelps DO modeling, as well as regional conditions defining water quality in coastal lakes of Egypt, the trophic and sediment-related properties were

considered key factors in selection. Primary, the parameters included for developing DO derivative algorithms were Turbidity, Total Suspended Sediments (TSS), and Chlorophyll-a. Also, Temperature was added in the DO retrieval process as an important driver affecting Oxygen level in water, especially with the thermal anthropogenic releases and flow dynamic irregularity within Lake Edku. Cutomarily, DO concentration in water is inversely related to the temperature. Therefore, zonation of thermal property is expceted to have direct reflection on DO retrieved distribution. In process, alternate combinations of the considered parameters have been investigated for optimal model results.

Turbidity and TSS levels were deduced using findings of the recent research study of Abayazid and El-Gamal (2017). Authors concluded regional algorithm models for remotely sensed Turbidity and TSS in the Nile delta coastal zone, in terms of Landsat 8's reflectance from spectral bands; Band2ref, Band4ref and Band5ref, as presented in Equations 3 and 4, respectively.

$$\text{LN TURBIDITY} = -1.2247 + [0.08112\ \text{Band4ref}] + [2.944\ \text{Ln}\ (\text{Band2ref}/\text{Band4ref}] \quad (3)$$

$$\text{LN TSS} = 0.0496\ [3.325 + 13.222\ \text{Band5ref}]3.2214 \quad (4)$$

While literature applications showed various retrieval algorithms for Chlorophyll-a (e.g. Dona et al., 2014; Akbar et al., 2010; Brivio et al., 2001), best agreeable results for quantifying Chlorophyll-a in Lake Edku were found with the ratio between reflectance from spectral bands 2 and 4 of landsat 8 (Eq. 5).

$$\text{Chlorophyll-a} = \text{Band2ref}/\ \text{Band4ref} \quad (5)$$

Thermal spectral data have been converted to Temperature "T", using the conversion formula presented in Equation 6 (USGS, 2015)

$$T = \frac{K_2}{Ln\ (\frac{K_1}{L_\lambda} + 1)} \quad (6)$$

Where Lλ is the spectral radiance, and K1 and K2 are the thermal conversion constants found in Landsat imagery metadata files. Surface water temperature levels are calculated using averaged values of Thermal Infrared Bands (10) and (11).

Sensitivity analysis was performed to select best combination of the considered parameters, with different seasonal conditions experinced in the lake. Accordingly, the optimal DO retrieval algorithm model with best fitting predictions, as well as least data requirement and calculation efforts, has been selected for result demonstration.

III. RESULTS

Many factors control the DO concentration within a waterbody; both sources and sinks (e.g. consumption by flora and aerobic organisms, oxidation of carbonaceous and nitrogenous material, decomposition of organic material, photosynthetic activity, degrading inorganic chemicals, re-aeration possibility as well as temperature, and dynamics in flow. Drainage water inflowing into Lake Edku from the interconnected stream networks reflect the expanding urban activities and industrial facilities, beside the intensive agricultural processes. In addition, the aquacultural practices add an extra polluting source.

A. Remotely Sensed Input Parameters

The four parameters initially considered as inputs for DO modeling have been spatially derived for spring, summer, fall and winter seasons of year 2016, with corresponding Landsat imageries. Example illustrations are found in figures 4, 5, 6 and 7 for Temperature, Turbidity, TSS and Chlorophyll-a levels within Lake Edku, respectively.

Figure 4. Spatial distribution of derived Temperature (℃) within Lake Edku in spring, 2016

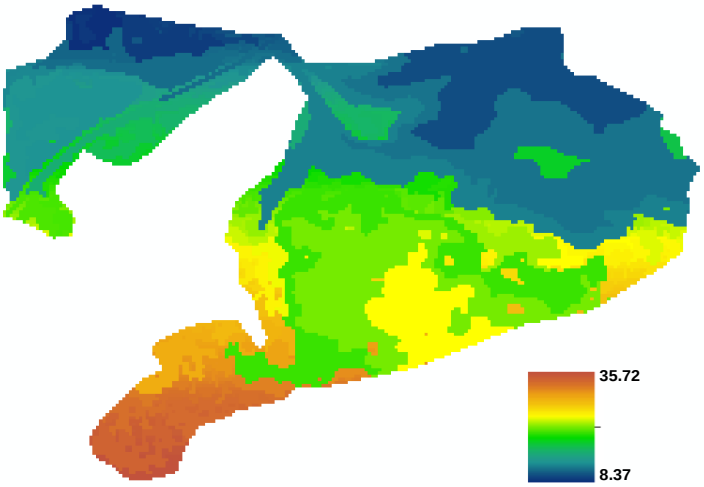


Figure 5. Spatial distribution of derived Turbidity (NTU) within Lake Edku in spring, 2016

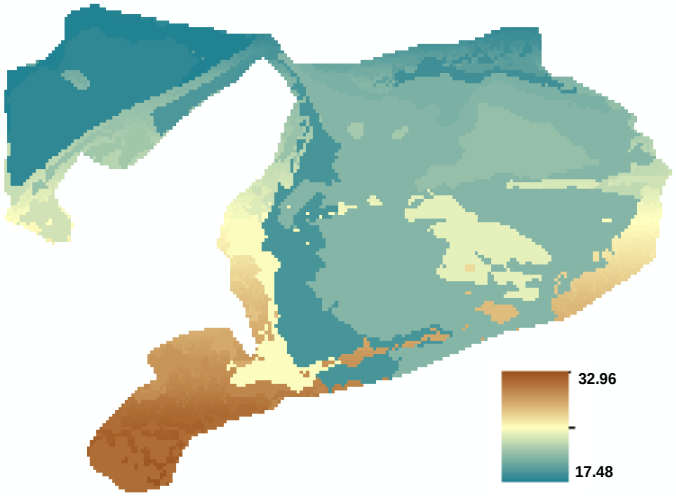


Figure 6. Spatial distribution of derived TSS (mg/L) within Lake Edku in spring, 2016

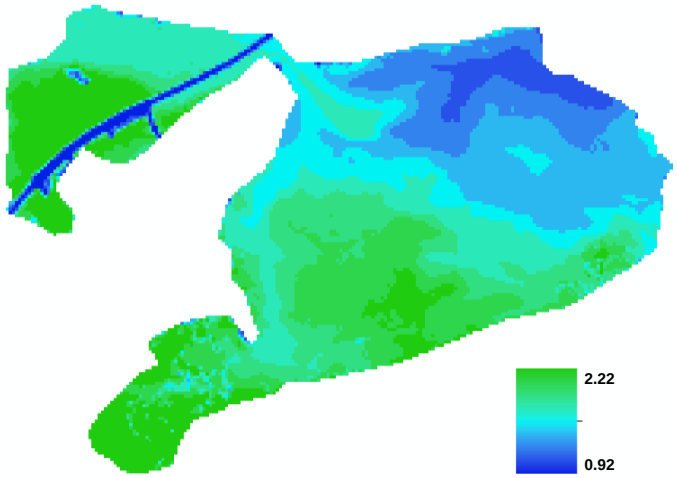


Figure 7. Spatial distribution of derived Chlorophyll-a (mg/m3) within Lake Edku in spring, 2016

B. Sensitivity Analysis

For developing satellite-based Dissolved Oxygen retrieval model, analysis has been carried out with various combinations of input parameters versus DO field measurements. The selected ground truth data is distributed throughout the lake zones. Furthermore, the data covers the four seasons so that a wide range of water quality levels experienced in the lake is considered in the developed model. Table (3) presents model predictive capacity and goodness of fitting while considering selective inputs as well as seasonal variations of DO presence in the lake waters.

Sensitivity analysis showed that TSS and Turbidity have similar effect in detecting Oxygen consumption in the waterbody under consideration. It was also found that the least influential factor is the Chlorophyll-a. Minor change with least effect in predictive capacity of the developed algorithm occurs when adding Chlorophyll-a to the input parameters.

TABLE III. SENSITIVITY ANALYSIS FOR OPTIMAL DO RETRIEVAL ALGORITHM MODEL

Seasons	Input Parameters	Regression Coefficient (R2)
Spring & Fall & Winter	Turb, TSS, Chl, Ln-temp	0.618
Summer & Fall & Winter	Turb, TSS, Chl, Ln-temp	0.630
Spring & Summer & Fall	Turb, TSS, Chl, Ln-temp	0.657
Summer & Fall	Turb, TSS, Chl, Ln-temp	0.781
Spring & Fall	Turb, TSS, Chl, Ln-temp	0.751
Spring & Winter	Turb, TSS, Chl, Ln-temp	0.651
Spring & Summer & Fall	Turb, TSS, Ln-temp	0.613
Summer & Fall & Winter	Turb, TSS, Ln-temp	0.601
Spring & Fall & Winter	Turb, TSS, Ln-temp	0.584
Spring & Fall	Turb, TSS, Chl	0.644
Spring & Fall	TSS, Chl, Ln-temp	0.676
Spring & Winter	TSS, Chl, Ln-temp	0.554
Summer & Fall	Turb, TSS, Ln-temp	0.766
Summer & Fall	Turb, Chl, Ln-temp	0.798
Summer & Fall	TSS, Ln-temp	0.756
Summer & Fall	Turb, Ln-temp	**0.792**

C. Developed Algorithm Model for DO Retrieval

Optimal derivative capacity for DO levels in Lake Edku, with least input parameter requirements, hence less processing works and costs, was found by using only Turbidity and natural logarithm of Temperature. The developed algorithm model, stated in Equation 7, proved reasonable fitness with regression coefficient of 0.79 (Fig. 8).

DO=36.27+0.19 Turbidity–10.36 Ln (Temperature) (7)

The proposed algorithm was then applied to the second group of data reserved for testing, and satellite-based derived DO concentrations were compared with the corresponding field measurements. Validation results proved acceptable predictive capacity of the developed algorithm model, with R2 of 0.66 (Fig. 9). Descriptive statistics for observed versus modeled yearly average DO levels within Lake Edku are presented in table (4). The developed model shows highly agreeable predictions with field measurements. However, the model failed to represent the very low DO concentration occurrence in the lake during summer season.

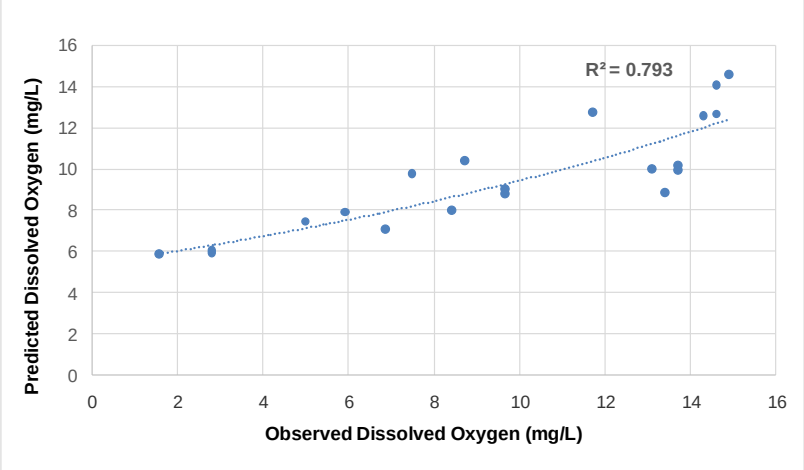


Figure 8. Predictive capacity of developed algorithm model for DO Satellite-based retrieval

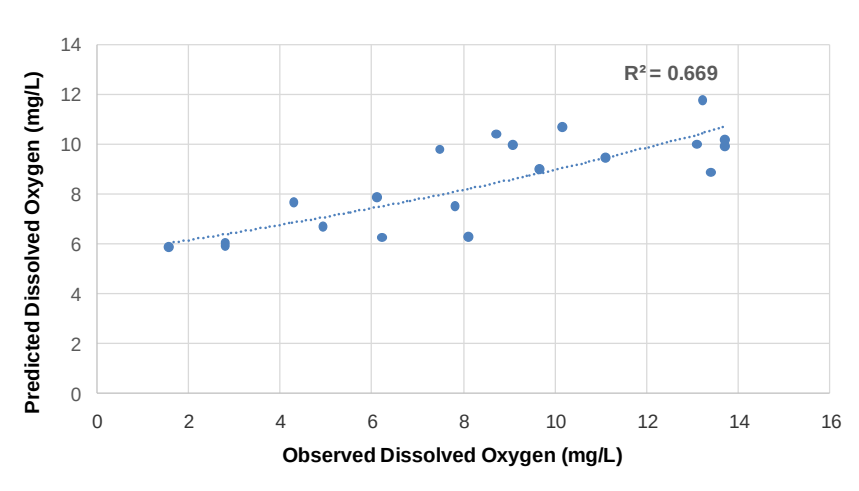


Figure 9. Validation of the developed model for DO retrieval

Once validated, the developed model has been applied to a set of landsat imageris to obtain retrieved DO spatial distribution in Lake Edku in time steps. Figure 10 illustrates comparison for observed versus derived DO concentrations during four seasons in Lake Edku. For the purpose of demonstration, figure (11) shows an example mapping of DO concentrations throughout the lake zones in winter time.

TABLE IV. DESCRIPTIVE STATISTICS FOR OBSERVED VERSUS DERIVED YEARLY DO LEVELS WITHIN LAKE EDKU

Descriptive Statistics	Do (mg/L)	
	Observed	***Modeled***
Mean	10.440	9.064
Minimum	1.560	4.552
Maximum	18.107	20.271
Standard Deviation	4.042	3.841

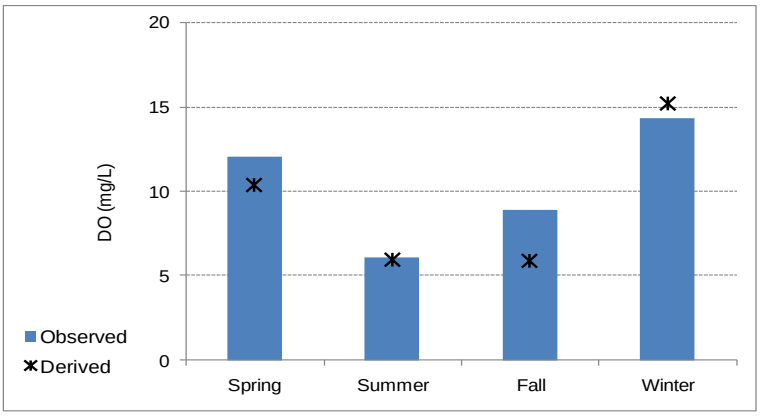


Figure 10. Observed versus derived DO concentrations during four seasons in Lake Edku

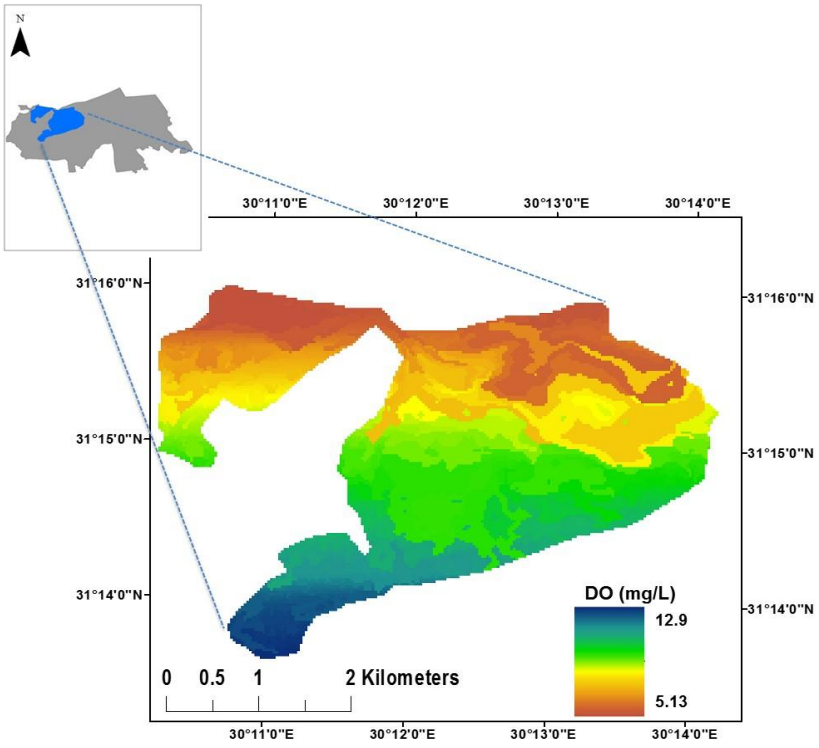


Figure 11. Retrieved DO concentrations in Lake Edku during winter season

IV. DISCUSSION

Main feature characterizes the Edku lake system is the patchy pattern of water quality. Dissolved Oxygen level ranges from less than 2 mg/L, in extremely poor water conditions, to concentrations over 15 mg/L. However, the exceedingly high DO level, with regional temperatures range of 15–30 ^{o}C in coastal lakes, is considered 150-250% supersaturation and potentially signifies an unhealthy eutrophication condition (EPA, 1999). In investigating DO concentrations with reference to location within the lake, this case is clearly demonstrated in zone D of Lake Edku.

It has been noted that there are very high DO levels, detected both in field measurements as well as derived DO concentrations, in zone D which comprise entrapped waters with rare interaction. In reviewing this condition, it was found that the area experience intensive unwarranted aquatic flora growth, and accordingly high rate of the photosynthetic oxygen production, that coincides with less active hydrodynamics and water exchange.

On the other hand, Zone A, that is the nearest to major drainage inputs into the lake, has healthier DO concentrations. This zone, while loaded with excessive pollutants, experiences inflowing water velocity along with shallow water depth that allows partial compensation with higher re-aeration rate. Moderate range of DO concentrations exists mostly in zone B, and zone C, with combined effect of low temperature and suspended sediment concentrations as well as slower flow dynamics in zone B and localized tidal effect in zone C.

V. CONCLUSIONS

Developments and consequent concerns about water resources beneficial capacity require continuous monitoring. Field-based assessment of quality state is usually faced by limitations in spatial coverage, frequency of sampling as well as possible economic and accessibility obstcles. Meanwhile, applications with remote sensing techniques have proved successful retrival of water quality parameters, yet for optically active ones that have directly-detectable spectral signals.

This research study presents an approach for deriving a non-optically active property of water quality, Dissolved Oxygen (DO), with reference to other space-based retrievable parameters that affect and be affected by DO concentrations. Derivation methodology is based on the grounds of DO modeling, as well as regional conditions that define water quality in coastal lakes of Egypt. The selected ground truth data is distributed throughout the lake zones. Furthermore, the data covers the four seasons so that a wide range of water quality levels experienced in the lake is reflected in the developed model.

The study also presents results of sensitivity analysis for alternate input combinations. Consequently, optimal DO derivative algorithm model, with best predictive capacity and least data requirement, was found. The developed optimal model comprises two satellite-based inputs, namely Turbidity and Temperature, for the Edku coastal lake. With the acceptable predictive capacity achieved, the validated model facilitates regular assessment, with more frequent DO mapping, and possible following of historical changes.

