RFID-based Electronic Identity Security Cloud Platform in Cyberspace

Bing Chen¹, ², ³ and Chengxiang Tan³
¹The 3rd research institute of ministry of public security, Shanghai, China
²Key laboratory of information network security, Ministry of Public Security, Shanghai, China
³Dept. of computer science and engineering of Tongji University, Shanghai, China
Email: bing_chen2000@163.com, jerrytan@tongji.edu.cn

Bo Jin, Xiang Zou and Yuebo Dai
The 3rd research institute of ministry of public security, Shanghai, China
Email: {jinbobo, xzou2008}@gmail.com, daizhiyu2006@163.com

Abstract—With the moving development of networks, especially Internet of Things, electronic identity administration in cyberspace is becoming more and more important. And personal identity management in cyberspace associated with individuals in reality has been one significant and urgent task for the further development of information construction in China. So this paper presents a RFID-based electronic identity security cloud platform in cyberspace to implement an efficient security management of cyber personal identity, and designs and realizes a strong and pervasive security cloud service platform, and discusses key technology including security authentication mechanism for the electronic identity card, super high frequency RFID with eID cards, multilevel privacy protection mechanism, security cloud service, security isolation and single-oriented transmission, and boundary security gateway protection, and it can well apply to personal identity management with virtual roles of citizens in cyberspace such as E-Government and E-Business, and the electronic identity security platform has been primary implemented and achieved good effects in actual applications.

Index Terms—electronic identity (eID), cloud computing, RFID (radio frequency identification), security platform, security infrastructure

I. INTRODUCTION

With our national scientific and technological information construction advancing deeply, technology and industry of Internet of Things will be more and more important and focused on. Development of our national E-Government in new period makes demands of achieving personal network identity management associated with individuals in reality to assure trusted security, fully exerting efficiency of E-Government. So electronic identity (simply called eID) management in cyberspace has been one important task for the further development of information construction in China.

Now, information technology has been making an explosive evolution, and there will be lots of security threats hidden in Internet of Things. And it has been faced with great challenge on security, accuracy and efficient management for eID management in the process of people’s network activities. So it is necessary to research RFID-based eID security cloud platform in cyberspace to achieve efficient security management of personal real identity in networks, especially about individual’s online activities in networks.

Challenges on RFID-based eID security cloud platform mainly focus on how to realize the system not only more efficient and safer but also protection personal privacy of citizens, but current solutions mainly include PKI system, CA center, and some state security strategy on Identity Ecosystem, these solutions haven’t dealt with the problems above well yet. Thus, the paper discusses key technology including security authentication mechanism for the electronic identity card, super high frequency RFID with eID cards, multilevel privacy protection mechanism, security cloud service, security isolation and single-oriented transmission, and boundary security gateway protection, and provides general security frame to solve problems of security and privacy in the process of personal identity management in cyberspace associated with individuals in reality.

II. RELATED RESEARCH

Now research about eID mainly focuses on digital identity management technologies and systems by governments and enterprises, and so on.

European Union (EU) presents a roadmap for a pan-European eID management framework by 2010, and prepares for identity management system among their member nations and other allied. And the suggestions will provide pervasive and cross-border digital identity administration service, especially for cross-domain service. But the framework hasn’t been practiced too well yet. [1-2]
The United States also presents state security strategy on Identity Ecosystem, expected to provide trusted identities in cyberspace. The Identity Ecosystem aims at providing secure, efficient, easy-to-use, and interoperable identity solutions to access online services so that it can promote confidence, privacy, choice, and innovation for individuals and society.

Many other nations such as Korean, Australia, Germany, also present related security eID management plan.

RFID [8-10] is a contactless automatic identification technology called radio frequency identification. And it can realize automatic identification in static or dynamic objects and personnel. And the most basic of RFID system consists of tags, readers and antennas.

The cloud [11-17] is not simply the latest fashionable term for the Internet. Though the Internet is a necessary foundation for the cloud, the cloud is something more than the Internet. The cloud is where we go to use technology when we need it, for as long as we need it, and not a minute more. We do not install anything on our desktop, and we do not pay for the technology when we are not using it.

