Cluster Computing (2019) 22:S451–S468
https://doi.org/10.1007/s10586-018-2516-1

Information security model of block chain based on intrusion sensing in the IoT environment

Daming Li[1,2,3] · Zhiming Cai[4] · Lianbing Deng[5,6] · Xiang Yao[6] · Harry Haoxiang Wang[7,8]

Received: 29 November 2017 / Revised: 7 March 2018 / Accepted: 12 March 2018 / Published online: 30 March 2018

Abstract

Block chain is a decentralized core architecture, which is widely used in emerging digital encryption currencies. It has attracted much attention and has been researched with the gradual acceptance of bitcoin. Block chaining technology has the characteristics of centralization, block data, no tampering and trust, so it is sought after by enterprises, especially financial institutions. This paper expounds the core technology principle of block chain technology, discusses the application of block chain technology, the existing regulatory problems and security problems, so as to provide some help for the related research of block chain technology. Intrusion detection is an important way to protect the security of information systems. It has become the focus of security research in recent years. This paper introduces the history and current situation of intrusion detection system, expounds the classification of intrusion detection system and the framework of general intrusion detection, and discusses all kinds of intrusion detection technology in detail. Intrusion detection technology is a kind of security technology to protect network resources from hacker attack. IDS is a useful supplement to the firewall, which can help the network system to quickly detect attacks and improve the integrity of the information security infrastructure. In this paper, intrusion detection technology is applied to block chain information security model, and the results show that proposed model has higher detection efficiency and fault tolerance.

Keywords Internet of things · Intrusion detection · Block chain · Information security · Model building · Technical analysis

1 Introduction

With the development of mobile Internet technology and the arrival of big data era, the supply chain logistics management has attracted much attention, and its development cannot be separated from the capital flow, information flow, flow of people and so on. Bitcoin was introduced in 2008, bitcoin digital currency encryption system began to enter the financial and other fields, block chain came into being. In October 2016, the application of block chain technology has extended to many fields such as internet of things, intelligent manufacturing, supply chain management and so on. Block chaining technology is regarded as the rudiment of the next generation cloud computing [1–3].

At present, the block chain has not formed a unified definition. Satoshi points out that the chain of blocks is maintained, managed and supervised by each node of the network, and has the characteristics of decentralized and

✉ Harry Haoxiang Wang
hw496@goperception.com

[1] The Post-Doctoral Research Center of Zhuhai Da Hengqin Science and Technology Development Co., Ltd., Hengqin, China

[2] City University of Macau, Macau, China

[3] International Postdoctoral Science and Technology Research Institute Co., Ltd., Wuhan, China

[4] Macau Big Data Research Centre for Urban Governance, City University of Macao, Macau, China

[5] Huazhong University of Science and Technology, Wuhan, China

[6] Zhuhai Da Hengqin Science and Technology Development Co., Ltd., Hengqin, China

[7] Cornell University, Ithaca, NY, USA

[8] GoPerception Laboratory, New York, NY, USA

Trustless. Block chain technology is a relatively recent technique of fire, it is accompanied by bitcoin gradually into the people's vision, while mentioning the block chain people will often think of bitcoin, but in fact the blockchain is not equal to bitcoin, it just bitcoin is the underlying technology, construction technology based bitcoin trading network and chain blocks information encryption. Block chain based on the principle of cryptography rather than on credit, both sides agreed to make any payment directly, do not need the participation of the third party intermediary, but bitcoin is a successful application of the block chain, but it is not equivalent to the block chain.

In essence, the block chain is a secure, trusted, and decentralized distributed database, or it is a distributed account book that records all transactions. The unprecedented security and credibility of the block chain as a landmark application technology, of course, has become a universal structure of digital currency (Fig. 1).

Block chain technology is not a single technology integration and innovation, but a variety of techniques, including mathematics, cryptography, algorithms and economic model technology, these technologies with new structure combined together to form a new data record, store and express way. The core technology of block chain technology mainly includes the following aspects.

A block chain is formed by chaining together data blocks, consisting of Header and Body. Big area including the current version number, hashPrevBlock, the current block target hash value (Bits), random number current block consensus process (Nonce), Merkle root node hash value (hashMerkleRoot) and Timestamp.