Spatial distribution of DO concentrations reflects the patchy pattern within Lake Edku, with regard to interactions in boundary as well as irregular flow dynamics within. The detected zonation nature calls for specific remedial measures that vary for each section.

Finally, remote sensing techniques proved having the potential to play more roles in monitoring processes, and offering valuable information for sustainability management. The approach illustrated in this study sheds the light at the opportunity to expand applications with space-based earth observation products. The achieved promising results open the field for exploring more non-detectable water quality parameters that are interlinked with optically active properties in water. However further applications with finer imageries and intensive ground truth data are recommended for relationship with higher accuracy.

REFERENCES

[1] Abayazid, H., 2015. Assessment of temporal and spatial alteration in coastal lakes-Egypt. In: Proceedings of the eighteenth International Water Technology Conference (IWTC 2015), Sharm El Sheikh, 12–14 Mar 2015, 598–608.

[2] Abayazid, H., El-Gamal, A., 2017. Employing remote sensing for water clarity monitoring in the Nile Delta coast. International Water Technology Journal IWTJ 7(4), 265-277.

[3] Akbar, T., Hassan, Q., Achari, G., 2010. A remote sensing based framework for predicting water quality of different source waters. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences 34, Part XXX.

[4] Bilge, F., Yazici, B., Dogeroglu, T., Ayday, C., 2003. Statistical evaluation of remotely sensed data for water quality monitoring. International Journal of Remote Sensing 24(24), 5317–5326.

[5] Brezonik, P., Menken, K.D., Bauer, M., 2005. Landsat-based remote sensing of lake water quality characteristics, including chlorophyll and colored dissolved organic matter (CDOM). Lake Reserv. Manag. 21, 373–382.

[6] Brivio, P., Giardino, C., Zilioli, E., 2001. Determination of chlorophyll concentration changes in Lake Garda using an image-based reductive transfer code for landsat TM images. International Journal of Remote Sensing 22(2), 487-502.

[7] Chapra, S.C., 1997. Surface water quality modeling. McGraw-Hill Co. Inc.

[8] Dona, C., Sánchez, J.M., Caselles, V., Domínguez, J.A., Camacho, A., 2014. Empirical relationships for monitoring water quality of lakes and reservoirs through multispectral images. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 7(5), 1632-1641.

[9] Dorji, P., Fearns, P., 2016. A quantitative comparison of Total Suspended Sediment algorithms: A case study of the last decade for MODIS and Landsat-based sensors. Remote Sens. 8, 810; doi:10.3390/rs8100810.

[10] Environmental Protection Agency (EPA), 1999. Guidance manual for compliance with the interim enhanced surface water treatment rule. United States, Environmental Protection Agency, Office of Water (4607) publishing, EPA-815- R-99-010, 201p.

[11] Ganoe, R., DeYoung, R., 2013. Remote sensing of Dissolved Oxygen and Nitrogen in water using raman spectroscopy. the NASA scientific and technical information (STI), NASA Center for AeroSpace Information, NASA/TM–2013-218142.

[12] Gholizadeh, M.H., Melesse, A.M., Reddi, L., 2016. A comprehensive review on water quality parameters estimation using remote sensing techniques. Sensors 16 (8), 1298; doi:10.3390/s16081298.

[13] Giardino, C., Bresciani, M., Stroppiana, D., Oggioni, A., Morabito, G., 2014. Optical remote sensing of lakes: an overview on Lake Maggiore. J. Limnol. 73(s1), 201-214; DOI: 10.4081/jlimnol.2014.817.

[14] He, W., Chen, S., Liu, X., Chen, J., 2008. Water quality monitoring in slightly-polluted inland water body through remote sensing - A case study in Guanting Reservoir, Beijing, China. Front. Environ. Sci. Engin. China 2(2), 163–171; DOI 10.1007/s11783-008-0027-7.

[15] Hossen, H., Negm, A., 2017. Sustainability of water bodies of Edku Lake, Northwest of Nile Delta, Egypt: RS/GIS Approach. Procedia Engineering 181, 404 – 411.

[16] Kloiber, S.M., Brezonik, P.L., Bauer, M.E, 2002. Application of Landsat imagery to regional-scale assessments of lake clarity. Water Res. (36, 4330–4340.

[17] Li, S., Wu, Q., Wang, X., 2002. Correlations between reflectance spectra and contents of Chlorophyll-a in Chaohu Lake. Journal of Lake Sciences 9 (14),228- 234.

[18] Okbah, M., Abd El-Halim, A., Abu El-Regal, M., Nassar, M., 2017. Water quality assessment of Lake Edku using physicochemical and nutrients salts, Egypt. Chemistry reseach journal 2 (4), 104-117.

[19] Siam, E., Ghobrial, M., 2000. Pollution influence on bacterial abundance and Chlorophyll-a concentration: case study at Idku Lagoon, Egypt. Scientia Marina SCI. MAR. 64 (1), 1-8.

[20] Sravanthi, N., Ramana, I.V., YunusAli, P., Ashraf, M., Ali, M.M., Narayana, A.C., 2013. An algorithm for estimating Suspended Sediment concentrations in the coastal waters of India using remotely sensed reflectance and its application to coastal environments. Int. J. Environ. Res., 7(4),841-850.

[21] Swain, R., Sahoo, B., 2017. Improving river water quality monitoring using satellite data products and a genetic algorithm processing approach. Sustainability of Water Quality and Ecology (9–10), 88–114.

[22] Thiemann, S., Kaufmann, H., 2000. Determination of Chlorophyll content and trophic state of lakes using field spectrometer and IRS-1C satellite data in the Mecklenburg Lake district - Germany. Remote Sensing of Environment 73, 227- 235.

[23] United Nations Educational, Scientific and Cultural Organization (UNESCO), 2005. water resources systems planning and management - ISBN 92-3-103998-9 – © UNESCO, 390 – 393.

[24] United States Geological Survey (USGS), Earth Resources Observation and Science (EROS) Center, 2015. LANDSAT 8 (L8) data users' handbook, Version 1.0, LSDS-1574.

[25] Zhang, Y.Z., 2002. Application of an empirical neural network to surface water quality estimation in the Gulf of Finland using combined optical data and microwave data. Remote Sensing of Environment 81(2), 327–336.

Design of a Vibration Detection Terminal

Guoshao Chen
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: 1825247141@qq.com

Fei Xu
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: xinfei2000@qq.com

***Abstract*—By detecting the vibration of bridge deck, the information of passing vehicles can be obtained indirectly, which is of great significance to grasp the dynamics of the enemy. In this paper, a micro-power wireless vibration detection terminal is designed. In order to reduce the overall power consumption of the terminal, which use two sensors, one is spring switch and another is acceleration sensor. When no vehicle passes by, the terminal is in a dormant state. When a vehicle passes by, the spring switch wakes up the CPU and the acceleration sensor to collect data. ZigBee network is used for data transmission, which has the advantages of low power consumption and ad hoc network. Experiments show that the average power consumption of the terminal is less than 7 mW. If the terminal is powered by 3.6v, 36AH lithium battery, In theory, it can work for at least two years.**

Keywords-Vibration Detection; Zigbee; Micro-power Consumption

I. INTRODUCTION

In the national defense and military affairs, the detection of passing vehicles in a specific area is of great significance for understanding each other's dynamics. The monitoring of bridge vibration can be more convenient to monitor vehicle dynamics. Considering the concealment, destructiveness and inconvenience of construction, this terminal uses wireless communication, battery power supply and micro-power design. Common wireless communication methods include Bluetooth technology, Wi-Fi technology, GPRS, ZigBee and so on. Because of the low power consumption of ZigBee network and autonomous network, this paper chooses ZigBee network.

In order to achieve low power consumption, this paper considers two aspects, one is sensor power consumption, the other is processor power consumption. There are two sensors, spring switch and acceleration sensor. If there is no vehicle passing, the system will sleep deeply to save power. When there is a vehicle passing, the spring switch will wake up the CPU and the acceleration sensor will start collecting data. With regard to processor power consumption, the terminal uses CC2530 chip for ZigBee communication. Because the chip integrates mcs51 core processors, the power consumption is reduced without additional processors. The processor Computational ability is relatively low, so the calculation of signal filtering and recognition is completed by the server. The detection terminal is responsible for signal acquisition and communication tasks.

In this paper, a micro-power vehicle vibration detection terminal is designed, which uses dual sensors to reduce power consumption, ZigBee wireless communication and battery power supply. At the same time, the communication reliability is guaranteed and the low power consumption is taken into account by waking up the communication at a fixed time. The detection terminal can meet the requirements of long-term maintenance-free work.

DOI: 10.21307/ijanmc-2019-060

II. PRINCIPLE

When vehicles pass the bridge, the vibration caused by the vehicles pass the bridge deck is violently than that pass the ground. Therefore, this paper obtains vehicle information by detecting the vibration of the bridge deck. When there is no vehicle passing, the detection terminal is in deep sleep state, CPU sleep, acceleration sensor and data memory power off, thus saving electricity. Once a vehicle passes by, the bridge vibration triggers the spring switch, wakes up the CPU, the switch opens, so the acceleration sensor starts to detect the bridge deck vibration amplitude, and the data is stored in the memory. When ZigBee network transmits data, it needs enough routing nodes to be awakened. Therefore, in order to ensure that ZigBee network works simultaneously, the terminal uses the method of periodic wake-up. During the wake-up period, data is transmitted to the server for processing and identification.

III. LOW POWER IMPLEMENTATION

In order to meet the battery power supply, maintenance-free long-term use, the terminal must reduce power consumption. This paper solves the problem of low power consumption from three aspects: hardware, communication and software.

The hardware is designed with dual sensors, low power CPU, power switch and unnecessary equipment shut down during sleep. ZigBee is used in communication, because of its advantages of ad hoc network, it can achieve low power relay transmission of data. In order to achieve low power consumption, to not lose information, on software, data acquisition using external interrupt mode, communication using timing wake-up mode.

IV. HARDWARE ARCHITECTURE

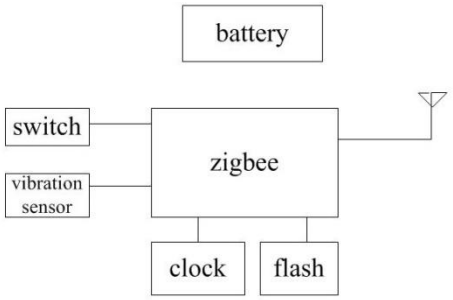


Figure 1. Hardware structure is shown

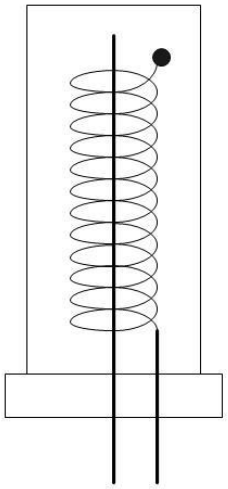


Figure 2. Switch structure

The overall hardware structure is shown in Figure 1. The spring switch is connected to the external interruption pin of the CPU. When no vehicle passes by, the spring switch breaks the power, no current passes through, and the power consumption of the spring switch is zero. When a vehicle passes by, the spring switch triggers the interruption and wakes up the CPU. The structure of the spring switch is shown in Figure 2. The center position is the wire and the surrounding is the spring. The vibration causes the short circuit between the spring and the wire, thus triggering the external interruption of the CPU. Vibration sensor adopts three-axis acceleration sensor. When the CPU is dormant, the vibration sensor is

disconnected to save power. When the CPU is awakened, the acceleration sensor is energized and starts to work. The clock is powered by a single battery using a DS1307 chip. The memory uses AT25DF641 to store the data of acceleration sensor temporarily, waiting for the arrival of the next communication cycle. The battery uses a disposable lithium battery with a capacity of 36 ah and a voltage of 3.6 v. The communication adopts ZigBee wireless mode. In order to save power, instead of increasing the CPU, the data acquisition and communication are carried out by using the 51 single chip microprocessor core integrated with cc2530. The power supply control is realized by electronic programmable switch ADG821, which can realize the maximum 150 mA current output capacity, short switching time and low power consumption.

V. OVERVIEW OF ZIGBEE NETWORK ESTABLISHMENT

Establishing a complete ZigBee mesh network consists of two steps: network initialization and node joining the network. There are two steps for a node to join the network: to connect to the network through a coordinator and to access the network through an existing parent node.

A. Initialize network coordinator

Firstly, it judges whether the node is a FFD node, and then it judges whether the FFD node has a coordinator in other networks or in other networks. Through active scanning, send a Beacon request command, and then set a scan duration . If no beacon is detected during the scan period, then FFD has no coordinator in its pos, then it can establish its own ZigBee network, and as the coordinator of this network, it generates beacons continuously and extensively. Broadcast. In a network, there is only one coordinator. Initialize network coordinators shown in Figure 3.

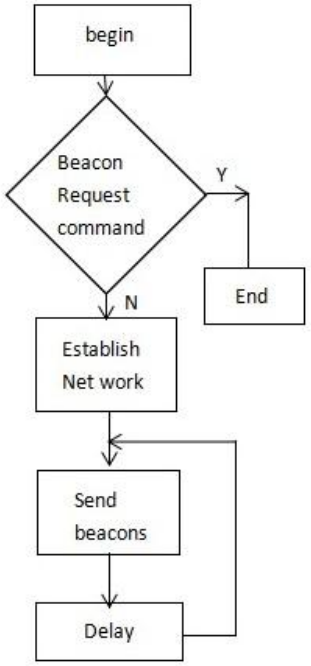


Figure 3. Initialize network coordinator

B. Channel scanning process

It includes two processes: energy scanning and active scanning. Firstly, it detects the energy of the designated channel or the default channel to avoid possible interference. Channels are sequenced incrementally to discard those channels whose energy values exceed the allowable energy level. Channels with allowable energy level are selected and labeled as available channels. Then active scanning is carried out to search the network information within the communication radius of the node. These messages are broadcast in the form of beacon frames in the network. Nodes obtain these beacon frames through active channel scanning. Then, according to these information, they find the best and relatively quiet channel. Through recording results, they select a channel, which should have the least ZigBee network, preferably without ZigBee devices. During active scanning, the MAC layer discards all frames received by the PHY layer data service except beacons.

C. Set up the network ID

When the appropriate channel is found, the coordinator will select a network identifier (PAN ID, value (= 0x3FFF) for the network. This ID must be unique in the channel used, cannot conflict with other ZigBee networks, and cannot be used as the broadcast address 0xFFFF (this address is reserved address, can not be used). PAN IDs can be obtained by listening to the IDs of other networks and selecting a non-conflicting ID, or by artificially specifying the scanning channels to determine the PAN IDs that do not conflict with other networks.

There are two address modes in ZigBee network: extended address (64 bits) and short address (16 bits), where extended address is allocated by IEEE organization for unique device identification; short address is used for device identification in local network. In a network, the short address of each device must be unique. When a node joins the network, it is allocated by its parent node and communicated by using short address. For coordinators, the short address is usually set to 0x0000.

After the above steps are completed, the ZigBee mesh network is successfully initialized, and then waiting for other nodes to join. When the node enters the network, the parent node (including the coordinator) with the strongest signal in the range of choice will join the network. After success, it will get a short address of the network and send and receive data through this address. The network topology and address will be stored in their flash.

D. Nodes join the network through Coordinator

When the node coordinator is determined, the node first needs to establish a connection with the coordinator to join the network.

In order to establish a connection, FFD nodes need to make a request to the coordinator. After receiving the connection request, the coordinator decides whether to allow the connection, and then responds to the node requesting the connection. Only when the node and the coordinator establish a connection, can the data be sent and received. The specific process of node joining the network can be divided into the following steps: Nodes join the network is shown in Figure 4.

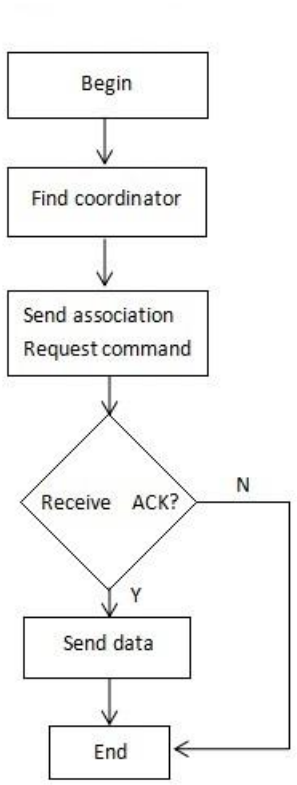


Figure 4. Nodes join the network

E. Find the network coordinator

Firstly, the coordinator of the surrounding network will be scanned actively. If the beacon is detected within the scanning period, the relevant information of the coordinator will be obtained, and then a connection request will be sent to the coordinator. After selecting the appropriate network, the upper layer will request the MAC layer to set the PIB attributes of PHY and MAC layer, such as phyCurrent Channel and macPANID. If not detected, after a period of time, the node re-initiates the scan.

F. Send the Associate Request command

The node sends the association request command to the coordinator. The coordinator replies to an acknowledgment frame (ACK) immediately after receiving it, and sends the connection instruction primitive to its upper layer to indicate that the connection request of the node has been received. This does not mean that a connection has been established, but only that the coordinator has received a connection request from the node. When the upper MAC layer of the coordinator receives the connection instruction primitive, it will decide whether to grant the join request of the node according to its own resource (storage space and energy), and then send a response to the MAC layer of the node.

G. Wait for the coordinator to process

When the node receives ACK from the coordinator to join the association request command, the node Mac will wait for a period of time to receive the coordinator's connection response. If a connection response is received within a predetermined time, it notifies its upper layer of the response. When the coordinator sends a response to the MAC layer of the node, it sets a waiting response time (T_Response WaitTIme) to wait for the coordinator to process the request command. If the coordinator has enough resources, the coordinator assigns a 16-bit short address to the node and generates a connection response command containing the new address and the successful status of the connection, then the node will succeed in building the coordinator. Vertical connection and start communication. If the coordinator resources are insufficient, the nodes to be joined will resend the request information and enter the network successfully.

H. Send data request commands

If the coordinator agrees to join the node in response time, the Associate Response command is generated and stored. When the response time is over, the node sends the data request command to the coordinator. The coordinator replies to the ACK immediately after receiving the command, and then sends the stored related response command to the node. If the coordinator hasn't decided whether to agree to join the node after the response time arrives, then the node will try to extract the related response command from the beacon frame of the coordinator. If successful, the network can be accessed successfully. Otherwise, the request information will be re-sent until the network is successfully accessed.

I. Reply

When the node receives the correlation response command, it immediately replies an ACK to the coordinator to confirm that it receives the connection response command. At this time, the node will save the short address and extended address of the coordinator, and the MLME of the node sends the connection confirmation primitive to the upper layer to notify the success of the association.

J. Nodes join the network through existing nodes

When the FFD nodes close to the coordinator are successfully associated with the coordinator, the other nodes within the scope of the network join the network with these FFD nodes as their parent nodes. There are two ways to join the network, one is through association, that is, the joining nodes initiate joining the network; the other is direct, that is, the joining nodes. The volume is added to that node as a child of that node. The association mode is the main way for new nodes to join the ZigBee network.