The cloud can be both software and infrastructure. It can be an application we access through the Web or a server that we provision exactly when we need it. Whether a service is software or hardware, the following is a simple test to determine whether that service is a cloud service:

If we can walk into any library or Internet cafe and sit down at any computer without preference for operating system or browser and access a service, that service is cloud-based.

It can define three criteria in discussions on whether a particular service is a cloud service:

- The service is accessible via a web browser (nonproprietary) or web services API.
- Zero capital expenditure is necessary to get started.
- We pay only for what we use as we use it.

Security isolation technology mainly includes GAP technology (Gap All Protocols), data pump technology, data diode technology, virtualization, application proxy, etc. [18-21] GAP technology is based on oriented ferry and intercommunication data transmission technology, and its principle is to simulate data copy by hand, and to remove applied data and to cut off the communication protocols of upper operation, and to adopt private communication or storage protocols. Data pump technology, based on communication, only permits single-oriented data transition and the opposite control information passing. Data diode technology, also called as the single-oriented technology of information flow, adopts blind sending, and the opposite direction not only has no data channels but also has no control channels, and it completely keeps the blind state.

ISO/IEC 18028-3 [22] integrates security domain partition and network area, and focuses achievement of security policy upon boundary security assurance of security domain. Protection technology of network boundary security includes firewall, invading and detecting, VPN, security gateway, network virus scanning, application proxy, and so on. It is the main trend to satisfy users’ security need by technology combination, including the firewall and IDS linkage, UTM, network access and control, etc. [23]

III. SECURITY RISK ANALYSIS

From security system architecture, eID system security has all-dimensional, multilevel and multi-aspect architecture. Generally, system security risk can be divided into five aspects as follows.

1) Link security: It means that link security between access terminals and access network boundary should exceed the private link or adopt encrypting technology to assure the information integrality.

2) Network security: It means that confidentiality and integrality of information transmission should be assured, and measures should be taken like encryption, isolation, and horse protection, also security authentication, privilege, and other security promotion should be provided with access terminals and users to defend the network security risk.

3) Host security: It means that security solidness with inner hosts including terminals and servers should be provided against host operating security.

4) Application security: It means that measures such as identity authentication, access control and system monitoring should be taken against application security risk.

5) Centralized monitoring and audit: It means that monitoring and audit data can be sent to centralized monitoring and audit system inside.

IV. GENERAL DESIGN AND IMPLEMENTATION

A. General Design Goal

RFID-based electronic identity security platform in cyberspace, comprised of related communication networks between network and citizens, software and hardware equipments, security policy and standards and specifications, will be simply called eID security platform hereafter.

The main goal of eID security platform is to realize security eID management in the process of citizens’ online activities. And contents mainly include five aspects as follows:

- The system should maintain more trustworthy and safer: PKI-based authentic public and private key-pairs can be used to encrypt/decrypt and sign the messages, and no information of private keys can be leaked from the eID card, so as to assure more trusted and secure, especially involved in online services.

- The system should maintain more convenient and efficient: eID cards with RFID can achieve contactless interfaces to authenticate citizens’ identity. Thus, eID cards can be deployed in more places and scenarios and apply to more security applications.
The system should maintain low cost: digital identity management systems constructed by E-Government and E-Business can be integrated as well. Many online services can use eID platform as its security infrastructure and additional security service.

The system should maintain more pervasive and authoritative: the system must be administrated by a function government to protect personal privacy and information authority.

The system should realize better privacy protection: digital identity management system must defend individual privacy information from others except eID signer. Especially, privacy information can’t be obtained by any of the third party.

B. General Security Architecture

According to the design goal, the system assures not only itself security but also safe and efficient and convenient for citizens between the system and users when people participating network activities. As shown in Figure 1, eID security platform generally can be divided into several aspects as follows:

1) Supporting Infrastructure: To be comprised of public key and privilege infrastructure, security threat awareness and forewarning, security administration and audit, etc., and to be the foundation of security mechanism of the system.