HashMerkleRoot is a numeric value computed by hash values of all transactions in the block body, primarily for checking whether a transaction exists in this block. The block body includes the number of transactions in the current block and all transaction records that occurred during the validation of the block creation. These records generate a unique Merkle root through the hashing process of the Merkle number and log into the block size.

Trust based block chain ownership is mathematics, with non-symmetric encryption algorithm to guarantee transaction data security, each node has a private key and a public key, private key only the nodes have the public key, open to all the nodes in the P2P network. When the transaction is sent, it is encrypted with a private key, and the receiver is decrypted with the sender's public key.

Accounting transactions completed jointly by the distribution of the number of nodes in the different places, each node records all transactions recorded in the network, so they can participate in the legal supervision of the transaction, can also be common for a transaction. Since the accounting nodes are large enough, in theory, the accounts will not be lost unless all nodes are destroyed, thus ensuring the security of the data of the accounts.

The block chain adopts distributed accounting, distributed communication and distributed storage, which ensures the data storage, transaction verification and information transmission in the system, all of which are centralized.

The consensus mechanism is how to reach a consensus among all nodes in the network and determine the effectiveness of a transaction. It is both a means of identification and a means of tamper proofing. The block chain proposes 4 different consensus mechanisms: workload certification (PoW), equity Certificate (PoS), authorization share certificate mechanism (DPoS) and authentication pool (Pool). These 4 consensus mechanisms are applicable to different application scenarios, such as the workload proof mechanism used in bitcoin. Powerful computing capability of proof of work to ensure the safety of the block chain and not tampered with, any block of data tampering attack or must recalculate the block and the workload of all subsequent blocks, only in the control of the whole network nodes more than 51% of the cases, the system can produce

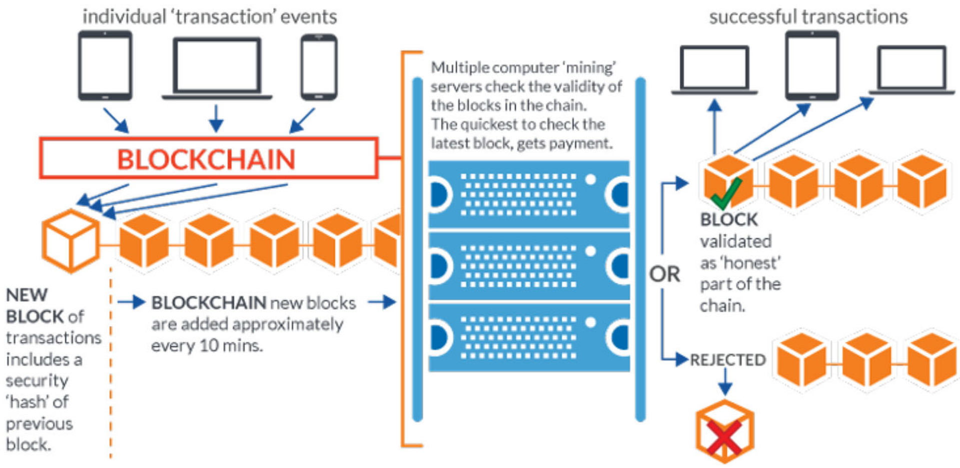

individual 'transaction' events
BLOCKCHAIN
NEW BLOCK of transactions includes a security 'hash' of previous block.
BLOCKCHAIN new blocks are added approximately every 10 mins.
Multiple computer 'mining' servers check the validity of the blocks in the chain. The quickest to check the latest block, gets payment.
OR
successful transactions
BLOCK validated as 'honest' part of the chain.
REJECTED

Fig. 1 Bitcoin as a successful application of block chain

a there are records, and the calculation speed must be forged chain length than the backbone, this attack will lead to the difficulty of far more than the cost of revenue.

The contract is a kind of intelligent protocol, it adopts programming language (script) rather than legal provisions, credible, do not tamper with the data based on the system a chance to deal with some unexpected trading patterns. When the agreed conditions are met, the system automatically implements predefined rules and terms [4–6] (Fig. 2).