For a node, only if it has not joined the network can it join the network. Some of these nodes have joined the network but lost contact with their parents (such as orphan nodes), while others are new nodes. When an orphan node is an orphan node, the information of the original parent node is stored in its adjacent table, so it can send the request information of the original parent node to join the network directly. If the parent node has the ability to consent to its joining, it will enter the network successfully by directly telling its previously

assigned network address; if the number of child nodes in its original parent node's network has reached the maximum, that is to say, the parent node can not approve its joining, it can only find and join the network as a new node.

For a new node, it first scans the network it can find on one or more pre-set channels actively or passively, searches for the parent node that has the ability to authorize itself to join the network, and stores the data of the parent node that can be found in its adjacent table. Data stored in parent nodes of adjacent tables includes ZigBee protocol version, protocol stack specification, PAN ID and information that can be added. Choose one of the smallest parent nodes in the adjacent table and send a request message to it. If there are more than two parent nodes with the same minimum depth, then randomly select one to send the request. If there is no suitable parent information in the adjacent tables, it means that the access process fails and terminates. If the request is approved, then the parent node will also allocate a 16-bit network address, at which time the network entry is successful, and the child node can start communication. If the request fails, look up the adjacent table again and continue sending the request information until joining the network.

VI. SOFTWARE DESIGN

A. Introduction to Working Schedule

The software work schedule is shown in Figure 5. data is transmitted by relay mode to achieve low power consumption. Therefore, in order to transmit data, it is necessary to wake up all nodes at the same time. The communication wake-up period is T. The selection of T value is based on the size of RAM capacity, the frequency of vehicle passing and the real-time requirement of data transmission. In each cycle, once a vehicle passes by, the sensor collects data, and the CPU stores the data in RAM. After data acquisition, it enters a deep dormant state, waiting for the next vehicle to pass or the next communication wake-up cycle.

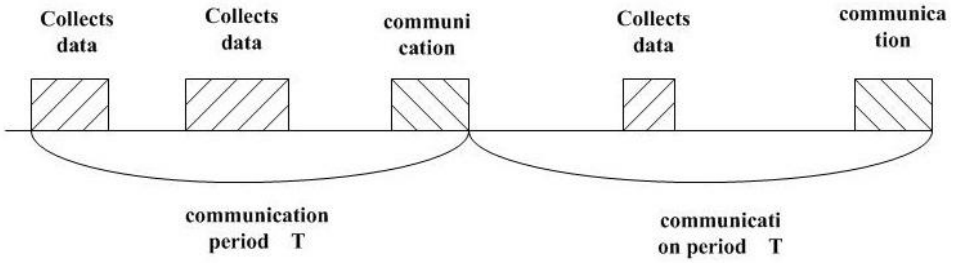


Figure 5. Software work schedule

B. Flow Chart Brief Introduction

The system software mainly consists of three parts: main function, data acquisition function and communication function.

The main function mainly completes the setting of startup parameters and entering the dormant state. Data acquisition function uses external interrupt wake-up. Communication function uses timer interrupt wake-up. The main function is relatively simple, and it is no longer necessary to elaborate. The following is a brief introduction of the two interrupt functions.

The flow chart of the data acquisition function is shown in Figure 6. When the vehicle passes by, the vibration switch is triggered and the CPU enters the external interrupt function. After external interruption wakes up the CPU, the power supply of each device is turned on through ADG821, and the data of acceleration sensor is collected, which is temporarily

stored in the data memory. The terminal collects data and keeps it until no vehicle passes by. After all the vehicles passed, the CPU turned off the power through ADG821, and the terminal went to sleep.

The communication function is shown in Figure 7. When the communication time arrives, the timer wakes up the cpu, detects the wireless signal, and waits for the central node to be ready. After Zigbee is successfully networked, each terminal uploads data in turn. If the network is idle after the transmission is completed, it will enter a dormant state. If there is no vehicle passing in the communication process, the sensor power supply need not be turned on.

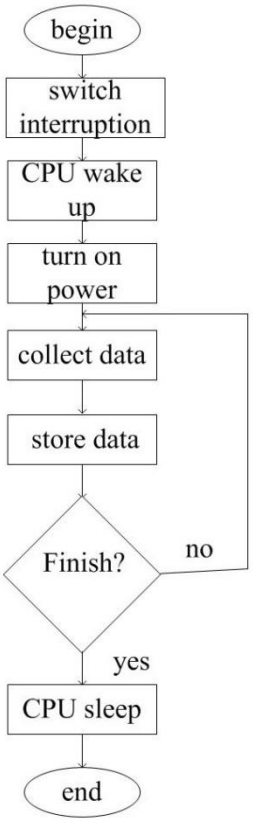


Figure 6. Data acquisition function

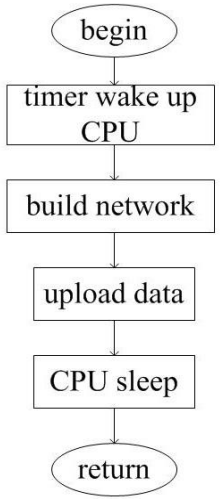


Figure 7. Communication function

VII. CONCLUSION

After the prototype is completed, it is placed outdoors for power consumption test. The outdoor ambient temperature ranges from - 5 C to 20 C, and the relative humidity ranges from 20% to 80%. In order to better simulate the vehicle and environment on site, data acquisition is carried out under the viaduct deck during the construction period. The weight and speed of construction vehicles are closer to the field vehicles than those of ordinary household cars. the average power consumption under different working conditions is: no more than 0.1 mW in dormant state, 120 mW in vehicle passing and 200 mW in communication. The average power consumption of the whole day is 162 mWH based on 30 minutes of vehicle passing time and 30 minutes of communication. The selected batteries are 36AH, 3.6V and the total power is 129.6WH. Considering the factors such as battery self-discharge, conservative estimates can work for 1000 days to meet the initial design requirements, that is, the equipment can work for at least two consecutive years. The data packet loss rate of wireless communication is less than 1%, and the failure rate of long-time equipment has not been tested yet.

This paper designs a micro-power bridge deck vibration detection terminal, which uses wireless ZigBee communication, can flexibly network, long-distance low-power transmission, and control the power consumption of hardware, so as to achieve micro-power work. Experiments show that disposable lithium batteries can work for more than two years. The detection terminal has strong concealment and simple construction, so it has good prospects in frontier monitoring and battlefield perception.

ACKNOWLEDGMENT

Fund Name: National and local joint engineering laboratory of new network and test control

Fund Number: GSYSJ2017003

REFERENCE

[1] Design of a Vibration Data Acquisition Device Yin Ming Wang Pingping Equipment Manufacturing Technology Issue 2018

[2] Design of an ultra-low power wireless vibration sensorXiuwei State Tang Shengwu Sensors and MicrosystemsVolume 35, Volume 2, 2016

[3] Vibration Detection of Ship Driving System Based on Sensor Network Feng Gang and Cai DonglingShip Science and TechnologyVolume 40, No. 12a, December 2018

[4] Design of Network Monitoring System for Oilfield Water Injection Wellblock. You Bo, Zhang Haitao, Jia Deli.Journal of Xi'an Shiyou University(Natural Science Edition), 2016, 9: vol31 no5.

[5] Research on implementation technology of ZigBee wireless communication protocol[J] . Ren Xiuli , Yu Haibin. Computer Engineering and Applications, 2007

[6] Design of oilfield wireless monitoring system based on WiFi and Zig-Bee[J]. Cao Qinghua, Liu Chang, Meng Kaiyuan. Journal of Xi'an Petroleum University (NaturalScience Edition), 2015, 30(3): 101-102.

[7] Based on ZigBee oil well remote monitoring system designand implementation[J]. Zhang Xiaohua, Zhang Wenfang, ShiRudong, et al. Control Engineering, 2013, 20

Research and Development of Millimeter Wave Technology

Bai Junying
College of InformationEngineering
North China University of Science andTechnology
Tangshan, 063000, China
e-mail: 15100586578@163.com

An Yongli*
College of InformationEngineering
North China University of Science andTechnology
Tangshan, Heibei, 063009, China
e-mail: tongxinayl@126.com

***Abstract*—This paper introduces the concept of millimeter wave, analyzes the advantages and disadvantages and propagation characteristics of millimeter wave, and expounds the research status of millimeter wave ground communication and millimeter wave satellite communication. The military application of millimeter wave communication technology in electronic countermeasures is taken as an example. Finally, the outlook for millimeter wave communication technology will open up new application fields in the future and have broad development prospects.**

Keywords-Millimeter Wave; Millimeter Wave Propagation

I. INTRODUCTION

With the rapid development of mobile communications, satellite communications, and on-board electronics, there is an increasing shortage of spectrum resources. However, users continue to put forward higher requirements on the speed, throughput and distance in wireless mobile communication, and the capacity requirements of the system are also getting higher and higher. Due to the extremely rich spectrum resources in the high-frequency microwave band, modern communication systems are developing towards high-frequency microwaves, especially in the millimeter-wave band. Millimeter wave communication has many unique features compared with traditional radio short wave, ultrashort wave and microwave communication. Since the millimeter wave is made up of microwaves and light waves (its wavelength is between the microwave and the light wave), it has some advantages of microwave and light waves. The communication device is small in size, and can be used with a small-sized antenna to obtain high directivity, which facilitates concealment and confidentiality of communication. The extremely high attenuation rate of millimeter waves propagating in wireless space is the biggest obstacle faced by millimeter wave systems in outdoor wireless communication applications. Fortunately, the millimeter wave has a small wavelength, allowing a large number of antennas to be installed without increasing the volume of the existing communication device, and the resulting large-scale antenna array can provide high beamforming gain, thereby obtaining sufficient link balance. the amount[1].

At present, Bell Labs USA has achieved significant capacity improvement and related efficiency improvements by using large-scale MIMO technology (multi-input and multi-output technology) in the millimeter wave band. With prototypes with peak transmission rates in excess of 50 Gbps, Bell Labs has successfully achieved spectral efficiencies of up to 100 bps / Hz in the 28 GHz millimeter-wave band, and its transfer rate allows users to download faster using the network, enabling only A few hundred megabytes of data transfer is reached in a few seconds. The realization of millimeter wave communication technology has provided a new development direction for future research on the realization of touchable Internet, low latency virtual reality and future applications such as 3D.

II. MILLIMETER WAVE CHARACTERISTICS

Compared with light waves, millimeter waves use the atmospheric window (millimeter waves and submillimeter waves propagate in the atmosphere, the attenuation due to the absorption of gas molecules is a small frequency, the attenuation is small), the attenuation is small, by natural light and The influence of the heat radiation source is small.

A. Advantages

1) Extremely wide bandwidth. The millimeter wave frequency range is generally considered to be 26.5 to 300 GHz, and the bandwidth is as high as 273.5 GHz. More than 10 times the total bandwidth from DC to microwave. Even considering atmospheric absorption, only four main windows can be used for propagation in the atmosphere, but the total bandwidth of the four

DOI: 10.21307/ijanmc-2019-061

windows is also up to 135 GHz, which is five times the sum of the bandwidths of the bands below the microwave. This is undoubtedly very attractive today when the frequency resources are tight.

2) The beam is narrow. The millimeter wave beam is much narrower than the microwave beam at the same antenna size. For example, a 12cm antenna has a beamwidth of 18 degrees at 9.4 GHz and a beamwidth of only 1.8 degrees at 94 GHz. It is therefore possible to distinguish small targets that are closer together or to see the details of the target more clearly.

3) Compared with lasers, the propagation of millimeter waves is much less affected by the climate and can be considered to have all-weather characteristics.

4) Millimeter wave components are much smaller in size than microwaves. Therefore, the millimeter wave system is easier to miniaturize.

B. Disadvantages

1) The attenuation in the atmosphere is severely attenuated.

2) The processing precision of the device is high.

III. MILLIMETER WAVE TRANSMISSION CHARACTERISTICS

Usually the millimeter wave band refers to 30 GHz to 300 GHz, and the corresponding wavelength is 1 mm to 10 mm. Millimeter wave communication refers to communication in which millimeter waves are used as a carrier for transmitting information. At present, most of the applied research focuses on several "atmospheric window" frequencies and three "attenuation peaks" frequencies[2][3].

A. Is a typical line of sight transmission

The millimeter wave belongs to the very high frequency band, and it propagates in space in the form of direct waves. The beam is narrow and has good directivity. On the one hand, since the millimeter wave is seriously affected by atmospheric absorption and rainfall fading, the single-hop communication distance is short; on the other hand, since the frequency band is high and the interference source is small, the propagation is stable and reliable. Therefore, millimeter wave communication is a typical communication technology with a high quality, constant parameter wireless transmission channel.

B. Has "atmospheric window" and "attenuation peak"

"Atmospheric window" refers to the 35 GHz, 45 GHz, 94 GHz, 140 GHz, and 220 GHz bands where millimeter wave propagation is less attenuated near these special frequency bands. In general, the "Atmospheric Window" band is more suitable for point-to-point communication and has been adopted by low-altitude air-to-ground missiles and ground-based radars. The attenuation near the 60 GHz, 120 GHz, and 180 GHz bands has a maximum value of about 15 dB / km or more, which is called the "attenuation peak". Often these "attenuation peak" bands are preferred by multi-channel concealed networks and systems to meet the network safety factor requirements.

C. The attenuation is severe during rainfall

Compared with microwaves, millimeter-wave signals are much more attenuated under harsh climatic conditions, especially during rainfall, which seriously affects the propagation effect. The conclusion of the study is that the attenuation of the millimeter wave signal during rainfall is closely related to the instantaneous intensity of the rainfall, the length of the distance and the shape of the raindrop. Further verification shows that: Generally, the greater the instantaneous intensity of rainfall, the farther the distance, and the larger the raindrops, the more severe the attenuation. Therefore, the most effective way to deal with rainfall attenuation is to leave enough level attenuation margin when designing a millimeter-wave communication system or communication line.

D. Strong penetration of dust and smoke

Atmospheric lasers and infrared light have poor penetrating power for dust and smoke, and millimeter waves have a clear advantage at this point. A large number of field tests have shown that millimeter waves have a strong penetrating power for dust and smoke, and can pass sand and smoke almost without attenuation. Even under the conditions of higher intensity scattering caused by explosions and metal foil strips, even if fading occurs, it is short-lived and will recover quickly. As the ions diffuse and fall, they do not cause severe disruption of millimeter wave communication.

IV. RESEARCH STATUS OF MILLIMETER WAVE COMMUNICATION

Current millimeter wave communication systems mainly include point-to-point communication on the earth and communication or broadcasting systems via satellite. Point-to-point millimeter-wave communications on Earth are now commonly used in relay communications where privacy is critical. The millimeter wave itself has strong concealment and anti-interference. At the same time, due to the attenuation of the millimeter wave in the atmosphere and the use of

a small-diameter antenna, a very narrow beam and a small side lobes can be obtained, so the interception of millimeter wave communication is obtained. And interference becomes very difficult[4].

A. Millimeter wave ground communication

The traditional application of millimeter wave terrestrial communication systems is relay (relay) communication. Numerous tests of millimeter wave propagation have shown that multi-hop millimeter wave relay (relay) communication is feasible. In order to reduce the risk, we start with the low end of the millimeter wave band and the high end of the centimeter wave band. At the same time as the development of high-band and large-capacity communication systems, medium- and low-capacity short-range millimeter-wave communication devices in higher frequency bands have also been introduced.

In the 1990s, the wave of global informationization was ushered in. With the rapid development of the Internet, the rapid growth of interactive multimedia services, broadband video services, and private network and radio communication, there is an urgent need to improve transmission rate, transmission bandwidth, and transmission quality. The demand for broadband access has become increasingly strong, and the development of various broadband access networks and devices has been promoted. Wireless broadband access technologies using millimeter waves have emerged[5].

B. Millimeter wave satellite communication

Due to the abundant frequency resources, millimeter wave communication has been rapidly developed in satellite communication. For example, in the interstellar communication, the 5mm (60GHz) band is generally used because the atmospheric loss is extremely large at this frequency, and the ground cannot detect the interstellar communication content. In the interstellar, because the atmosphere is extremely thin, it will not cause the signal to decline. The US "tactical, strategic, and relay satellite systems" is an example. The system consists of five satellites with an upstream frequency of 44 GHz, a downstream frequency of 20 GHz, a bandwidth of 2 GHz, and an interstellar communication frequency of 60 GHz.

Compared with other communication methods, the main advantages of satellite communication are: a) the communication distance is long, and the cost of establishing the station is independent of the communication distance. b) Working in a broadcast mode to facilitate multiple access. c) The communication capacity is large, and there are many types of services that can be transmitted. d) can be spontaneous, self-receiving, monitoring, etc. In the 1970s and 1980s, satellite communications were mostly carried out using geostationary orbits (also known as synchronous orbits). After the 1990s, satellite communication systems using medium and low orbits came to the fore. However, in the case of large-capacity communication services, satellite communication systems using geostationary orbit are still the protagonists. According to statistics, in the 10 years of the 1990s, as many as 200 communication satellites were launched into the synchronous orbit, with the C-band being the most and the Ku-band being the second. The resulting spectrum congestion of satellite communications has also become increasingly prominent, and the move to higher frequency bands has become an inevitable trend.

In fact, experimental research on millimeter-wave satellite communications began in the early 1970s. Most of the development work in this area is carried out in the United States, the former Soviet Union and Japan. In the late 1980s and 1990s, in addition to the introduction of the experimental satellites in the millimeter-wave band that continued to be used in a wider range and more content, the practical Ka-band satellite communication system began to appear. It should be noted that many of these satellites use a range of advanced technologies, including multi-beam antennas, on-board switching, on-board processing, and high-speed transmission.

V. MILLIMETER WAVE APPLICATION

Military needs are an important factor in promoting the development of millimeter-wave systems. At present, millimeter waves have been widely used in radar, guidance, tactical and strategic communication, electronic countermeasures, remote sensing, and radiation measurement. Among them, strategic communication and electronic countermeasures are very important application directions. Electronic confrontation refers to the electromagnetic struggle between both hostile parties using electronic equipment or equipment, and is an important means in modern warfare.

With the development of millimeter-wave radars and guidance systems, corresponding electronic countermeasures have also developed. In addition to strong firepower and high density in modern warfare, an important feature is that the entire battle is carried out in intense electronic confrontation. Therefore, communication equipment is required to have strong anti-interference ability, and millimeter wave shows a

clear advantage in this respect. For example, the selection of ship-to-ship millimeter-wave communications in the three "attenuation peak" bands of 60 GHz, 120 GHz, and 200 GHz, using the characteristics of severe attenuation of signals in these bands, can greatly improve the anti-jamming and anti-jamming of ship-to-ship communication. Interception ability. In foreign countries, the development of electronic countermeasure devices such as direction finding machines, jammers and signal analyzers in the millimeter wave band has been vigorously carried out.

The millimeter wave beam is very narrow, and the side lobes of the antenna can be made very low, making reconnaissance and active interference more difficult. Therefore, passive interference has a great development in the millimeter band. For millimeter waves below 35 GHz, the most common means of interference is to place non-resonant millimeter-wave chaffs and aerosols to scatter the enemy millimeter-wave radar beam, which can interfere with a wider frequency band without having to accurately measure the enemy radar in advance. Frequency of. In addition, it is also possible to generate plasma by explosion, thermal ionization or radioactive elements to absorb and scatter millimeter waves to interfere with enemy radar.