2) Data information security: To assure inner data information security and protected networks from aspects such as storage security, content security, and fault-tolerant recovery.

3) Applied boundary security: To be comprised of identity authentication, privilege access control, and security isolation, providing applied boundary security protected networks and systems.

4) Data transmission security: To be comprised of privacy, integrity, and non-repudiation. Based on cipher service provided by public key infrastructure, data transmission security of inner and boundary can be implemented by correlative cryptography technologies.

5) Applied environment security: To be comprised of terminal security, host security, and applied security, and construct security application environment based on it.

C. System Implementation

According to the general goal and security architecture above, the system implementation mainly includes realizing supporting infrastructure, storage and content security, applied boundary security, data transmission security, and applied environment security.

The supporting infrastructure mainly includes public key infrastructure system, security threat awareness and forewarning system, and security management and audit system. And public key infrastructure system issues eID cards with certifications, and provides LDAP service and OCSP service, and other security services. And the security threat awareness and forewarning system by sensors fixed at key nodes implements real-time monitoring of security threat situation of the platform, and actively finds frangibility of vulnerabilities, aggressive behaviors, infections of virus and horses, assets situation and utilization, and other abnormal behaviors, and assesses in real time security threat, alerting by console or short-message-sending. And the security administration and audit system achieves real-time monitoring and audit of the whole eID platform to be audit and monitor conveniently and safely.

The storage and content security of data information security can be achieved on interior application servers and other storage media of the system. And fault-tolerant recovery security can mainly be realized by interior security isolation and single-oriented transmission system, disaster recovery system, system recovery, and correlative verification mechanisms.

Applied boundary security can be individually realized on boundary of every application system and protection and control systems of boundary security. Boundary security assurance can be provided by security mechanisms such as terminal identity authentication, user identity authentication, mandatory access control of boundary access, application proxy, security isolation and single-oriented transmission.

Data transmission security can be realized in communication links of intranet, and between boundary and outer users such as citizens, and mainly include the data transmission security from terminals to boundary security gateways, from boundary security gateways to application servers, from terminals to application servers, and between application servers. Also security can be promoted by security isolation and single-oriented transmission system.

Applied environment security can be implemented by interior application systems and servers, and by terminals of safely accessing the system.

V. THE KEY TECHNOLOGY OF THE SYSTEM

Applied key technologies on security authentication mechanism, multilevel privacy protection mechanism, super high frequency RFID, security cloud service,
security isolation and single-oriented transmission, and boundary security gateway protection will be discussed as follows.

A. Security Authentication Mechanism

According to eID security platform deployment above, security authentication mechanism of eID security platform can be described as shown in Figure 2.

![Figure 2. System security authentication mechanism.](image)

Issuance and authentication process includes three parties: Users, Service Providers and Public Key Infrastructure, and includes issuance process and authentication process.

Issuance process mainly includes: first, a public/private key pair is generated safely in the eID card; the user submit request contained public key and his identity information to eID management infrastructure also called public key infrastructure. After checking truth and uniqueness of the user, the public key infrastructure issues a digital certificate containing the public key and user’s eID associated with the identity in reality. Thus, the digital certificate encapsulated as digital envelop will be sent back to the user and written into the eID card. Also the service provider needs its server certificate from the public key infrastructure. Secondly, the user’s eID registration and validation will be completed between the user and the service provider.

Identity authentication process occurs between the user and the service provider by the handshake process when the user accessing information resources on application servers. The two-way handshake process will be promoted as follows without the public key infrastructure participating. As the user certificate is encrypted for privacy, the two-way handshake process is implemented by the extension of SSL handshake process comprised of two phases: one SSL channel is established through one-way SSL handshake process; then the service provider completes the user authentication and trust relationship is achieved consequently.

B. Multilevel Privacy Protection Mechanism

Mechanism of multilevel privacy protection can construct user privacy policy formulation and policy fusion mechanism to realize administrable and controllable function of user attribute privacy information issuing, as shown in Figure 3.