Block chain is divided into three categories: public block chain, private block chain, and union block chain. The public no organization, no official block chain management mechanism, no central server, the world any individual or group can be used as the node according to the rules of free access network system, out of control, any node can send the transaction, and the transaction can obtain the block chain effective confirmation, anyone can participate in the consensus process. The public block chain is the earliest block chain, and is also the most widely used block chain at present. The digital currency of the major bitcoin series is based on the public block chain [7–9].

The private block chain is owned by the company or individual, and the system operating rules are set according to the company or individual requirements. Read and write access is limited to a few nodes, but only using the block chain general ledger technology for billing, which is not very different from other distributed storage schemes.

The union block chain is between the public block chain and the private block chain, and a plurality of preselected nodes are designated as accounting persons within a group. The generation of each block is determined by all the preselected nodes. The pre selected nodes participate in the consensus process, and other access nodes can participate in the transaction, but do not interfere with the accounting process. Anyone else can do a qualified query through the open API of the block chain.

Block chain consists of many nodes to form an end-to-end network, and there is no centralized device or management mechanism. The rights and obligations of any node are equal, the data exchange is verified by digital signature technology between the nodes, without the need to trust each other, as long as the system in accordance with the established rules, not between nodes cannot deceive the other nodes, and the damage to or loss of any node will not affect the operation of the whole system. Robustness, to the center of the structure has an excellent block chain system at the same time, the structure to the center can greatly improve the efficiency of the system, and greatly reduce operating costs.

Block chain system is open, in addition to the parties to the transaction's private information is encrypted, open for all data blocks in the chain, anyone can participate in the block chain network, you can open the query interface block chain data and the development of related applications, each device can be used as a node. Each node has a complete copy of the books distributed database, so the system is highly transparent information. Bitcoin as the

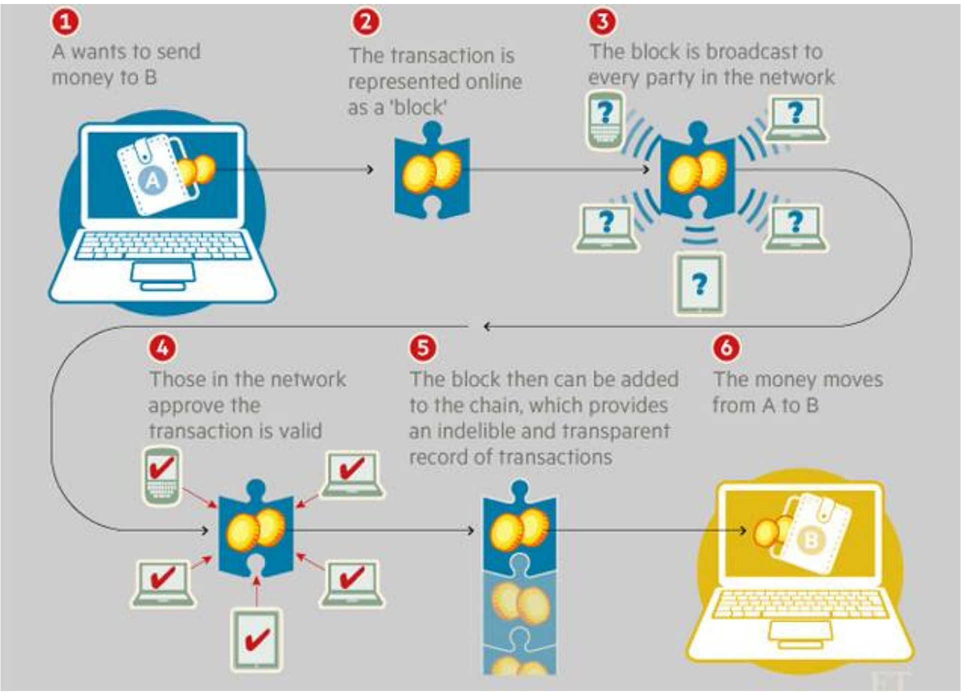

1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B
FT

Fig. 2 How a block chain works

representative of digital currency in the transaction verification of the characteristics of centralized and collective participation is the decisive factor for open and transparent distribution books. The transmission of value in bitcoin networks does not depend on a specialized third party mechanism, and each transaction is shared by all miners, accounting for one random miner.