The frequency coverage of most radar reconnaissance and warning systems in service has been extended to 0.5 GHz to 40 GHz. According to reports, part of the radar reconnaissance equipment in the US electronic countermeasures equipment can reach 110 GHz and is developing to 300 GHz. The frequency of radar warning equipment has been extended to 40 GHz to 60 GHz. NATO is developing a vehicle-mounted millimeter-wave warning device with a frequency range of 40 GHz to 140 GHz. In addition, the communication reconnaissance band covers the 10 GHz millimeter band, and the communication interference portion below 40 GHz has been put into practical use and is developing to 110 GHz. Stealth technology can also be utilized in the millimeter band. When dealing with an active millimeter wave radar, as in the microwave band, it is possible to reduce the shape of the radar cross section or apply a millimeter wave absorbing material such as ferrite to the surface to reduce the intensity of the reflected wave. For a passive radar that tracks the target by detecting the contrast between the low millimeter wave radiation of the metal target and the background radiation, a target with a strong millimeter wave radiation is applied to make the radiation and background radiation substantially equal. Thereby merging the target into the background.

In short, millimeter-wave communication is very necessary and significant for military applications. It is a promising communication means with narrow beam, high data rate, concealed radio waves, good confidentiality and anti-interference performance, and rapid opening. Easy to use and flexible, and working around the clock. In addition to its application in the field of electronic countermeasures, the application of military millimeter wave communication includes far (outer space) near (atmosphere) distance communication, rapid emergency communication, submarine communication, satellite communication, interstellar communication, and the way down the microwave trunk line. Cable breaks the device, etc. [6]

VI. RELATED TECHNOLOGY RESEARCH

A. Millimeter wave multi-antenna system

Marconi proposed in 1908 to use MIMO technology for anti-channel fading. In the 1990s, AT&T (American Telephone & Telegraph Company) made a lot of groundbreaking work on the application of MIMO technology to communication systems. In 1995, Teladar derived the system capacity of MIMO under fading channels in the laboratory. In 1996, Foschini developed an algorithm for preprocessing signals in the MIMO channel—D-BLAST (Diagonal-BLAST) algorithm. In 1998, Wolinansky et al. used the V-BLAST (Vertical-BLAST) algorithm in the laboratory to build a MIMO system and obtained a spectrum utilization rate of 20 bps/Hz. This experiment caused great sensation in the communication industry and played a huge role in promoting the development of MIMO technology. However, as LET enters the commercial age, the demand for communication has increased year by year, and the performance of current MIMO systems cannot meet the demand for communication. Therefore, the Massive MIMO system has been proposed in recent years. Massive MIMO systems can make full use of space resources, greatly improve spectrum efficiency and power efficiency, and their system performance is greatly improved compared with MIMO systems.

Massive MIMO was first developed by Thomas L. of Bell Labs, USA. Researchers such as Marzetta suggested. Thomas L. Researchers such as Marzetta found that when the number of base station antennas tends to infinity, channel effects such as additive white Gaussian noise and Rayleigh fading are negligible, greatly increasing the data transmission rate. Massive MIMO has hundreds of antennas and even thousands

of antennas at the base end, which is 1-2 orders of magnitude higher than the number of base station antennas in the existing LTE-A, thus providing a higher transmission rate.

The main consideration is the typical Massive MIMO system, which assumes that there is an antenna at the base station and serves a single antenna user (and receives signals). The downlink system block diagram is shown in Figure 1. The received signal can be expressed as Equation 1-1:

$$y = \sqrt{\rho} HW p^{1/2} x + n \tag{1}$$

Among them, ρ is the downlink transmission power, $H \in C^{K \times N}$ is the downlink channel matrix, $CN(0,1)$ obeys the distribution, $W \in C^{N \times K}$ is the downlink precoding matrix, $p = diag(p_1, \cdots, p_k)$ is the power allocated by the base station to each user, $x \in C^{K \times 1}$ is the signal vector before precoding, $n \in C^{K \times 1}$ is additive Gaussian white noise.

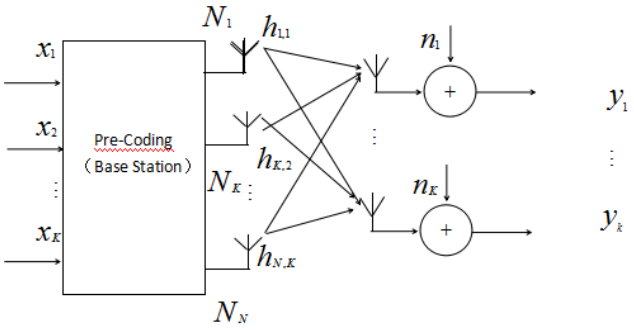


Figure 1. Block diagram of the downlink system of the millimeter wave multi-antenna system

B. Interference alignment

Interference alignment technology is an emerging method of interference management. When multiple users perform wireless communication, there will be interference between each other, and the interference will affect the signal reception quality and reduce the channel capacity of the receiver. Existing techniques for handling interference, such as frequency division multiplexing (FDMA), time division multiplexing (TDMA), and code division multiplexing (CDMA), primarily eliminate the effects of interfering signals on desired signals by orthogonalizing the signals. In fact, when multiple users share spectrum resources, this processing method can only allocate spectrum resources among K users. For example, when the number of users interacting with each other is K, the spectrum resource that each user can obtain is 1/K of a single user. Therefore, when the number of users is large, the spectrum resources available to each user are still very limited.

The interference alignment technique was proposed to solve this problem. In 2008, the system description was first given by Professor Syed A. Jafar and his student Viveck R. Cadambe. The core idea is to jointly design the transmitter precoding matrix to divide the signal space into two parts: the desired signal space and the interference signal space. The precoding technique is used to make the interference overlap at the receiving end, thereby compressing the signal capacity occupied by the interference and eliminating interference. The effect on the desired signal is achieved for the purpose of increasing the channel capacity.

Taking the implementation of spatial interference alignment as an example, the core idea of interference alignment is to limit the interference signal to a range of stator space at the receiving end. After decoding the received interference suppression matrix, the subspace where the desired signal is located and the interference signal are located. The subspaces are just orthogonal, so the desired signal is not affected by the interfering signal. In the spatial interference alignment algorithm, the transmission precoding matrix and the reception interference suppression matrix are designed according to information such as the obtained channel matrix.

VII. PROSPECT

Millimeter wave communication technology is a typical dual-use technology. In the military field, it can be applied to inter-satellite communication or relay, secret communication in the millimeter wave band, and millimeter wave enemy and foe identification system; in the civilian field, it can be applied to broadband multimedia mobile communication systems, measurement radar, vehicle and ship collision avoidance, topographic mapping. , radio astronomy, interactive large-capacity television broadcasting and satellite millimeter wave link system and many other aspects, and will further expand its market. In short, a large amount of research work has been carried out in the field of domestic and foreign millimeter wave communication, covering everything from basic communication theory to practical system application, which fully demonstrates that millimeter wave communication is a promising wireless communication technology.

ACKNOWLEDGMENT

National key research and development plan project (2017YFE0135700)

Hebei Provincial Department of Education Science and Technology Project (QN2017114)

Hebei Provincial Natural Science Foundation (A2015209040)

North China University of Technology Doctoral Research Start-up Grant Project.

REFERENCES

[1] Meng Qingqi. Application and Development of Millimeter Wave Communication[J]. Microwave and Satellite Communications, 1996, (02): 20-23.

[2] Li Yanli. Research Status and Development of Millimeter Wave Communication Technology [A]. Sichuan Communication Society. Proceedings of 2010 Annual Conference of Sichuan Communication Society [C]. Sichuan Communication Society:, 2010: 4.

[3] Wang Xiaohai. Development and Application of Millimeter Wave Communication Technology [J]. Telecom Express, 2007, (10): 19-21.

[4] Zou Weixia, Du Guanglong, Li Bin et al. A new beam search algorithm in 60GHz millimeter wave communication. Journal of Electronics and Information, 2012

[5] Zhang Wei, Li Bin, Liu Yun, Zhao Chenglin. Research on uplink hybrid beamforming technology in 60 GHz millimeter wave communication. Journal of Electronics and Information, 2012

[6] Wu Zhengde. Development of China's millimeter wave technology. Journal of University of Electronic Science and Technology of China, 1991 (6)

Comparative Research on Key Technologies from IPv4, IPv6 to IPV9

Sun Huai
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China
e-mail: sh1227467868@163.com

Liu Zhang
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China
e-mail: 604463203@qq.com

***Abstract*—Since the United States developed the IPv4 protocol based on TCP/IP in the 1970s, it has been more than 30 years old. IPv4 is the "fourth edition of the Internet Protocol." From a technical point of view, although IPv4 has a brilliant performance in the past, it seems to have revealed many drawbacks. With the addition of multimedia data streams and security considerations, IPv4's address space is running out of crisis, and IPv4 is no longer sufficient. Under such circumstances, IPv6 was born as needed. When designing IPv6, not only the IPv4 address space was expanded, but also the parties to the original IPv4 protocol were reconsidered and a lot of improvements were made. In addition to the large number of addresses, there is higher security, better manageability, and better support for QoS and multicast technologies. It is an abbreviation for "6th Edition of Internet Protocol." IPV9 was proposed in 1992 to replace the IPv4 with the ISO/OSI CLNP protocol, using the 20B NSAP address and the platform for the available OSI transport protocol. Later, DDNS was introduced and gradually developed into an IPV9 decimal network with a 256-bit address. IPV9 masters "the right to control the use of the Internet, the allocation of IP addresses, the initiative of information monitoring, the right to use routing protocols, and the ownership of technology patents." Therefore, the research and application of a new generation of Internet Protocol Next Generation has become a worldwide hotspot.**

Keywords-IPv4; IPv6; IPV9

I. INTRODUCTION

Internet Protocol (IP) is a communication protocol designed for computers to communicate with each other in the network. IP provides a common rule for computers to access the Internet. The Internet has become the largest open network in the world. With the rapid development of the global economy, the advancement of communication technology and network technology, the penetration rate of computers and mobile terminals is getting higher and higher. The problems with IPv4 are also exposed [1]. For example, in the address space, performance, network security and routing bottlenecks, IPv4 makes it difficult to meet the needs of the Internet in the future. To solve the IPv4 many problems, IPv6, IPV9 and other Internet protocols have been born.

II. THE STATUS OF IPV4

IPv4 plays a key role in the development of the network. However, with the continuous expansion of the network scale, it can no longer meet the network development needs. Firstly, the address resources are exhausted, which directly leads to the address crisis, although the CIDR technology is not classified. The network address translation NAT technology alleviated the address crisis, but still cannot solve the problem. Secondly, the routing table expansion problem, the topology structure of the address space directly causes

DOI: 10.21307/ijanmc-2019-062

the address allocation form to be independent of the network topology. As the number of networks and routers increases, the excessively expanded routing table increases the lookup and storage overhead and becomes the bottleneck of the Internet. At the same time, the length of the packet header is not fixed, and it is very inconvenient to use hardware to implement path extraction, analysis and selection, so it is difficult to improve the routing data throughput rate. There is also an uneven distribution of IP addresses. Since most of the addresses are from the United States, most of the addresses are in the United States, resulting in a serious imbalance in IP address allocation.

There is also a lack of QoS (Quality of Service) support. The design does not introduce the QoS concept. The original intention is for the military. It does not want to be open to the outside world. Therefore, it is lacking in quality of service QoS and security. It is difficult to be real-time. Commercial services such as multimedia and mobile IP provide rich QoS functions. Although protocols such as RSVP have been developed to provide QoS support, the cost of planning and constructing IP networks is relatively high.

III. THE CHARACTERISTICS OF IPV6

The IPv4 protocol is currently widely deployed Internet protocols. The IPv4 protocol is simple, easy to implement, and interoperable. However, with the rapid development of the Internet, the shortage of IPv4 design is becoming more and more obvious. The number of IPv4 address spaces is insufficient and the number of routing table entries to be maintained is too large[2]. Compared with IPv4, IPv6 has the following characteristics.

1) IPv6 has a larger address space. IPv4 specified IP address length is 32 bits, there are 2^32-1 addresses, and IPv6 the IP address length is 128 bits, there are 2^ 128-1 addresses. Compared to the 32 -bit address space, its address space is greatly increased.

2) IPv6 uses a smaller routing table. The IPv6 address allocation follows the principle of aggregation (Aggregation) at the beginning, which enables the router to use a record (Entry) to represent a subnet in the routing table, which greatly reduces the length of the routing table in the router and improves router forwarding. The speed of the packet.

3) IPv6 adds enhanced multicast (Multicast) support and the support of convection(Flow Control), which makes multimedia applications on the network has made great development opportunity for quality of service(QoS , at Quality of Service) provides control Good network platform.

4) IPv6 has added support for Auto Configuration. This is an improvement and extension of the DHCP protocol, making network management more convenient and faster.

5) Better header format. IPV6 uses a new header format with options that are separate from the base header and can be inserted between the base header and the upper layer data if needed. This simplifies and speeds up the routing process because most of the options do not need to be routed.

Although IPv6 has obvious advantages, the number of IPv4 routers is huge. The transition from IPv4 to IPv6 is a gradual process, and IPv6 must have backward compatibility. Therefore, the coexistence of IPv6 and IPv4 will coexist for a long time. Moreover, IPv6 has great drawbacks in the design of its address structure. IPv6 confuses the network hierarchy in design. The interface ID embeds the address of the physical layer into the logical address layer. In this respect, the space of the physical address forms a restriction on the IP address space, and the security does not belong to the IP layer. Designing security technologies at the IP layer should not be. Because with the development of security technology, the security method and key length will continue to change, so the development of security technology will eventually lead to the redesign of IP addresses. Due to

the chaos of network-level logical relationships, IPv6 creates far more new problems than it solves.

IV. DEFINITION OF IPV9

The new IPV9 network covers three new technologies: address coding design, new addressing mechanism and new address architecture design. It aims to build a core technology system based on the underlying IP network. On this basis, a new framework can be formed. Connected and compatible with a network system that covers existing networks (Internet with IPv4 and IPv6 technologies). 2011 US government agency has the authority of the professional and technical confirmation from the law, my country has IP framework with the United States Internet network to the prior art, proprietary technology core network sovereignty[3]. This is the patented technology of IPV9 (Method of using whole digital code to assign address for computer). The official patent name is "the method of allocating addresses to computers using full digital coding".

The IPV9 protocol refers to the 0-9 Arabic digital network as the virtual IP address, and uses decimal as the text representation method, which is a convenient way to find online users. In order to improve efficiency and facilitate end users, some of the addresses can be directly used for domain name. At the same time, it is also called "new generation security and reliable information integrated network protocol". It uses the classification and coding of the original computer network, cable radio and television network and telecommunication network.

V. THE ARCHITECTURE OF IPV9

By using IPV9 routers, clients, protocol conversion routers and other devices to build a pure IPV9 network, IPV9/IPv4 hybrid network to achieve a new generation of Internet systems with independent and secure intellectual property rights. Including the domestically controllable IPV9 future network root domain name system, promote technology convergence, service integration, data convergence, and achieve cross-level, cross-regional, cross-system, cross-department, cross-business collaborative management and services. With the data concentration and sharing as the way, we will build a national integrated national big data center, accelerate the promotion of domestically-controlled independent control alternative plans, and build a safe and controllable information technology system. Separate from the control of the US domain name system and realize the independent domain name system. In order to speed up the promotion of China's international discourse rights and rules-making rights to cyberspace, we will make unremitting efforts towards building a network-strengthening country.

In the existing TCP/IP protocol, conventional packet switching cannot support true real-time applications and circuit switching, and supports applications such as transmitting sound or images in circuits in a four-layer protocol. With the demand for voice, image and data triple play, the incompatibility of human-machine interface and the environmental protection requirements for redundant links, especially the original security mechanism is unreasonable, it is imperative to establish a new network theory foundation. So in 2001, China established the Decimal Network Standard Working Group (also known as IPV9 Working Group) to study and implement security-based first-come-authentication communication rules, address encryption, as short as 16 bits up to 2048 bits of address space, resource reservation, virtual real circuit The communication network transmission mode, such as character direct addressing and three-layer four-layer hybrid network architecture, was first proposed by China and has formed a demonstration project.

The existing TCP/IP protocol is a connectionless, unreliable packet protocol with a maximum packet length of 1514 bytes. The TCP/IP/M protocol of IPV9, which is led by China, not only inherits the connectionless and unreliable packet protocol of the

existing TCP/IP protocol, but also develops absolute code stream and long stream code. The data packet can reach tens of megabytes or more. After three can be transmitted directly by telephone and cable television data link is established without affecting the existing transmission network until four transmission new transmission theory until they have finished the removal of three of four transport protocol.

And continue to develop and develop and manufacture the ISO-based future network "naming and addressing" and "safety" led by China. Such as:

1) Based on three / new four-core network architecture of PC desktops and mobile phone network Operating system kernel.

2) An instruction set of a new kernel based on a three-layer / four-layer network architecture network operating system.

3) A chip based on a new core of a three-layer / four-layer network operating system architecture.

4) The IPV9 block domain of the new kernel based on the three-layer / four-layer network operating system architecture.

5) New operating network for optical switching and router based on network operating system.

6) Research and development based on the header encryption system for communication after verification and IPV9 based mobile phone and industrial control.

VI. THE ADVANTAGE OF IPV9

Compared with the traditional IPv4 and IPv6, the changes of IPV9 mainly include the following aspects. IPV9 has a larger address space than IPv4 and IPv6. The address length of IPv4 is 32 bits, that is, there are 2^32-1 addresses. The address length of IPv6 is 128 bits, that is, there are 2^128-1 addresses. But IPV9 increases the address capacity to 256 bits, that is, there are 2^ 256-1 addresses. In mobile communications, the biggest drawback of IPv4 is that there are not enough addresses available for mobile devices that people use. If IPv6 is widely used, the problem of IP shortages around the world will be solved.

B. Digital Domain Name System

In the digital domain name system, IPv4 and IPv6 are domain name resolutions through the United States, while IPV9 is set by countries, which avoids the limitation of IP addresses and reduces the use of domain names by the state. IPV9 is a "decimal network" with independent intellectual property rights developed according to the invention patent "Method of Allocating Addresses for Computers Using All Digital Encoding". Its decimal network introduces a digital domain name system, which can be used to convert the original binary through a decimal network. The address is converted into decimal text, allowing the computers on the network to connect to each other, to communicate and transmit data to each other, and to be compatible with Chinese and English domain names.

The digital domain name technology used by the IPV9 decimal network reduces the difficulty of network management, the vast address space and the newly added security mechanism, and solves many problems faced by the existing IPv4 [4]. The advantages of other aspects can also meet the different levels of demand for various devices in the future.

C. Routing

In terms of routing, the increase in the size of the Internet has caused the IPv4 routing table to swell, making the efficiency of network routing declining. The emergence of IPV9 solves this problem, and the optimization of routing improves the efficiency of the network. IPV9 establishes an IPV9 tunnel between the mobile unit and the proxy , and then relays the data packet sent to the mobile unit's home address received by the “proxy” used as the mobile unit to the current location of the mobile unit through the tunnel, thereby implementing Network terminal mobility support.