![Figure 3. The multilevel privacy protection mechanism.](image)

The user’s virtual business account binding with real identity can provide the account in application system with trusted token. But for assuring user privacy security, business account management system can’t see real identity information in the process of identity binding. And for many cyber business applications, it requires real identity information joining. So we can provide user attribute information for applications by attribute issuing process to assure business application system to operate regular.

After identity binding, the real identity service provider should assess the business type and the deploying security environment, and according to the formulated XACML attribute privacy policy, deciding to issue the attributes, attribute information proving, and provides the retrieval and issuing service of the user’s identity information for the business account service level by the cyber business application requirement. And the forbidden issuing attribute information can’t be seen by the account service level to realize the user attribute privacy protection. Also, attribute privacy policy should be constructed by assessing the account service level requirement and the deploying security environment and by the trusted party as the real identity administrator, thus, it can forbid the application system by cheating way to get the extra user attribute information and to use other way, which may lead to leakage of user privacy.

The user attribute assertion policy includes system policy and user prescribed policy. We can describe the policy as follows:

Policy::=⟨SP, UP⟩

SP::=⟨SAn, AWn, AMn>,…⟩ (n=1, 2 , …, m)

UP::=⟨UAn, AWn, AMn, ARn>,…⟩ (n=1,2,…,m)

Policy consists of system policy (SP) and user prescribed policy (UP).

The SP includes all kinds of attributes, the application ways (AW), and the assertion methods (AM) which will issue to all application systems and users.

In addition to all kinds of attributes, the application ways, and the assertion methods will issue to a specific application system or user. The UP allows users to specify attribute rules (AR) for different application system. We can note that only UP permits users to choose the attribute assertion to operate.
The user’s administrable and controllable attribute assertion can assure digital identity management platform only to provide attribute assertion results for the user’s privilege application system. And the application service provider requests some user attribute information after it finishes the mutual authentication with users and gets the user privilege and gives the attribute assertion to the digital identity platform. Safe attribute assertion assures application server not to fake the user privilege and also not to use the user privilege limitless, so as to assure the user privacy privilege.

On the other hand, for promoting the efficiency of the attribute assertion, forbidding the application service to get the attribute assertion every time from the eID information service platform, and lessening the pressure of the eID information service platform, system can choose some attribute information stored into the eID digital identity according to system policy and eID digital identity capacity, as shown in Figure 4.

![Figure 4. The users’ controllable attribute assertion (rapid mode).](image)

If the application service requires getting the attributes information, and the user eID includes the same attributes, the user can only provide the required attributes of the application service by privacy protection technology, and confirms the attribute authenticity.

C. Super High Frequency RFID

RFID includes tags, readers and antennas. The basic principles of RFID system includes as follows: Firstly, readers send certain frequency RF signals by antennas, then tags generate induced currents and are activated when they reach the workplace of the antennas; secondly, tags send their own codes information out through built-in antennas; thirdly, the antennas receive carrier signals sent by tags and sent to readers. Readers demodulate and decode signals, and then sent to the background of the main system; fourthly, the main system judges the legality of the card by logistic operation, carries out corresponding processing and control according to different settings, and sends out instruction signals to control the actions.

In addition, the super high frequency RFID can be achieved by two antennas independently operating and comprehensive analyzing and comparing to promote the identification ability. And the promoted readers and antennas can obtain the distance transmission and identification. So the super high frequency RFID can realize the transmission and identification of the users such as the distance beyond 25 meters and the moving speed as 180 km per hour. Thus, it can provide more convenient and efficient service for citizens according to the requirement.

D. Security Cloud Service

In the time with cloud technology, the cyber service has the peculiarity of application mode diversification, information platform incorporation, information node diversification, thus, we apply the cloud technology to the security service of the platform.