The IPv6 routing table is smaller than IPv4. IPv6 address allocation follows the principle of aggregation, which enables the router to use a record to represent a subnet in the table, which greatly reduces the length of the routing table in the router and improves the routing table forwarding[5]. IPV9's routing table is very small. IPV9's address allocation follows the principle of geospatial clustering. This allows a record in the IPV9 router to represent a country subnet and an application subnet, greatly reducing the routing in the router. The length and cleanliness of the table increases the speed at which the routing table forwards packets. At the same time, this subnet can express a specific geographical location. According to this logic, only one route is needed between the country and the country. For example, the route to China is 86/64. The IPv4 routing table is extremely large and irregular. The IPv6 routing table is smaller than IPv4, but the IPv6 routing table does not contain geographic information and the routing is cluttered.

D. Security

IPV9 encryption technology and authentication technology have significantly improved than IPv4, and the encryption technology proposed by IPV9 is difficult to decipher at the physical level, and the confidential performance has been significantly improved. However, at the level of network information security, there are still many factors that cause insecure network information in China. The fundamental reason is that the root servers of IPv4 and IPv6 are in the United States. Many patents related to the network are in the hands of the United States. At the same time, the risk of information exposure may also be introduced. The IPV9 is to have independent intellectual property rights of Internet Protocol, can bring a lot of protection to the information security of the country. IPV9's address space enables end-to-end secure transmission, making it possible for people to use devices to directly assign addresses[6]. Both IPv4 and IPv6 do not have the concept of national geographic location. Most of their domain name resolution servers are in the United States, and IPV9 proposes the concept of "sovereign equality", which enables each country to have its own root domain name system, which guarantees that all countries are on the Internet.

VII. APPLICATION RESEARCH OF IPV9 SYSTEM

We designed the following 10 test scenarios to fully reflect the features and advantages of the IPV9 network system. Covers some functions of the IPV9 network system, and the test case selects several typical scenarios for testing.

A. Application 1—Pure the IPV9 Network Architecture

This application implements a pure IPV9 network architecture. The simplest system includes IPV9 client / server A, IPV9 client / server B, 10G IPV9 Routers C, D. The network topology is shown in Figure 1.

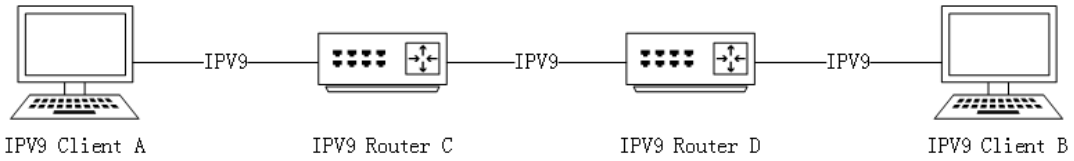


Figure 1. Pure IPV9 client - server test topology

The pure IPV9 client - server scenario is suitable for building a pure IPV9 network in an area, which is suitable for establishing an independent IPV9 network system.

B. Application 2—IPv4 network by purely the IPV9 connected to the network

This application implements IPv4 network applications through pure IPV9 network communication. The simplest system includes IPv4 client / server A, IPv4 client / server B, IPV9 10G router C, D. The network topology is shown in Figure 2.

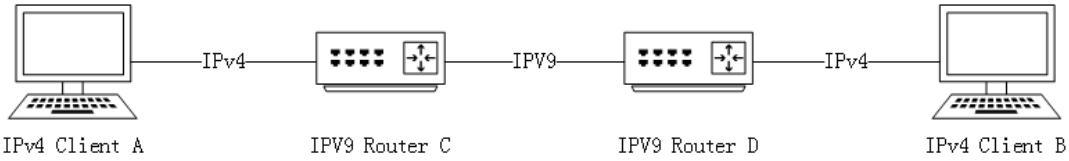


Figure 2. The IPv4 network by purely the IPV9 connected to the test network topology

This scenario is applicable to IPv4 networks in several different areas connected through the IPV9 core network to implement penetration access between different IPv4 networks. One of the main features is that in addition to the existing IPv4 network, other areas use IPV9 protocol transmission, which requires special network connections (such as fiber, DDN line, etc.) between different IPv4 networks.

C. Application 3—IPv4 network through 9over4 connection tunnel

This application implements IPv4 network through 9over4 tunnel communication, the simplest system comprising an IPv4 client / server A, IPv4 client / server B, the IPV9 1OG routers C, D. The biggest difference between scenario 3 and scenario 2 is that the IPv4 public network address between routers C and D is based on 9over4 tunnel communication. This scenario simulates the IPV9 network using the existing IPv4 public network to achieve IPV9 network connectivity in different geographic regions under the current conditions, and has the ability to build a national network. The network topology is shown in Figure 3.

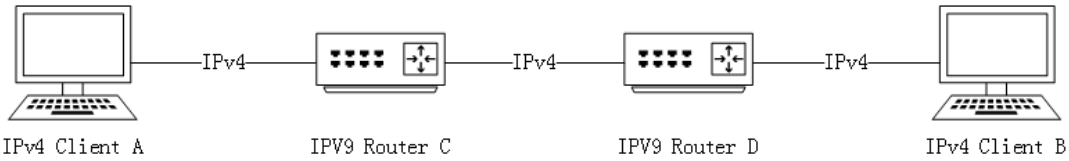


Figure 3. The IPv4 network through 9over4 connection topology tunnel test

IPv4 networks in different areas are connected through the IPV9 over IPv4 core network to achieve transparent access between different IPv4 networks. A major feature is the use of existing IPv4 networks between core networks, communicating via 9over4 tunnel mode. You can use the existing IPv4 public network to quickly establish connections between different regional IPv4 networks and implement penetration access.

D. Application 4—The IPV9 network via 9over4 tunnel connection

This application implements the IPV9 network applications by 9over4 tunnel communication, the simplest system comprising the IPV9 client / server A, the IPV9 client / server B, the IPV9 1OG routers C, D. The biggest difference between this scenario 4 and scenario 1 is that the IPv4 public network address between routers C and D is based on 9over4 tunnel

communication. This scenario simulates the IPV9 network using the existing IPv4 public network to achieve IPV9 network connectivity in different geographic regions under the current conditions, and has the ability to build a national network. The network topology is shown in Figure 4.

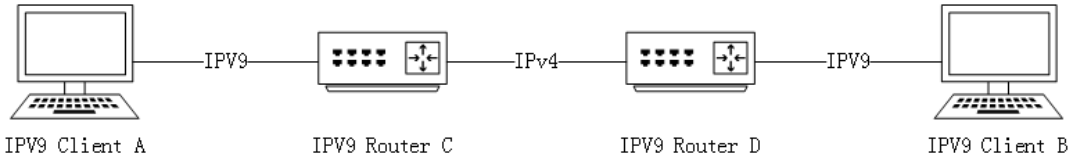


Figure 4. The IPv4 network through 9over4 connection topology tunnel test

The application implements the IPV9 network islands of N scenarios 1 to be connected through the IPV9 over IPv4 core network to implement penetration access between different IPV9 networks. A major feature is the use of existing IPv4 networks between core networks, communicating via 9over4 tunnel mode. Can use existing IPv4 quick connect different regions of the public network the IPV9 network, and access to achieve penetration.

E. Application 5—hybrid network architecture

In this application, the client side of the IPV9 access router accesses the IPv4 network at the same time, the IPV9 network, and the network side of multiple IPV9 access routers access the user side of the same core router, and the network side of the core router Simultaneous access to IPV9 networks and IPv4 networks (including public networks). Can be achieved (1) IPv4 clients penetrate the network access to other subnets IPv4 clients. (2) IPv4 client normal access to the Internet. (3) IPV9 clients to access other autonomous domain of IPV9 clients. (4) Between the access routers using the OSPFV9 dynamic router protocol networking. (5) The IPV9 core routers can choose to use the 9over4 network to access the Shanghai node IPV9 network, or use the pure IPV9 protocol to access the Beijing node IPV9 network. The network topology is shown in Figure5.

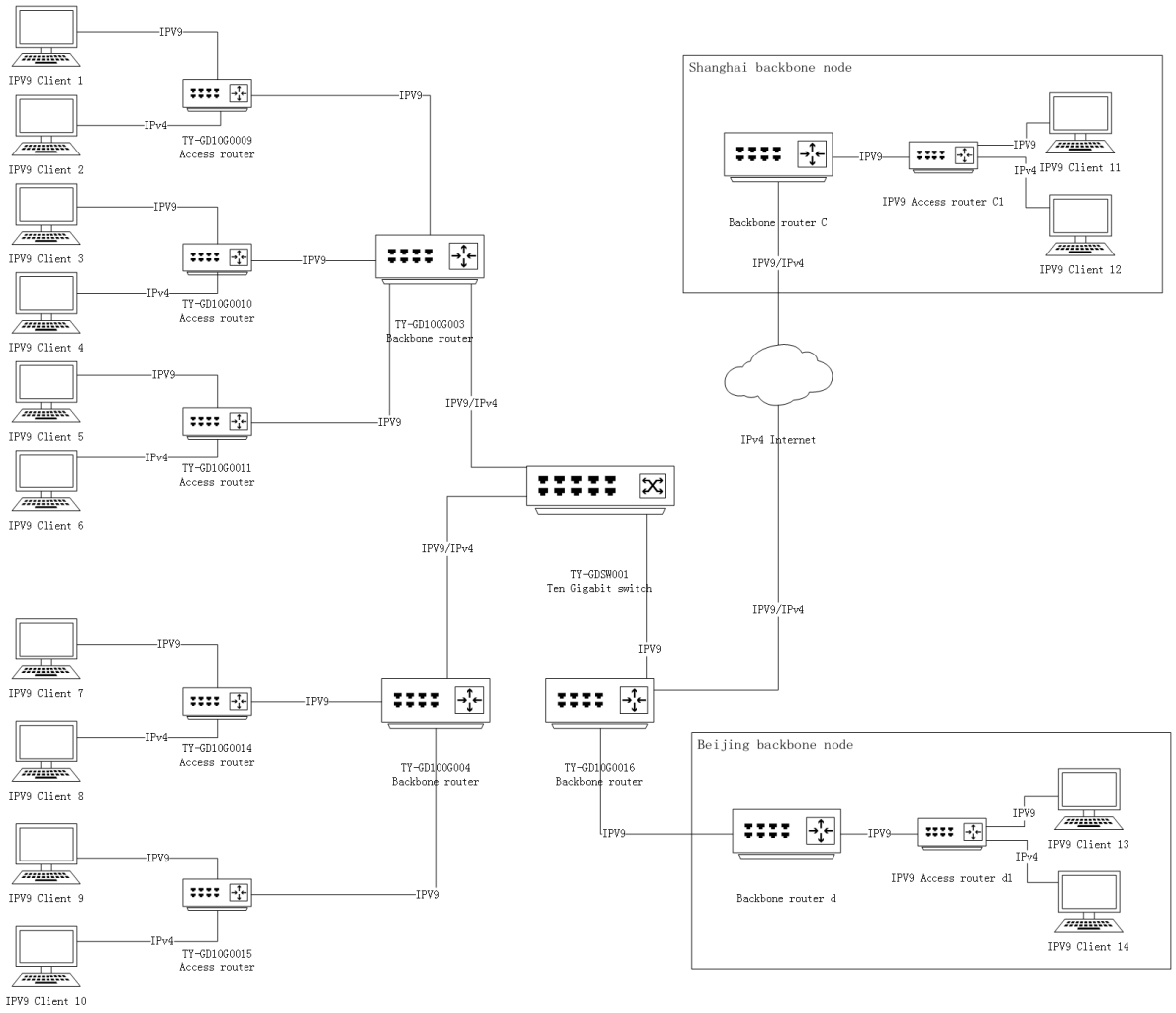


Figure 5. The IPV9 hybrid network topology architecture test

This application scenario is mainly used to build an IPV9 network environment, seamlessly integrate IPv4 networks, and IPV9 networks. All IPv4, IPV9 network islands are connected using the IPV9 protocol or the existing IPv4 public network. It is convenient and quick to connect independent networks in different regions to form a national unified network by using the IPV9 network system.

VIII. DEVELOPMENT AND OBSTACLES

Whether transitioning from IPv4 to IPv6 or evolving to IPV9 is a gradual process, it is necessary to maintain mature services based on IPv4 and support interoperability between new and old protocols.

Net network only charge network access fees, mainstream technology not well supported by successful business models, which is IPV9 of fatal weakness. IPv6 is supported by governments and vendors around the world. IPV9 supporter limited, difficult to scale and provide good service in the short term, relying on China's own development, it is difficult to fight IPv6 research network externalities and spend a huge human and financial resources have formed the results. It is difficult through the inlet into commercial use the network market to form economies of scale and reduce costs.

IX. CONCLUSION

With the development of the Internet, the number of Internet users is increasing, and the lack of IPv4 address resources has become a bottleneck restricting its development. Regardless of the evolution from IPv4 to IPv6 or to IPV9, IPv4-based mature services are required to support protocol compatibility. IPV9 absorbs a large number of advanced design concepts and technologies at home and abroad in the design and development process. It is a secure and controllable network information platform that can be compatible with the current IPv4 and IPv6 Internet, and can operate independently. It is suitable for establishment. National government, banks and other private networks. The IPV9 network has established a digital domain name resolution center in Shanghai, and has established sub-centers in Beijing, Changsha, and Macao, and is operating normally. In military networks and some government networks, IPV9 may gain a place from the perspective of national security. Regardless of future trends, providing a safe, efficient, stable and reliable network environment is our common goal.

REFERENCE

[1] Xie Jianping etc. Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[2] Zang Qianli etc. A Survey on IPv6 Address Structure Standardization Researches [J]. Chinese Journal of Computers. 2019: 1-23 [2019-03-04].

[3] Xie Jianping etc. A method of assigning addresses to network computers using the full decimal algorithm [P]. CN: ZL00135182.6, 2004.2.6.

[4] V. Fuller, T. Li,Network Working Group. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy, RFC-1519, 1993.9.

[5] Kohler E, Li J, Paxson V, et al. Observed Structure of Addresses in IP Traffic [J]. IEEE/ACM Transactions on Networking, 2006, 14(6):1207-1218.

[6] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.

Cyber Security Cookbook for Practitioners

Devesh Mishra
Technologist – Mount Sinai Health System, NY
New Jersey, USA
e-mail: dkm2144@columbia.edu

***Abstract*—The scope of this paper is to provide the essential framework to C-suite/Management executives in the case of cyber events. This paper will further analyze the various threat vectors from the operational perspective and provide the remediation plan during the case of cyber-attacks.**

Keywords-Component; (CIO; CISO; CFO; Risk Management)

I. GENERAL OVERVIEW

Organizations prepare for various types of emergencies by developing a disaster recovery plan to cover flood, fire, earthquakes, and other unforeseen events that may disrupt their operations. It is important to protect the organization's assets against cyber threats and having a robust playbook as well. According to IBM's CEO, "Cyber Crime Is the Greatest Threat to Every Company in the World"1. Darkreading.com states, "Global cost of cybercrime predicted to hit $6 trillion annually by 2021"2.

Cybersecurity should be an integral part of corporate strategy. As Touhill advises, the cybersecurity plan focuses on the following (Touhill & Touhill, 2014, as of Page 97):

- Where are we now?
  - SWOT analysis
- What do we have to work with?
  - Information
  - Technology
  - Finances
  - Personnel
  - Plans
- Where do we want to be?
  - Value
  - Risk Management
  - Effectiveness
  - Competencies
- How do we get there?
  - What will be done?
  - Who is responsible for doing it?
  - How will it be done?
  - What resources are required?
  - Risk Management
  - Measuring progress and success

The basic security principles of Least Privilege, Defense in Depth, and Separation of Duties are observed. These concepts will drive many of the security design decisions, just like Confidentiality, Integrity, Availability, and Accountability will inform the requirements for controls to mitigate specific risks. (Wheeler, 2011, Page 19).

II. ENTERPRISE RISK MANAGEMENT

Risk Management is defined as "the function of determining the proper steps to manage risk, whether it be to accept, mitigate, transfer, or avoid the risk". (Wheeler, 2011, Page 149):

- Accept: A decision to accept the risk
- Avoid: Ceasing (or not engaging in) the activity that is presenting the risk altogether
- Transfer: Shifting responsibility or liability for a risk to another party by contracting the corresponding cyber insurance
- Mitigate: Limit the exposure in some way

A. Risk Management and FAIR

Risks are identified and managed in accordance with corporate strategy and the corporation's risk appetite (Wheeler, 2011 Chapter 3 as of Page 43). Risk management incorporates the following:

- Resource Profiling
- Risk Assessment
- Risk Evaluation
- Documentation
- Risk Mitigation
- Validation
- Monitoring and Audit

The Factor Analysis of Information Risk (FAIR)3 is used as a model for understanding, analyzing and

DOI: 10.21307/ijanmc-2019-063

quantifying information risk in financial terms and builds a foundation for developing a scientific approach to information risk management.

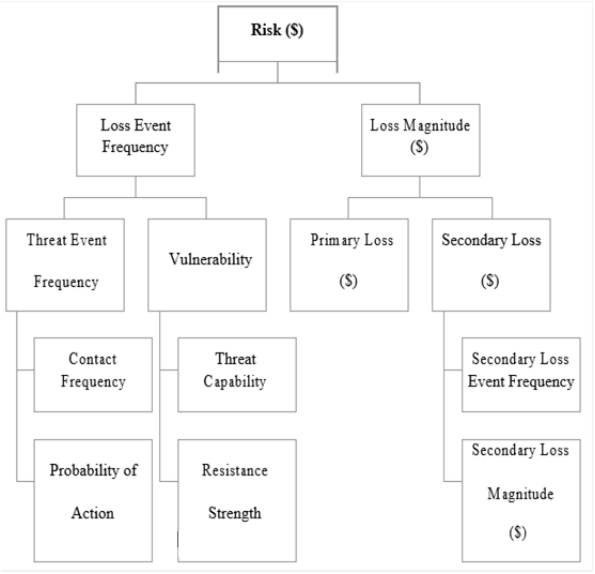


Figure 1. Factor analysis of information risk

For resource profiling, all resources are identified and the level of sensitivity is defined for each. A detailed threat analysis is performed quarterly to identify exposure and quantify risk and security controls are defined and implemented. It classifies the likelihood and consequences associated with each risk and how that risk could impact the business (See Tables 1, 2).

TABLE I. ENTERPRISE RISK MANAGEMENT LIKELIHOOD

Likelihood Table					
Level	Descriptor	Description	Frequency of Occurrence		
			Strategic	Operational	Routine
1	Rare	May only occur in exceptional circumstances	Less than once every 50 years	Less than once every 10 years	Less than once every 5 years
2	Unlikely	Could occur at some time	At least once in 20 years	At least once in 5 years	At least once in 3 years
3	Possible	Might occur at some time	At least once in 5 years	At least once per year	At least once per year
4	Likely	Will probably occur in most circumstances	At least once per year	At least once per quarter	At least once per month
5	Almost Certain	Expected to occur in most circumstances	More than once per year	At least once per month	At least once per week

TABLE II. ENTERPRISE RISK MANAGEMENT CONSEQUENCES

Consequences Table					
Impact	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme
Safety	No injuries	First aid treatment	Medical treatment, lost time	Medical treatment, extensive injuries	Fatalities
Financial Loss	< $50k or 0.5% of OB	$50k - $250k or 1% of OB	$250k - $3M or 2% of OB	$3m - $10m or 6% of OB	> $10m or > 10% of OB
Asset Loss	Little or no impact on assets	Minor loss or damage to assets	Major damage to assets	Significant loss of assets	Complete loss of assets
Interruption to Services	< ½ day	½ - 1 day	1 day – 1 week	1 week – 1 month	> 1 month
Information Management		Inaccurate data entry	Loss or corruption of database	Failure of backup data	System failure and/or extensive hacking attack
Legislative Compliance		Breach of Regulations	Warning from Regulator	Successful Prosecution	Cessation of Activities
Management Effort	An event, the impact of which can be absorbed through normal activity	An event, the consequences of which can be absorbed but management effort is required to minimise the impact	A significant event which can be managed under normal circumstances	A critical event which with proper management can be endured	A disaster with the potential to lead to the collapse of the University
Reputation and Image	Unsubstantiated, low impact, low profile or no news items	Substantiated, low impact, low news profile	Substantiated, public embarrassment, moderate impact, moderate news profile	Substantiated, public embarrassment, high impact, high news profile, third party actions	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party actions

III. DEFENSE AWARENESS

Part of building a proper structure to mitigate potential and future risks from cyber security attacks involves conducting workshops to educate personnel. Guidelines and training documents provide details on user access privileges. Institutions should maintain an inventory of assets, devices and applications, that a user needs access to, and this is secured with CyberArk, Multi-Factor Authentication is enforced to protect the firm from unauthorized access to corporate assets. Penetration tests are conducted regularly and maintains a robust vulnerability management system to monitor

changes within information systems. Application security policies include written procedures with secure coding standards to ensure secure development of in-house applications.

The following cybersecurity workshops and training are mandatory for executives and employees:

Workshop 1: Agree on which entities to cover and what information is considered nonpublic, as well as the materiality of transactions that relate to audit trail

Workshop 2: Enforce MFA and how to reconstruct an audit trail

Workshop 3: Clarify the certificate of destruction, and the feasibility of the Retention policy

Workshop 4: Train the staff and monitor for threats

Workshop 5: Discuss the feasibility of encryption of nonpublic information and test first line of defense on Microsoft office format documents.

A. Policies and Procedures

A set of 15 must-have policies complements the company's cybersecurity best practices and accompany the strategy to enforce its fulfilment. Policies and Procedures are communicated to all employees. Additionally, where required, appropriate sections are distributed to suppliers and contractors. In doing so, their importance is emphasized. Given that fulfilling them is compulsory, the firm audits compliance, provide continuous oversight, demand accountability, and, where necessary, impose sanctions upon those who violate these rules. The list of policies can be found as an Appendix B.

B. Safety and Physical Security

At any Institutions, employees' safety is a priority. Therefore, counting with the experience of a private security company, specific measures have been taken to ensure the safety of all employees either when working on premises (garage included) or when they travel for work purposes.

On the other hand, understanding that cyber-attacks can sometimes begin with a physical breach -for instance, when an outsider to surreptitiously gather fodder for a social engineering scheme or when an insider (such as a so-called "bad leaver") gains access to a company's network and wreak havoc, without initially using malware or other clandestine technological means- Institutions should take the physical security of facilities into consideration as part of the Cybersecurity strategy. The physical security in the firm's premises including the reception and entry checkpoints; ID scanner and other access records; video; physical logs; and garage records. Safety and physical security measures are audited periodically by a renowned firm to check they are implemented and working as expected, and updated or fixed if necessary.

C. Sytem Development Life Cycle and Change Management

All information systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of a system development life cycle. Requirements definition is a critical part of any system development process and begins very early in the life cycle, typically in the initiation phase. Security requirements are a subset of the overall functional and nonfunctional (e.g., quality, assurance) requirements levied on an information system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements. As recommended by the NIST4, early integration of information security requirements into the system development life cycle is the most cost-effective and efficient method for an organization to ensure that its protection strategy is implemented.

With regard to configuration management and control, it is important to document the proposed or actual changes to the information system and its environment of operation and to subsequently determine the impact of those proposed or actual changes on the overall security state of the system. Information systems and the environments in which those systems operate are typically in a constant state of change (e.g., upgrading hardware, software, or firmware; redefining the missions and business processes of the organization; discovering new threats). Documenting information system changes as part of routine SDLC processes and assessing the potential impact those changes may have on the security state of the system is an essential aspect of continuous monitoring, maintaining the current authorization, and supporting a decision for reauthorization when appropriate.

D. Continuous monitoring

As recommended by the NIST5, a critical aspect of managing risk to information from the operation and use of information systems involves the continuous monitoring of the security controls employed within or inherited by the system. The objective of the continuous monitoring program is to determine if the

set of deployed security controls continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. A well- designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective mechanism to update security plans, security assessment reports, and plans of action and milestones. Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

E. Monitoring Strategy

The monitoring program is integrated into the organization's system development life cycle processes. A robust continuous monitoring program requires the active involvement of information system owners and common control providers, CIO, CISO, and authorizing officials. The monitoring program allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real- time risk management and represents a significant change in the way security authorization activities have been employed in the past. The firm uses vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system.

F. Monitoring program includes:

- Configuration management and control processes for organizational information systems;
- Security impact analyses on proposed or actual changes to organizational information systems and environments of operation;
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the organization-defined continuous monitoring strategy;
- Security status reporting to appropriate organizational officials; and
- Active involvement by authorizing officials in the ongoing management of information
- System-related security risks.

G. Metrics

The results of our cybersecurity strategy are measured through a set of metrics that help us to monitor and control the implementation of the same, better manage our risk and make informed decisions. The list of metrics can be found as an Appendix C.

H. Documentation and Status Reporting

Continuous monitoring results are considered with respect to any necessary updates to the security plan, security assessment report, and plan of action and milestones, since these documents are used to guide future risk management activities. Updated security plans reflect any modifications to security controls based on the risk mitigation activities carried out by information system owners or common control providers. Updated security assessment reports reflect additional assessment activities conducted by assessors to determine security control effectiveness based on modifications to the security plan and deployed controls. The results of monitoring activities are reported to authorizing officials on an ongoing basis in the form of status reports to determine the current security state of the information system, to help manage risk, and to provide essential information for potential reauthorization decisions.

IV. SECTION 0 – TYPES OF ATTACKERS

According to the US Dept. of Homeland Security, "Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. "[6]

Knowing the enemy requires understanding the different threat actors, what their motivations and goals are, how they operate and their sophistication levels, all of which can be used to assess degree of risk. Security experts understand the continuum of threat actors well, based on monitoring and analysis of incidents. A variety of actors with different motivations and objectives are constantly looking for vulnerabilities. These players range from the "inadvertent actor" with no malicious intent to a sophisticated, well-funded and resourceful character that presents a much higher risk of significant impact.

The following table illustrates the types of cyber security actors, with references to historical cybersecurity cases for clarity:

TABLE III. CYBERSECURITY ACTORS. SOURCES: FORTUNE AND MCAFEE

Attacker	Who	Objectives	Targets	Signature	Likelihood	Consequences	Classic Case
State sponsored	China, Iran, Israel, Russia, U.S	Intelligence, state secrets, sabotage	Foreign governments, terrorists, industry	Multi-tiered, precisely orchestrated attacks that breach computer systems	Possible	Major	One-fifth of Iran's nuclear centrifuges crashed after Stuxnet, a worm reportedly developed by U.S. and Israeli intelligence, penetrated computers at an Iranian enrichment facility. Iran allegedly retaliated by disrupting access to the websites of J.P. Morgan (JPM, +1.25%), PNC (PNC, +1.27%), Wells Fargo (WFC, -1.05%), and others.
Hacktivists	Anonymous, AntiSec, LulzSec	Righting perceived wrongs, publicity, protecting Internet freedoms	Bullies, Scientologists, corporations, governments	Leaking sensitive information, public shaming, creepy YouTube videos	Likely	Minor	The websites of PayPal, Visa (V, +0.30%), and MasterCard (MA, -0.05%)were disrupted during Operation Payback, an Anonymous-led effort to punish companies that suspended the accounts of WikiLeaks in 2010. Some $5.6 million was lost by PayPal alone.
Cyber Criminals or black-hat hackers	Nigerian "princes," carders, identity thieves, spammers	Treasure	The gullible, online shoppers, small businesses, data-rich health care and retail companies	Stealing data, looting bank accounts	Possible	Minor	Coreflood, malicious software that records keystrokes and passwords, infected 2.3 million computers in 2009, some in police departments, airports, banks, hospitals, and universities. Affected companies suffered six-figure fraudulent wire transfers.
Insider	Disgruntled employees, contractors, whistleblowers	Score-settling, leaks, public good	Large companies, governments	Document theft	Unlikely	Major	Maroochy Shire, an Australian district along the Sunshine Coast in Queensland, was inundated with millions of gallons of untreated sewage in 2001 when a contractor hacked and took control of 150 sewage-pumping stations. He had been passed over for a job with the district. His dirty work cost Maroochy Shire upwards of $1 million.
Script Kiddies	Bored youth	Thrills, notoriety	Low-hanging fruit such as unprotected websites and e-mail accounts	Defacing or dismantling websites	Likely	Insignificant	An e-mail subject-lined I LOVE YOU duped people -- some of them inside the Pentagon -- in 2001. The virus it contained, which originated in the Philippines, destroyed files and simultaneously replicated itself, seeding in-boxes as it went. The so-called Love Bug caused an estimated $10 billion in digital damage and lost productivity.
Vulnerability Broker	Endgame, Netragard, Vupen	Hacking as legitimate business	Agnostic	Finding so-called zero-day exploits -- ways to hack new software, selling them to governments and other deep-pocketed clients	Rare	Minor	French firm Vupen hacked Google's (GOOG, +0.44%) Chrome browser at a security conference last March. Rather than share its technique with the company (and accept a $60,000 award), Vupen has been selling the exploit to higher-paying customers.
Cyber Terrorists	Terrorists	Spread fear, terror and commit murder	non-believers in their political or religious beliefs	create fear and chaos by disrupting critical infrastructure	Possible	Moderate	Ardit Ferizi was arrested in Malaysia charged in October 2015 with stealing the data belonging to the US service members and passing it to the members of the ISIS with the intent to support them in arranging attacks against Western targets.
Spy hackers	Hackers working for competing corporations	Steal trade secrets	Specific corporations	Leak information that are critical to victim's organization	Possible	Major	Chinese cyber spying of US for military and political reasons.

A. The Cyber Attack Decision Tree

Institutions should implement a Cybersecurity Framework based on NIST7. These are the framework's core functions:

- Identify
- Protect
- Detect
- Respond
- Recover

These core functionalities translate into the following actions:

1) Identify known cybersecurity risks to their infrastructure

2) Develop safeguards to protect the delivery and maintenance of infrastructure services

3) Implement methods to detect the occurrence of a cybersecurity event

4) Develop methods to respond to a detected cybersecurity event

5) Develop plans to recover and restore the companies' capabilities that were impaired as a result of a cybersecurity event

The following attack vectors have been considered and a decision tree based on the framework is provided below:

- Data Loss
- Insider Threat
- Vendor/Partner Compromise
- Compromise of Individual Device
- Phishing
- Network/System Breach
- DDoS Attack
- Ransomware

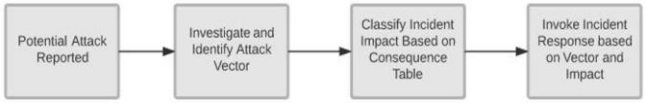


Figure 2. Detect and Identify

When a potential incident is reported, the incident will be investigated to determine if it is valid based on known attack vectors. Once validated, one or more members of the incident response team will collaborate to determine and classify the impact using the Consequence Table. The categories of incidents are insignificant, minor, moderate, major, and extreme. (See Consequence Table)

Each attack vector has the potential to overlap, particularly for data loss or insider threat. One or more of the following decision trees may be put into action depending on the circumstances of the breach.

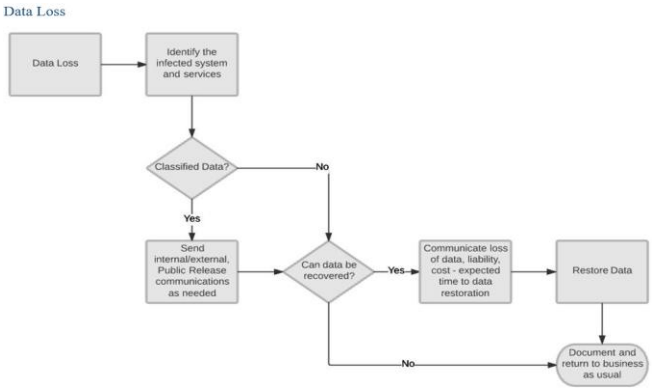


Figure 3. Respond and Recover

An incident that involves loss of data must be immediately analyzed for the loss of classified or sensitive data. If the data contains PII (Personally Identifiable Information), PCI (Payment Card Industry), SOX (Sarbanes Oxley) or other types of data deemed as classified or sensitive, then specific communications will be formulated to the necessary individual(s) and agencies.

The Communications Officer will be responsible for these communications with oversight from the C-Suite, CEO, CISO, CFO and CIO. For any other loss of data, the data recovery, backup and restore will be performed by Information Technology and business will resume as usual.

Figure 4. Insider Threat

If it is determined that any compromise was the result of an insider threat, whether it be a vendor, employee, consultant or former employee, an official investigation will be conducted to determine the goals of the attacker, data loss and entry points on the intrusion. Additionally, the investigation will expand to cover any individuals with close relations to the attacker and identification of additional known conspirators.

Immediately following the identification of an insider threat, the users account will be disabled based on IT guidelines. Furthermore, checks will be performed to identify any unknown accounts and logs will be assessed regularly for other suspicious unauthorized activity.

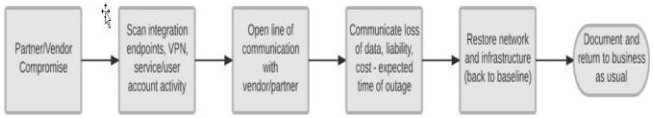


Figure 5. Vendor/Partner Compromise

In the event that a vendor account or endpoint is compromised, a line of communication will be opened with the vendor to assist in identifying the extent and nature of the breach. Data loss and network breach decision trees will be acted upon as well as investigation into any insider threats based on those who have access and knowledge of vendor systems and their inner workings. The goal will be to restore operations with the vendor in a timely manner while gathering the appropriate data to assess the damage and enable additional security protocols to secure the connection in the future.

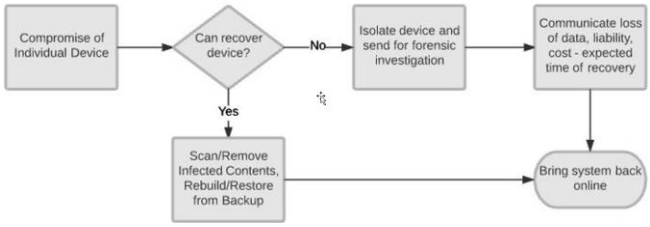


Figure 6. Compromise of individual device

If an individual device is compromised, the Desktop Support team will determine if the device is recoverable through scan and removal of malicious software or through backup and restore. If the device is an unrecoverable state, or the device is known to contain highly sensitive information, the device will be isolated, removed from the network and sent for forensic analysis. The CISO will work with the CIOO to communicate unusual findings.

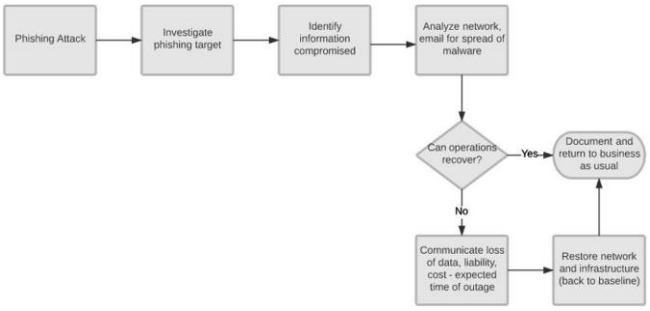


Figure 7. Phishing attack

If there is a malware detection that can be traced back to a phishing campaign, or a user reports a suspicious email or other form of communication that seems like a potential phishing attack, then the decision trees for data loss, system and network recovery will also be enacted.

There will be an investigation into the phishing target with the goal of determining the intention of the attacker and what information they were seeking (See Section 0 on common types of hackers) or may have retrieved. Depending on the extent of the breach, various members of the C-Suite will convene to determine next steps. The Human Resource department will be responsible for investigating the phishing target(s) to determine if any sensitive information was obtained. Further rules for response on data loss or network breach will be followed.

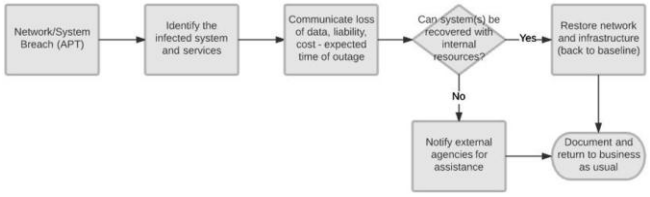


Figure 8. Network systembreach

In the event of an advanced persistent threat (APT), involving a multifaceted breach of network and system resources, it will be determined if systems can be restored with internal resources through collaboration of Information Technology and Information Security. If the breach is beyond internal expertise, external agencies such as the FBI (Federal Bureau of Investigation or DHS (Department of Homeland Security) will be contacted for assistance as needed. All members of the C-Suite, CEO, CISO, CIOO, CFO, as well as HR (Human Resources), will formulate a specific recovery plan and proper communications based on the severity and financial impact to the company by referring to the Consequences Table.

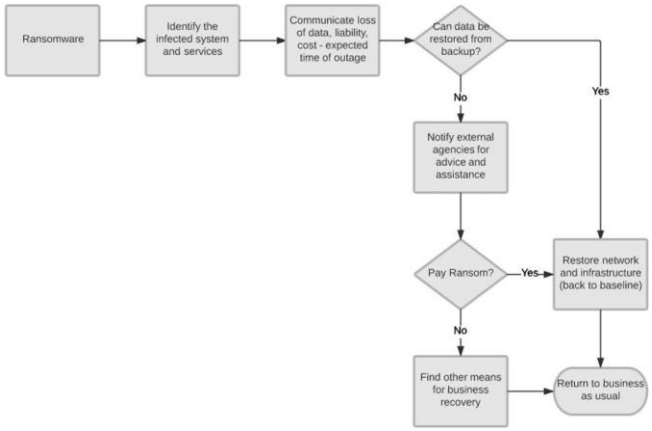


Figure 9. Ransomware

In the unfortunate case of ransomware, where there is potentially unrecoverable data loss through encryption and the data is being held for ransom, the data loss decision tree will also be invoked. If the data is considered classified or sensitive, or poses a risk where the business cannot recover financial loses, than external agencies will be notified for advice and assistance. All members of the C-Suite will be active in assessing the damage of a ransomware attack and determining the proper action.