We adopt the cloud-based identity management and authentication technology with users as the center to have the advantage as follows: First, we assure users’ authenticity and validity as the first important action, and the official department named the Ministry of Public Security will become the identity audit organization. Second, we provide the cloud service in place of the middleware technology, and it can give all kinds of applications the trusted service with flexible policy and better privacy protection. Third, we consider the cloud service with trusted technology to support the identity management and authentication well.

According to the super huge scale users of the cyber identity eID management system, the security cloud service deploys plenty of authentication nodes, and assigns dynamically huge users’ request to promote the response time and reliability of the authentication service, and authentication is the self-governed security service, and the authorized personal users and enterprises (websites) can realize united identity authentication through the fixed access node. The architecture is shown as figure 5.

![Figure 5. The architecture of the security cloud service.](image)

The security cloud service comprises authentication data platform, authentication nodes, and authentication data interface.

The authentication platform includes the identity data of personal users and enterprise users, personal authentication nodes, and enterprise authentication nodes. And the authentication interface realizes the authentication protocols, and provides the authentication service for applications and users, and receives the authentication request and returns the authentication results. And privilege management nodes provide personal users’ identity privilege policy for application service providers (application websites), and the policy decides the obtained information of the application service provider of the user accessing after the user finishing the authentication.

The security cloud service supports the security authentication protocols as follows: the enterprise
(website) authentication protocol and personal user authentication protocol. And the enterprise (website) authentication service provides the users utilizing the enterprise (website) service with the real and legal proof of the enterprises (websites), and users can get the materials through hitting the icon of the objective website.

The personal authentication service based on eID provides the proof of the user real identity, and protects personal privacy from the objective websites. By the attribute service interface and the information issuing interface, the online applications such as E-Business and cyber amusement can finish the related eID applications of the united entity authentication, the entity identity management, and the information booking and reading.

E. Security Isolation and Single-oriented Transmission

The security isolation and single-oriented transmission is achieved by the light emitting diode, the light sensor, and two high efficient security data transmission cards, combining the data fault tolerant technologies of forward error correction, matrix redundancy check, and scrambling code transmission to implement the error control of data transmission. And the high efficient data transmission is completed through the universal processor and coprocessor, optimized and cut the operation system, communication protocols, and application processing logic.

The security isolation and single-oriented transmission technology, based on the security isolation and transmission technology, adopts the interior and outer security cards, and between that transmitting the information in the fiber channel. The outer security card has the light sending adapter, and the interior has the light receiving terminator. The light sending adapter can modulate the data signal sending required by the outer machine into the light signal, and sends in the fiber channel. The light receiving terminator of the interior security card can receive the light signal from the sending pole, and convert it into the data signal. And then commit it to the chip processor to further process, at last store the whole information into the interior machine cache, and at the same time inform the upper application to get.

The single-oriented transmission of the operation data implemented by the system, should get the files required single-oriented transmission from the outer application server to the system outer machine, and then handle the encapsulating data and fragment, and the outer security card transmit the information to the interior machine with binary streams bit by bit in the fiber channel. And the proxy programs of the interior machine will receive and combine the files, and send it to the file server in the interior machine network by the file transfer protocol. Not only the outer machine but also the interior machine will resolve data packets in application layer, and transmit the application data between the interior and outer machines.

F. Boundary Security Gateway Protection

The boundary security gateway system comprises the client subsystem and the server subsystem, and the client subsystem includes the client software subsystem, the hardware cipher subsystem, and the application client interface. And the server subsystem combines the server software subsystem, the hardware cipher subsystem, and the application server interface.

The client and the server should authenticate each other and implement the user’s identity authentication based on the digital certificate and the terminal’s equipment authentication based on the software and hardware features, and finish the keys exchange by the security communication protocols, and construct the security connection by the security encryption channel, and in real time and automatically detect the system kernel, the key process, and the storage area, and then form the comprehensive report, according to the security report and the security policy issued by the server system, implement the client network connection control, the application operation control, the terminal security monitoring, the application proxy, the input and output control, etc, and at last finish the interaction with the background application, the PKI/PMI system, and the security administration and audit system.

The boundary security gateway can implement the mandatory identity authentication, the privilege access control, and transmission protection.

The identity authentication realizes the identification of the users and terminals. Terminal authentication can be achieved based on the features such as the operation system, IP, MAC, CPU, hardware serial. The terminals, connected with the protection and control systems of boundary security, register in the security administration and audit system, after audited and information will automatically be sent to the boundary security gateway. And the terminals unregistered or unaudited can’t access the protection and control systems of boundary security and the internal information resource by the boundary security gateway. The user authentication should be implemented with the mutual authentication based on the hardware certificate and the PKI technology, and the certificate should be issued by the public key and privilege infrastructure of the systems.

The privilege access control will mainly be realized at the network and application layers. The link access control is achieved based on the 802.1x protocol, and the unauthorized end node will be forbidden to connection with the systems. The network control of the end node will be implemented based on the condition detection firewall technology. The application access control will be realized according to the authentication and administration policy of the security administration and audit system, and based on the certificate Role-and-Attribute-Based Access Control model of the digital signature with the PKI technology. And the access control regulation can be denoted as four element objective: user-role-attribute-privilege.

The transmission protection will be implemented between the boundary security gateway and terminals, and based on the IPSec protocol or SSL protocol, to assure the privacy and integrality of information transmission.
VI. DISCUSSION

A. Efficient Security Service

Because of the huge user numbers in China, the efficient security service is one key point. In spite of the cloud service technology adopted, the service efficiency can be promoted well, more new technology such as high speed computing and retrieving technology should be considered. That is, all related high speed ways should adopted to advance the efficiency of the cloud security service with the development of scientific technology deeply.

B. Potent Privacy Protection

The convenience and security are both very important, especially personal privacy protection becomes more focused on. The security policy and security authentication protocols are considered in the platform, but the new security method should be traced all the time to defend the privacy leaking.

C. Potential Safe Threats for eID

As one key security infrastructure of the Internet of Things, some potential safe threats as follows may exist during the functioning of the eID system:

1) Inappropriate authorization or delegation: As no combination with citizen’s bio-information in the eID card, the eID card may be held by other person.

2) Loss or theft: Once the eID card is lost or stolen, the identity of the citizen will be at serious risk. But the citizen can use a PIN to protect the eID card, thus the risk can be reduced.

The above threats are hard to defend, thus, administrative methods, such as giving laws to punish this criminal, may deal with it.

D. No Bio-information Used in eID

According to the Internet of Things, an intuitive idea is to use bio-information of the citizen in the eID card. For example, Germany stores citizens’ fingerprint in EU passports, and uses biometric templates rather than pictures to protect the real fingerprint [10]. Even, we can inject the ID into the body of citizens to realize tight link between the citizen and the ID.

It can’t use the above methods while considering the personal privacy and deployment issues. If the eID contains the citizen’s bio-information, the loss and theft issues will hardly be dealt with.

Bio-information is the unique information for the citizen and hard to change. Thus, once the eID card is held by malicious users, the critical bio-information will be at risk. In addition, it can’t inject our eID into the body of citizens because it is hard to operate in the large scale in China. As a result, there is no bio-information used in eID.

E. System Security Administration

Because of all kinds of potential threats such as the eID card held by other persons, system security administration also should be attached important to. That is, except the main technologies, we should research many rules and specifications and standards, even some laws to support the system running more correctly.

VII. CONCLUSION

The paper presents RFID-based electronic identity security cloud platform in cyberspace to realize efficient security management of personal cyber identities, and designs the implementation framework of pervasive security platform, and discusses key technology including security authentication mechanism, multilevel privacy protection mechanism, super high frequency RFID, security cloud service, security isolation and single-oriented transmission, and boundary security gateway protection, and it can broadly apply to citizens’ identity management with virtual roles in all kinds of circumstances of Internet of Things such as E-Government and E-Business, and the electronic identity security cloud platform has been primary implemented and achieved good effects in actual applications such as new social assured cards system in Shanghai to provide safer and more convenient services of Internet of Things.