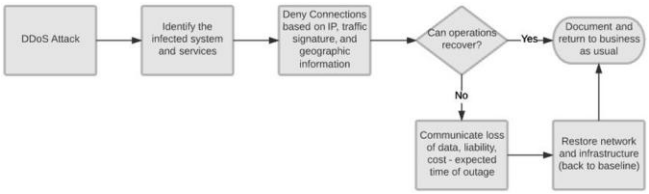


Figure 10. DDOS attack

In the event of a DDoS attack (Distributed Denial of Service), flooding of the network or targeted machines through an overload of requests, the IT Operations team will be responsible for denying traffic and reporting on any potential loss of data and or revenue streams. The CISO will work jointly with the CIOO to communicate the impact of the attack and set expectations for recovery time before returning to business as usual.

B. Protect and Prevent

The CISO will be responsible for cyber security education and overseeing ongoing improvements to cyber defenses. The Incident Response team will review the cyber security playbook quarterly and conduct table top exercises to rehearse incident response procedures. Knowing that attack vectors evolve over time and that attacks become more sophisticated each day, the decision tree will be updated and will adapt to lessons learned.

The cyber security playbook decision tree is meant as a general guideline. Each incident must be accessed and categorized individually and it is the responsibility of the C-Suite to analyze, communicate and react according to the various circumstances of each individual threat.

V. SECTION 2 – C-SUITE RESPONSE

Cybersecurity issues are no longer limited to the Information Technology department. Security breaches threaten every aspect of the organization and pose a significant threat to ongoing business continuity and reputation. These issues extend well beyond the technical environment and reach across the entire business ecosystem.

Cybersecurity solutions must encompass not only technical fixes, but also changes in business processes, controls, and management and employee behavior. Therefore, the Board of Directors understands that being prepared to understand cybersecurity issues, make the key decisions that prevent cyber issues from evolving into full-scale problems, and handle issues from the front-row if presented are the Board's responsibility.

Moreover, the factors that can help "to make the strategy succeed are: identifying information critical to your business; making cybersecurity part of your culture; considering cybersecurity impacts in your decisions; and measuring your progress". (Touhill & Touhill, 2014, Page 124).

As part of the governance model and following the recommendation of the National Association of Corporate Directors (NACD), An Institutions should follow these Five Guiding Principles:

1) Understand and approach cybersecurity as an enterprise-wide risk-management issue, not just an IT issue

2) Understand the legal implications of cyber risks as they relate to their company

3) Have adequate access to cyber security expertise and discussions should be held regularly at board meetings

4) Make sure that management establishes an enterprise-wide risk management framework with adequate staffing and budget

5) Identify which risks to avoid, accept, mitigate, or transfer through insurance.

The following sections detail the response for each C-Suite role:

A. Chief Executive Officer (CEO)

The CEO makes sure that Cybersecurity is incorporated into our strategy as a cornerstone of our business. "Our brand reputation, partnerships, potential investment opportunities, and competitive advantage all rely on the integrity of our information". The following factors have been taken into consideration to make our strategy succeed:

- Identification of the information critical to the business
- Cybersecurity as part of the company's culture
- Cybersecurity impacts considered in all decisions taken
- Measurement of the progress.

There are three initial considerations that the CEO takes into account: first of all, protecting our company against cybersecurity threats goes beyond the pure compliance with standards or regulations. Secondly, we strive to find the balance between cybersecurity and productivity, as. "Cost, performance, and ease of use are key attributes of an efficient and successful cybersecurity program." (Touhill & Touhill, 2014, Page 273). Thirdly, we take into account the risk management lifecycle.

Based on these initial considerations, our cybersecurity strategy distinguishes three **Areas of Focus:**

1) Establishing a governance model for security, including enterprise-wide collaboration,

2) Identifying and protecting critical data and applications, and

3) Developing and implementing an effective response plan.

The details of the Response Plan can be found in Section 1 of this Playbook but the Appendix D includes a comprehensive checklist taken into consideration for the firm's CEO when evaluating cybersecurity and taking major decisions before, during and after an incident.

Regarding the CEO responsibilities and according to the NIST Framework, "the head of agency (or chief executive officer) is the highest-level senior official or executive within an organization with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

As additional responsibilities, the following are considered:

- Making sure cybersecurity is part of the company's strategy and operational planning, the board discussion and the company's daily routine. This involves transforming the company culture, providing the necessary resources in terms of security systems and security trained personnel, and taking into account lessons learnt from previous incidents (if any) to improve its security posture.
- Creating a Security Committee lead by the CISO and which consists on the members of the C-suite (CEO, CISO, CFO, COO/CIO, Head of Legal/Head of Communication). This committee is in charge of protecting the privacy of corporate and customer data on the network and it from intruders, defining the company's risk posture, engaging 3rd party for hidden vulnerabilities or active compromises, developing and implementing the policies or guidelines required -in compliance with regulations-, and consider cyber insurance for the company and the Directors.
- Overseeing the company's response, especially the communication strategy in close contact with the General Counsel and the Head of Communication.
- Overseeing the damage control especially what is related to approving the investments and personnel needs to strengthen the company's defenses.
- Assisting the law enforcement after an incident -if required- in close collaboration with the General Counsel.
- Repairing the company's reputation with customers, partners, regulators, media, etc. in close collaboration with the Director of Communication.

B. Chief Financial Officer (CFO)

As most firms have the proper C-Suite executives working together in order for a strong collaborative effort to respond to any potential issues, the Chief Financial Officer (CFO) must be aligned for financial data. The CFO works closely already with CEO and CISO to understand the value in the data that could be possibly taken from a cybersecurity breach. From a financial view, the CFO works directly with technology and security to understand the leaks from a breach to manage potential risks. Majority of hacks including ransom cyber-attacks have a dollar value tied to them. The CFO needs to address these type of concerns, plus the costs of remediating the attack with appropriate amount of resources, risk mitigation activities, software upgrades, and patches. The CFO works with General Counsel, Legal, and Director of Communications to analyze the financial impact of the current hack and potential future hacks to understand the deep dive financial matters.

The CFO works directly with the CEO to discuss briefing matters on financials budgets associated with cyber-attacks. Each attack a company encounters needs to be justified to provide the correct amount of costs for man-hours for a patch, and software upgrades to internal systems to build preventive measures within an organization. The CFO is responsible for recommending a budget with C-Suite executives on an annual 3-year rolling forecast to factor in maintenance of upgrades to all internal and external systems that could possibly be faced with any type of cyber threats.

An approved allocated budget from the C-Suite executives allows CTO and CISO to work with external consulting providers to recommend equipment upgrades instead of fulfilling the requirements of hacker if a ransom was requested. It's worth remembering that when a company pays a ransom once, it will flood the gates with additional hackers in the foreseeable future to attack our organization for a quick payment instead of the organization getting cybersecurity expert law enforcement involved. Plus, this type of preventive measure keeps senior management in the loop to keep on investing more in security space of our organization by increasing annual budget to build workshops for firm awareness and risk mitigation.

- Budget: For 2017, the total is $650,000 for consulting and professional services for gap assessments for the year, which will allow senior management to focus on meeting requirements for 2018.
- Budget: For 2018, the total is $14,800,000 with CAPEX and OPEX for GTS/AME accounting for nearly $7,000,000.
- Status/Approach: Feb 2018, key deadlines include setting up a Cyber Security program, with policies and a CISO to manage all three lines of defense. Includes annual penetration testing and annual penetration testing and vulnerability assessments.

C. Chief Information Officer and Chief Operations Officer (CIOO)

Due to our complete reliance on technology to conduct business, the board may decide to combine the roles of CIO and COO into one: the CIOO. The combined role yields pronounced efficiencies/benefits in as far as cybersecurity is concerned, more so during and after attacks.

VI. SCOPE

It is understood that protection against and detection of cyber-attacks is the responsibility of the CISO.

The CIOO partners with the CISO in formulating and executing remediation. The CIOO is equally responsible for:

1) Responding:

a) Apply security patches to vulnerable or affected infrastructure components

b) Isolate/turn off infrastructure components

c) Deploy teams to investigate or remediate issue

2) Recovery:

a) Business recovery (BR) e.g. repair affected application, databases and systems

b) Activate business continuity (BC) plans

c) Activate disaster recovery and service continuity (DR/SCM) plans

Business continuity and recovery components to be addressed during and after a cyber-attack:

3) Adherence to legal, regulatory and governance requirements: refer to the Crisis

Management section of the firm's Governance Policy. The aim is to operate within the governance and regulatory framework even in the event of a crisis.

The objective is to guard against operational havoc by:

a Not violating governance, legal, and regulatory guidelines

b Not opening the door for exploitation of crisis situations by malicious actors

c Maintaining accountability, records and consistency (see figure below)

- **Collaborate with authorities** – SEC, FBI & NSA**.**
- **Address external risks** – partner/supplier relationships and communications
- **Global Context** – political, economic and social changes and events

VII. SYSTEMS CLASSIFICATION

To formulate appropriate responses and communications during a cyber-attack, the CIOO and their delegate would consult with the Applications and Systems Registry which contains, in addition to business and technical information, the appropriate RACI diagram. It should be used as the backdrop against which action is taken (see figure below).

TABLE IV. THE CIOO AND THE APPROPRIATE RACI DIAGRAM

Role	Assess Risk	Manage Risk	Fund Resources	Implement	Assure
Application Owner	I	R, A	R, A	A	A
IT	I	C	I	R	I
Operational Risk	R, A	I	I	I	C
Security	C	C	I	I	R

Responsible: Person or function responsible for executing the activity
Accountable: Person or function that owns the activity, approves work and is held accountable for it
Consulted: Person or function with information relevant to the activity
Informed: Person or function to be informed of progress and results

A. Data Classification

The firm assigns the highest priority in assessing the impact of an attack to the following classes of data:

1) Personally Identifiable Data (PII)

2) Non-Public Material Data (NPMI) such as SEC filing info, board resolutions of clients, etc.

3) Confidential Supervisory Information such communications from the SEC and other regulatory bodies.

Attacks impacting systems housing any of the above three types of data are high risk by nature. The default severity of any such attack is Major until it is downgraded.

B. Cybersecurity Events & Change Management

Since remediation and recovery entail changing components in the ecosystem and infrastructure, the CIO has put in place the following processes:

1) Emergency Change Management – Extreme and Major events justify the activation of these processes where signed pre-approvals are deposited by:

a) Business Application Owners

b) Business Unit Leaders

c) The BoD – subject to final sign-off based on the scope of action where there is:

- A need to communicate externally
- A legal liability
- Financial risk

2) Expedited Change Management – Moderate events warrant a scaled down change process where:

a) Pre-approved Damage Control (limited isolation of components/apps)

b) Fast-track change management - convening skeleton meetings within pre-approved timeframes based on affected apps/components attended by Application Owner and Business Unit representatives.

C. Structure and Delegation

The CIO has two delegates working in tandem and collectively participating in day-to-day business as well as during cybersecurity events:

- VP Operations Management
- VP IT Management

The CIO participation and delegation during cyber events is based on severity as shown below[8.]

TABLE V. THE CIO PARTICIPATION AND DELEGATION DURING CYBER EVENTS BASED ON SEVERITY

Cyber Event Participation Levels

Position	Extreme	Major	Mode rate	Minor	Insignificant
CIO	100%	100%	50%	25%	0%
VP IT	100%	100%	75%	50%	25%
VP Ops	100%	100%	50%	25%	10%

Participation levels are described as follows:

- 100% :
  - Cancel all personal commitments for 72 hours
  - Physically on-site in nearest offices for 72 hours OR if remote, via phone and email with access to appropriate dashboards and/or metrics.
- 75% :
  - Cancel all personal commitments for 48 hours
  - Physically on-site in nearest offices for the first 24 hours OR if remote, via phone and email with access to appropriate dashboards and/or metrics.
- 50% :
  - Keep personal commitments but refrain from alcohol
  - Maintain unfettered access to phone and email communication

- Maintain the ability to join conference calls or video conference meeting as necessary

- 25% :
  - Keep personal commitments and minimize alcohol consumption
  - Maintain unfettered access to phone and email communication o Anticipate periodic status update calls or messages

[8]Please note that a similar model applies to the rest of the members of the C-Suite.

D. Chief Information Security Officer (CISO)

Change is inevitable in every industry. But in finance, the pace of change is driven by regulatory flux, ever changing geopolitical landscape and the constant evolution of technology. Today's financial organizations face an unprecedented array of new challenges in the form of cyber-attacks. According to Cisco, "Playbook is perspective collection of repeatable queries against security event data sources that lead to incident detection and response". Cyber threats are dynamic in nature so it is important for the CISO's to have essential planning and communication skills while protecting shareholder value.

VIII. WHY CYBER SECURITY?

From the CISO perspective, the questions to answer are:

- What am I trying to protect?
- What are the threats?
- How do I detect them?
- How do I respond?

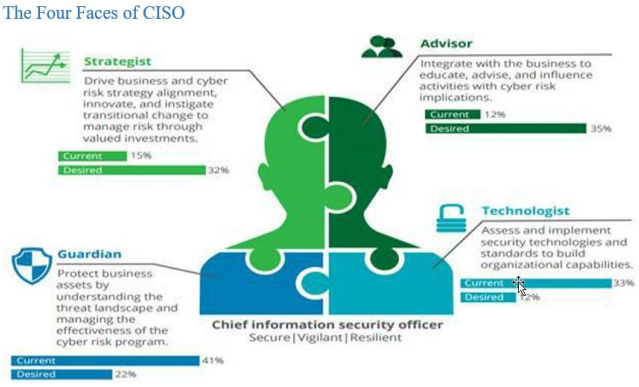


Figure 11. The four faces of CISO

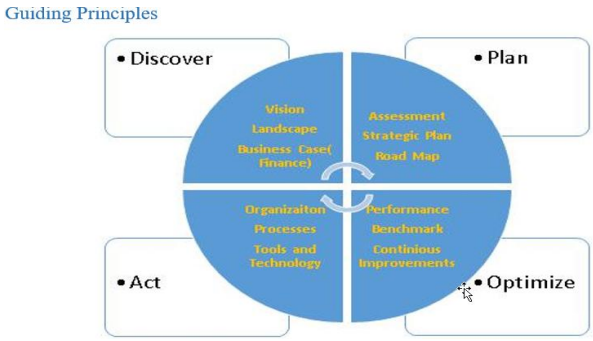


Figure 12. Guiding principles

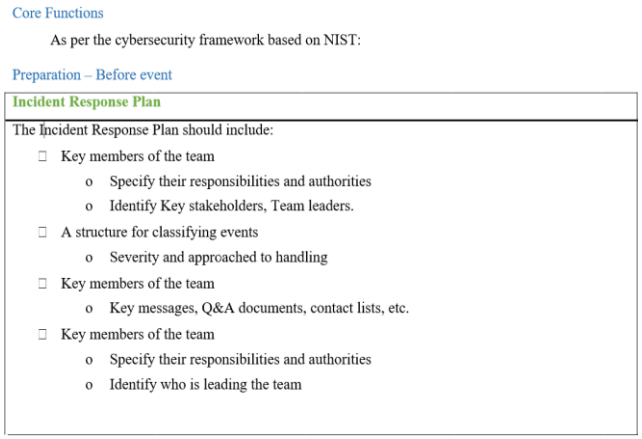


Figure 13. Preparation–Before event

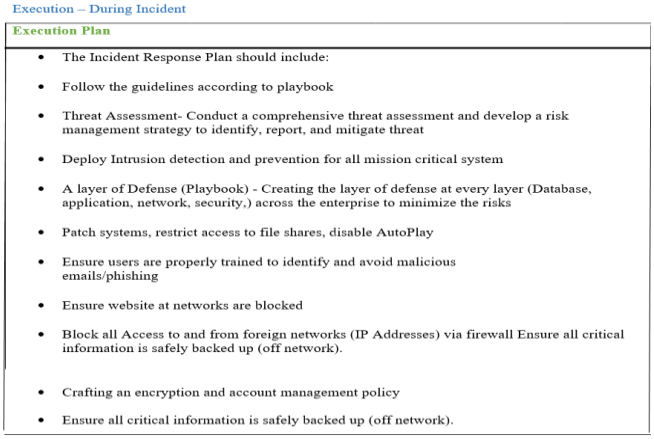


Figure 14. Execution-During Incident

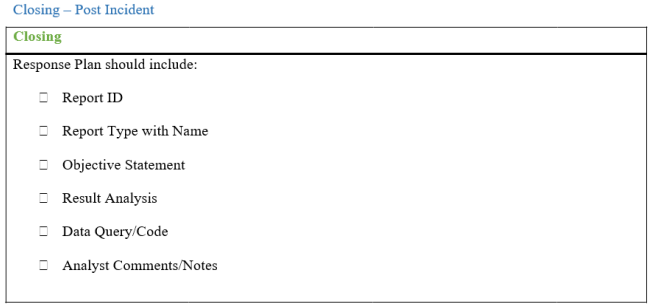
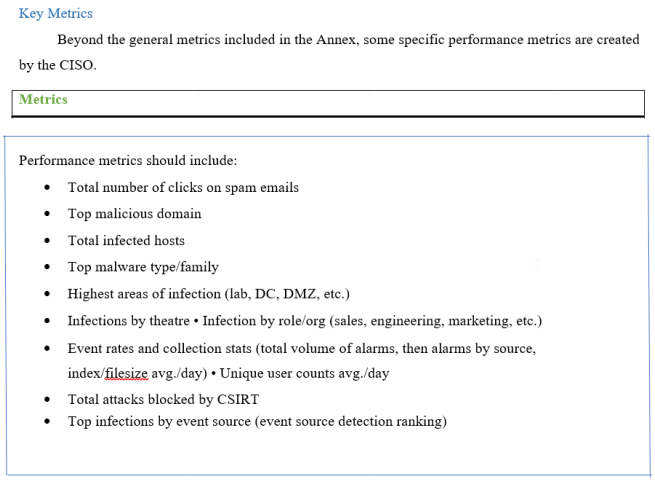


Figure 15. Closing-post incident


Key Metrics

Beyond the general metrics included in the Annex, some specific performance metrics are created by the CISO.

Metrics

Performance metrics should include:

- Total number of clicks on spam emails
- Top malicious domain
- Total infected hosts
- Top malware type/family
- Highest areas of infection (lab, DC, DMZ, etc.)
- Infections by theatre • Infection by role/org (sales, engineering, marketing, etc.)
- Event rates and collection stats (total volume of alarms, then alarms by source, index/filesize avg./day) • Unique user counts avg./day
- Total attacks blocked by CSIRT
- Top infections by event source (event source detection ranking)

Figure 16. Key Metrics

IX. LEGAL COUNSEL (AKA GENERAL COUNSEL)

The Legal Counsel side of the issue is critical to the attack, applying to the regulations of the state or country will prevent further damage in the form of lawsuits or penalties. Rules such as the GDPR needs to be adhered to because if found that after an attack not all proper precautions were followed according to the guidelines, a hacker will be the least of our worries. While legal is necessary for incident response, following the proper protocols ensures an attack has minimal damage.

A. Key concerns for General Counsel heavily revolve around compliance to meet Federal Mandates

It is a sole responsibility for C-Suite Executives to be aware of all information security regulations that apply to the company, such as Health Insurance Portability and Accountability Act (HIPAA), 1999 Gramm-Leach-Bliley Act, and the Federal Information Security Management Act (FISMA) as part of the 2002 Homeland Security Act, General Data Protection Regulation (GDPR), and Payment Card Industry Data Security Standard (PCI DSS). General Counsel needs to work with both CISO and CIO to ensure information system security practices follow proper guidelines. Moving forward we need to be up to date on National Institute on Standards and Technology on best practices of cyber security infrastructure and policies.

Next aspect of General Counsel is to ensure that audits follow proper methodology for Federal Review and are set in place in order to produce efficient controls. Keeping semi-annual audits of internal information security infrastructure, where a draft is written up to help conclude how the system can be improved. With all of the Third-Party vendors working with our organization we need to ensure audits are conducted based on information security policies and systems will not be a liability to the company. General Counsel needs to adhere to best practices in risk management so as to have minimal or no damage in an attack.

The General Counsel moves in the direction to ensure that proper law enforcement barriers are set up in our preventive measures and resolution plan. We have drafted a created list based on scenarios on how much damage and type of damage expectations to occur before involving the federal authorities. Internally, within our organization, we have established connections with security clearance authorities as well to understand the scope of the investigation to address how it will affect the firm's information and business processes.

General Counsel has developed a proper Data Retention Policy for internal employees and external clients to keep data secured then protected. We need to understand the policies of data retention of how to properly manage and maintain data as evidence in case of a customer request for information (RFI). Then a major focus is on ensuring the integrity of the data is preserved as well as having documented the chain of custody which begins in the collection phase.

General Counsel have created the proper documentation to executive opinions that could possibly affect Attorney-Client privilege. The knowledge of the incident response fall under normal operations and which are protected under attorney client privilege. Counsel should be involved in all communication whether it be phone, email, etc. between company and the cyber security consultants brought in for the attack. Direct contact with General Counsel is required immediately after an attack as the worst part of the attack is right after it has taken place because of speculation on incomplete information, damaging communication is likely to occur.

1) Compliance

As we are in a growing age of cyber security breaches and constant hacks from outside parties of each organization, the laws of data security and provisioning have been increasing. The US Regulators have forced organizations with client and customer data to take increase precautionary methods to ensure governance. Some of these types of new regulations include Department of Financial Services (DFS) Cyber Law, GDPR, Multi-Factor Authentication, and Third-Party Security Program.

The DFS Cyber Law remediation plan is heavily focused on proper governance requirements to meet Federal Requirements by FINRA. As the need for proper preventive methods, C-Suite Executives turn to Legal Counsel to build property strategies to implement a strong cyber security infrastructure that resembles all divisions of the company from Front to Back office. This includes a program to design a risk based approach with policies to address key elements reviewed by the General Counsel and CISO to oversee the program.

The General Counsel will need to translate Federal Requirements to build a variety of tools with alignment from all areas of the organization. These types of technical implementations include Multi-Factor Authentication to network access, encryption to protect information, and breach notification to notify the DFS within 72 hours of a cyber-attack. With the new mandates being consistently brought up in the media, it is aggressive timeline to implement these requirements based on the increase amount of threats within cyber-attacks. Information Technology stakeholders globally such as ITEC and GTS will help with the execution and regulatory requirements such as GDPR outline exactly what is needed to be followed for US regulations.

2) Guidelines for Compliance

Purpose: Law requires banks regulated by DFS to establish and Maintain Cyber Security Program

- **Section 1**: Compliance by August 28, 2017 such as CS program, policies, and CISO
- **Section 2**: Compliance by March 1, 2018 such as MFA, Training and Risk Assessment
- **Section 3**: Compliance by September 2, 2018 such as Audit Trail, Data Encryption and Monitoring
- **Section 4:** Compliance by March 1, 2019 such as Third-Party Security Program

B. Director of Internal and External Communication

The main responsibility of the Director of Internal and External Communication in a cybersecurity breach is to keep the public aware of any risk mitigation issues and a strong response to the media that we as C-Suite level employees are ensuring best practices to safely protect the data of our customers. In this day and age, it is very crucial to develop relationships outside the organization with correct media outlets to release significant details while gaining the trust of our shareholders. These types of breaches have in the past caused many issues by not focusing efforts on communication and keeping shareholders and stakeholders in the loop.

1) Internal Communication

Internal communications address two groups that will include the employees as well as any business partners. Effective internal communications will mitigate the need of panic by individuals and organizations who are working in the company or with the company. If employees or business partners panic and make consequential decisions based on incomplete information they could cause much more harm than the attack itself. An effective communication plan will allow for smooth flow of information at the time of crisis so attention can be given to the more pressing issue of how to stop the attack and not with its secondary effects.

Managing the internal communication between employees and C-Suite is a fundamental need quickly as a response. This keeps employees in the loop and aware not to communicate outside of the organization that could reflect negatively within the media. Right away as soon as the attack occurs and management is notified, all employees will receive an email from Human Resources. This information will report that a breach has occurred and further information will be made available as soon as possible. Also, all internal emails by non-members of the internal team investigating the incident should cease because speculation could cause unnecessary panic. There will be a request to not use social media at this time and listing the consequences of misinformation can cause. All Information Technology senior management will receive a separate protocol which depending on the specifics of the attack will notify how their department will be responding to the attack. The CISO here will be the main supervisor in charge of all necessary changes that need to be made to any information systems.

Other banks and broker-dealers our firm does business with should be notified in a proper response method in order to protect business with our partners. If the company has any legal obligations to inform of an attack in a specified amount of time as is the case with the GDPR regulations on breach notification, let the entity know of the attack, whether it be for compliance, insurance, or CIRT. Let any business partners know how any vulnerabilities to their information, so they can begin any incident response plans to help keep their business from being affected by the attack.

2) External Communication

External Communications will focus on stakeholders of the company as well as the media. External communications will be less specific and will be to keep the public image of the company as one that in top of the attack and give assurance to stakeholders and customers alike. A great example of bad external communications is the SONY hack, where SONY's reputation was tarnished for not standing up to the hackers.

Based on external communications a major area of concentration needs to be on top of the stakeholders and shareholders in the organization to get the latest up to date information. This type of direct involvement by C-Suite executives makes shareholders feel part of the organization with engagement notifications. The focus on these type of communications is based on specifics of the cyber-attack, the plan created to ensure that the company does not allow further information or data to be viewed in public mindset. The communication externally will be able to then come up with a strategic plan to discuss increase in security controls, password resets, identification requirements, and preventive measures for a patch. The communication that will be shared with the public will be drafted by the C-Suite to explain all of the above with additional answers to questions faced by media scrutiny.

Managing Public Relations is going to be key in our cyber breach playbook. Depending on the scope of the attack, a strong Public Relations response and resource will need to be positioned here as majority of the C-Suite will be completely consumed in responding to the attack. The first response to the media will be crucial in order to have control of any negative news that could hurt our organization. The company will make it a top priority to have the appropriate response in order to set up proper damage control and manage expectations. The public relations team will have to set up proper contacts within each media organization ahead of time to reveal minimal details of the attack and assure the public of the risk mitigation activities being performed by senior management.

3) Communications to regulators

The firm has decided to adopt a doctrine of transparency in reporting cybersecurity attacks, despite the fact that the practice is optional. The reporting, however, is qualified in that it should apply only to Extreme and Major events. The rationale is that the company needs to guard against long-term reputational loss/damage, despite the short-term risks of stock price fluctuation. In the event of Extreme and Major attacks, the executive board will approve communications based on form 8-k using Fish & Richardson Disclosure Decision Tree depicted in figure below:

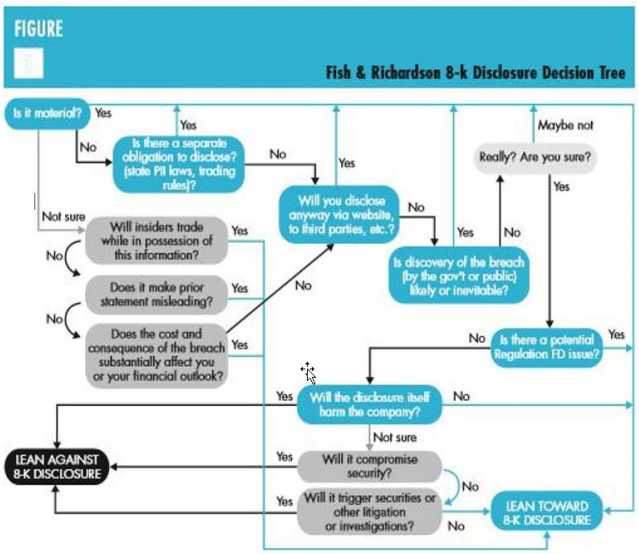


Figure 17. Appendix A. Organization Chart

TABLE VI. APPENDIX B. CYBERSECURITY POLICIES

Retrieved from (Touhill & Touhill, 2014, Page 197)

1. Acceptable Use Policy	6. Employee Internet Use Monitoring and Filtering Policy	11. Remote Access Policy
2. Computer Ethics Policy	7. Technology Disposal Policy	12. Mobile Device Policy
3. Password Protection Policy	8. Physical Security Policy	13. Software Policy
4. Clean Desk Policy	9. Electronic Mail Policy	14. Access Control Policy
5. Use of the Internet Policy	10. Removable Media Policy	15. Network Management Policy

TABLE VII. APPENDIX C. CYBER SECURITY METRICS

Question	Metric Category	Metric
How Vulnerable Are We	**1.0**	**Number of Threats Detected**
	1.0.1	How many times are we being "pinged" and "probed"?
	1.0.2	How much spam is filtered?
	1.0.3	How many phishing messages are we receiving?
	1.0.4	Who is targeting us?
	1.1	**Number of Known Vulnerabilities**
	1.1.1	System vulnerabilities
	1.1.1.1	Number of vulnerabilities discovered
	1.1.1.2	Percentage of vulnerabilities mitigated in prescribed time frames
	1.1.1.3	Number of residual vulnerabilities
	1.1.2	Other Vulnerabilities
	1.1.2.1	Percentage of systems and devices beyond projected life span
	1.1.2.2	Percentage of software beyond projected life span
	1.2	**How Many Cyber security Incidents Have We Detected?**
	1.2.1	Number of cybersecurity incidents detected
	1.2.2	Number of detected cybersecurity incidents by category
	1.2.3	Cost per incident
	1.2.4	Who is responsible for cyber security incidents
How Effective Are Our Systems and Processes?	**2.0**	**Network Performance Measures**
	2.0.1	Network Performance Measurement
	2.0.2	How does network performance compare to previous measurements?
	2.0.3	Percentage of devices with current security software
	2.1	**Change Management**
	2.1.1	Number of unauthorized changes, Unauthorized changes to your systems are not good
	2.1.2	Percentage of maintenance successfully accomplished within schedule and budget
	2.2	**Software configuration management**
	2.2.1	Percentage of software current with all known patches. This is a critical cybersecurity measure. It makes sense to patch your soft
	2.2.2	Number of unauthorized software and media detected on network and devices
	2.3	**Physical Security**
	2.3.1	Number of physical security incidents allowing unauthorized access into facilities
	2.3.2	Number of violations of clean desk policy
	2.4	**Acquisition**
	2.4.1	Percentage of System and service contracts that include security Requirements and/or Specifications
Do we have the right people, are they properly trained, and are they following proper procedures?	**3.0**	**Percentage of employees who have current Cybersecurity training**
	3.1	**Percent of technical staff with current certifications**
	3.2	**Number of Users with system administrator privileges**
	3.3	**Number of security violations during reporting period**
	3.4	**Percentage of security incidents/violations reported within required timelines**
Am I Spending the Right Amount on Seurity?	**4.0**	**Cyber security Costs**
	4.0.1	Percentage of the IT budget devoted to cybersecurity
	4.0.2	Percentage of the organization budget devoted to cybersecurity
	4.0.3	Execution of current budget
	4.1	**Value of Information**
	4.2	**Consequences of Information loss, Tampering, or Destruction**
	4.2.1	Cost to replace
	4.2.2	Estimated costs associated with loss, tampering, or destruction of information
	4.2.3	Estimated costs associated with regulatory fines for failing compliance
	4.3	**Cybersecurity Risk Exposure**
	4.3.1	Cybersecurity risk

TABLE VIII. APPENDIX D. CHECKLIST FOR CEO(EXECUTIVES IN GENERAL)

Appendix D. Checklist for CEO (Executives in general)

Retrieved from (Vantage Point, 2016)

Before an Incident

1 - Stay current on the latest threads and cyber security best practices	4 - Research, design, and deploy security technology. Consider access control, data security, training, processes, and procedures	7 - Ensure the response plan covers communications, analysis, mitigation, and other critical tasks	10 - Discuss with counsel whether cybersecurity risk factors in the company should be disclosed (i.e. SEC 10-K filings) in public
2 - Designate a board committee tasked with cyber security responsibilities. Establish links between board and C-level executives, specially CIO and CISO	5 - Develop and deploy the appropriate systems to identify a cyber security event as soon as possible	8 - Run practice drills to test the plan and revise it as needed	11 - Obtain liability insurance specifically covering cyber security risk for directors and officers as well as for the corporation
3 - Identify the firm's security posture and the risks to the company. Assess the company's systems, assets, data, and capabilities. And identify risks unique to your industry	6 - Create an incident response plan that lays out who reports to whom. Build in contingencies in case some people are unavailable at the time of an incident	9 - Establish a recovery plan to restore any capabilities or services impaired by a breach and to protect the company from further attacks	12 - To limit the company's liability in certain kinds of attacks, consider cyber security vendors certified by U.S. Department of Homeland Security's SAFETY ("Support Anti-Terrorism By Fostering Effective Technologies") Act

TABLE IX. ONE EVENT FOLLOWED BY ANOTHER

During an Incident

1 - Oversee an incident response. Serve as a conduit between incident responders within the company and external stakeholders including customers, partners, and regulators	2 - Understand that news of the incident usually comes to the company from outsiders, such as law enforcement or partner companies. Keeping the event under wraps is no longer very likely	3 - Work closely with your legal counsel and public relations team to advise C-level executives about how to disclose incident details, especially to news media. Don't disclose facts until they've been verified	4 - Stay in touch with your response team to assist as needed during response and through remediation

After an Incident

1 - After a breach has been repaired, intruders ejected, and systems restored, assist in damage control to fix the company's infrastructure and reputation	2 - Review incident response to assess how it went. Identify weaknesses in equipment, systems, and procedures to determine where to make improvements	3 - With guidance from your legal counsel, determine how to make customers whole if their data was exposed or stolen	4 - Consider offering free credit monitoring, issuing new account numbers, and so on. Identify the "churn rate". Counsel can advise as to any consumer remedies required by law

REFERENCES

[1] Morgan, S. (2015, November 24). IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'. Retrieved August 05, 2017, from https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#75f85d3973f0

[2] Global Cost of Cybercrime Predicted to Hit $6 Trillion Annually By 2021, Study Says. (2016, August 16). Retrieved August 05, 2017, from http://www.darkreading.com/attacks-breaches/global-cost-of-cybercrime-predicted-to-hit-$6-trillion-annually-by-2021-study-says/d/d-id/1326742

[3] Cybersecurity Questions for CEOs. (n.d.). Retrieved August 5, 2017, from https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[4] Fry, E. (2014, June 12). The 6 worst kinds of computer hackers. Retrieved August 05, 2017, from http://fortune.com/2013/02/26/the-6-worst-kinds-of-computer-hackers/

[5] M. (2016, October 24). 7 Types of Hacker Motivations. Retrieved August 05, 2017, from https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

[6] Enterprise Risk Management Consequence and Likelihood Tables. (n.d.). Retrieved August 6, 2017, from https://ppl.app.uq.edu.au/sites/default/files/Risk%20Consequence%20and%20Likelihood %20Table%20-%20Form.pdf

[7] Touhill, Gregory J., and C. Joseph Touhill. Cybersecurity for Executives, Wiley, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/columbia/detail.action?docID=1707094.

[8] Wheeler, E. (2011), Security Risk Management, Chapter 8, Risk Evaluation and Mitigation Strategies, Elsevier Inc.

[9] Institute, F. (n.d.). FAIR, an international standard by the Open Group. Retrieved August 08, 2017, from http://www.fairinstitute.org/an-international-standard

[10] Deinert, A. (2016), "Cybersecurity Breach Playbook: What Every IT Administrator Needs to Know", Vantage Point Solutions, Mitchell, SD

[11] Framework for Improving Critical Infrastructure Cybersecurity. (n.d.). Retrieved August 8, 2017, from

[12] https://www.bing.com/cr?IG=46B942FD8FD04ED7A2EF4DE7E061BAE0&CID=18B3474BBA4361240BCE4D93BB45607D&rd=1&h=qHbOGImxzOpDg5E54Eh7p9I1gen0wVX Vy1g-wVCQk6w&v=1&r=https%3a%2f%2fwww.nist.gov%2fdocument-3766&p=DevEx,5063.1

[13] Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2017, February 19). Computer Security Incident Handling Guide. Retrieved August 08, 2017, from https://www.nist.gov/publications/computer-security-incident-handling-guide

[14] Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2017, February 19). Computer Security Incident Handling Guide. Retrieved August 08, 2017, from https://www.nist.gov/publications/computer-security-incident-handling-guide

[15] NIST. (2014, February 12) Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[16] Scholtz, T., McMillan, R. (2017, January 26). Institute Cybersecurity and Risk Governance Practices to Improve Information Security. Gartner.

[17] Kark, K., Francois, M., Aguas, T. (2016, July 25). The new CISO: Leading the strategic security organization. (n.d.). Retrieved August 09, 2017, from https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html

[18] Fry, E. (2014, June 12). The 6 worst kinds of computer hackers. Retrieved August 09, 2017, from http://fortune.com/2013/02/26/the-6-worst-kinds-of-computer-hackers/

[19] M. (2016, October 24). 7 Types of Hacker Motivations. Retrieved August 09, 2017, from https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

[20] https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[21] https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#bfb909373f07

[22] http://www.darkreading.com/attacks-breaches/global-cost-of-cybercrime-predicted-to-hit-$6-trillion-annually-by-2021-study-says/d/d-id/1326742

[23] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[24] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[25] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[26] K. Elissa, “Title of paper if known,” unpublished.

[27] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[28] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[29] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[30] Electronic Publication: Digital Object Identifiers (DOIs):

Article in a journal:

[31] D. Kornack and P. Rakic, “Cell Proliferation without Neurogenesis in Adult Primate Neocortex,” Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

Article in a conference proceedings:

[32] H. Goto, Y. Hasegawa, and M. Tanaka, “Efficient Scheduling Focusing on the Duality of MPL Representatives,” Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.