ACKNOWLEDGMENT

The research work was sponsored by the National High Technology Research and Development Program of China 2008AA01Z412, and the National Development and Reform Commission Program of China [2010]3044.

REFERENCES


of information network security, Ministry of Public Security, China, and has earned the research fellow position. And he also has earned the research fellow position in University of Tokyo, Japan, and Tongji University, China.

Prof. Tan got five awards of the progress prize in science and technology in China, and has published more than fifty theses in periodicals, magazines, and conference all over the world recently.

Bo Jin was born in 1972, Zhejiang Province, China, earned the doctor’s degree from East China University of Science and Technology in 2000, and majored in automation control and project application technology.

He has worked in the 3rd research institute of ministry of public security, Shanghai, China, from 2005, and researches about the network security and application, and becomes the headmaster of the key laboratory of information network security, Ministry of Public Security, China, and has earned the research fellow position.

Dr. Jin got five awards of the progress prize in science and technology in China, and has published more than thirty theses in periodicals, magazines, and conference all over the world recently, and has held and joined many large projects from 2000.

Xiang Zou was born in 1977, Anhui Province, China, earned the doctor’s degree from Chinese University of Science and Technology in 2004, and majored in automation control and project application technology.

He has worked in the 3rd research institute of ministry of public security, Shanghai, China, from 2004, and researches about the network security and application, and becomes the associate headmaster of the key laboratory of information network security, Ministry of Public Security, China, and has earned the associate research fellow position.

Dr. Zou got three awards of the progress prize in science and technology in China, and has published more than twenty theses in periodicals, magazines, and conference all over the world recently, and has held and joined many large projects from 2004.

Yuebo Dai was born in 1978, Jiangsu Province, China, earned the bachelor's degree from Southern Yangtze University in 2002, and majored in computer science and application technology, and became the master graduate student in software engineering school of Huazhong University of Science and Technology.

She has worked in the 3rd research institute of ministry of public security, Shanghai, China, from 2011, and researches about the network security and application, and has earned the middle research fellow position.

Ms. Dai has published more than ten theses in periodicals, magazines, and conference all over the world recently.

Bing Chen was born on October 19th, 1978, in Wuhan, China, and earned the bachelor’s degree from Wuhan University in 2000, and earned the master’s degree from Wuhan University in 2003, and both majored in computer science and application technology, and became the doctor graduate student in computer science and application technology school of Tongji University in 2010.

He has worked in the 3rd research institute of ministry of public security, Shanghai, China, from 2003, and researches about the network security and application, and becomes one super researcher in the key laboratory of information network security, Ministry of Public Security, China, and has earned the associate research fellow position.

Dr. Chen got the second award of the progress prize in science and technology honored by Ministry of Public Security, China, in 2009, and has published more than twenty theses in periodicals, magazines, and conference all over the world recently, and has held and joined many large projects from 2003.

Chengxiang Tan was born in 1965, Hubei Province, China, earned the doctor’s degree from Northwestern Polytechnical University in 1994, and majored in computer science and application technology.

He has worked in computer science and application technology school of Tongji University in Shanghai, China, from 1994, and researches about the network security and application, and becomes one super expert in the key laboratory of information network security, Ministry of Public Security, China, and has earned the research fellow position. And he also has earned the research fellow position in University of Tokyo, Japan, and Tongji University, China.

Prof. Tan got five awards of the progress prize in science and technology in China, and has published more than fifty theses in periodicals, magazines, and conference all over the world recently.

Bo Jin was born in 1972, Zhejiang Province, China, earned the doctor’s degree from East China University of Science and Technology in 2000, and majored in automation control and project application technology.

He has worked in the 3rd research institute of ministry of public security, Shanghai, China, from 2005, and researches about the network security and application, and becomes the headmaster of the key laboratory of information network security, Ministry of Public Security, China, and has earned the research fellow position.

Dr. Jin got five awards of the progress prize in science and technology in China, and has published more than thirty theses in periodicals, magazines, and conference all over the world recently, and has held and joined many large projects from 2000.