The blockchain trust relationship established by pure mathematical methods, transaction data encryption/decryption through non symmetric key algorithm, added to the main chain in each transaction, will run the complex hash algorithm of transaction data, transaction identity and transaction history based on the results, in order to ensure the correctness and security of transaction. Each node stores all the transaction data, the attacker is unable to change the history of transactions, so that all nodes can exchange data freely and safely in trusting environment, makes the trust of the people to trust the machine, any human intervention has no effect. In a digital currency network represented by bitcoin, all participants have their own stock backups, and the accounts remain synchronized in real time, and data that has been validated and recorded cannot be tampered with.

Once the data is validated and added to the block chain, will be permanently stored, unless it can also control more than 51% of the nodes in the system, or a single node changes to the database is meaningless, so the data stability and high reliability block chain. Each transaction in the block chain is linked in series with two adjacent blocks by cryptography, so we can trace back to any transaction record of transaction costs.

The operation rules and data information of block chain are open and transparent, and the data exchange between nodes follows a fixed algorithm, and the data interaction needs no trust. Therefore, the node does not need to open identity, so that the other side of their own confidence, each node involved is anonymous, greatly protect the user's privacy.

2 Internet of things environment

2.1 Introduction to internet of things

The internet of things is intuitively an Internet connected goods, as well as a product of the next generation of networks and the internet. As the research on internet of things has not yet been done at home and abroad, both academia and industry do not fully understand the intrinsic nature of internet of things, and lack the knowledge of the complexity of internet of things. The Internet is a new stage based on Internet based ubiquitous network development, it can be through a variety of wired and wireless networks and Internet integration, comprehensive application of mass sensor, intelligent terminal, global positioning system, to achieve things and things, things and people everywhere to realize intelligent management and connection. Control. Things to lead the third wave of the information industry revolution, will become the future social and economic development, social progress and technological innovation is the most important infrastructure, but also to the country in the future some of the physical facilities safety use and control [10].

Although the internet of things is developing rapidly, the security of internet of things is becoming more and more prominent. A typical case is the Stuxnet virus, it is the first infrastructure attacks in industrial control of the virus, the virus in the form of worms in Internet diffusion, and focus on the diffusion to the U disk, once the mobile media into the industrial control network, for the SIEMENS WINCC system and infect them, once infection, can in the PLC administrator without detection, send to PLC or modify data returned from the PLC. The virus attacked Iran in Natanz uranium enrichment plant, causing about 20% of Iran's centrifuge control, scrap, lead to power delay. A series of Internet information breaches at the end of 2011 showed that the threat of information security is much more serious than many of us think.

The internet of things is a major change in the field of information technology. It is considered the third wave of information industry after the computer, Internet and mobile communication network. The Internet is the extension and expansion on the basis of the Internet network, through information sensing equipment, in accordance with the contract agreement, to anything connected with the Internet, information exchange and communication, to achieve a network intelligent identification, positioning, tracking, monitoring and management. The basic characteristics of internet of things are comprehensive perception, reliable transmission and intelligent processing of information. The core of internet of things is the interaction between objects and objects and information between human beings and objects [11, 12].

2.2 The framework of the internet of things

The internet of things model of three views proposed by Atzori et al. only integrates and analyzes the existing internet of things systems and technologies, which does not involve the essential issues and core technologies of the internet of things. The essence of the internet of things must be explored from the point of view of the integration of virtual network world and the physical world. The internet of things is essentially an inevitable product of the integration of the virtual information network world and the physical world. The internet of things (IOT) is a general term of the actual available systems that are integrated with the virtual world. CPS is only one of the key technologies for the integration of the virtual and the real world. In real and virtual world integration of key technologies, including CPS and front end item identification and information collection and information technology related materials, as well as the semantic CPS and the rear end of the physical space and time processing semantic related physical network system (PCS) technology. The integration of the virtual and the real world must involve a range of social, economic, legal and privacy concerns. For example, how the monetary system of the virtual world relates to the monetary system of the physical world, and how the legal system of the physical world extends into the virtual world. From this we can see that the conceptual model of internet of things based on the integration of the virtual world and the physical world can touch the essence of the internet of things (Fig. 3).

2.3 Public internet of things and special internet of things

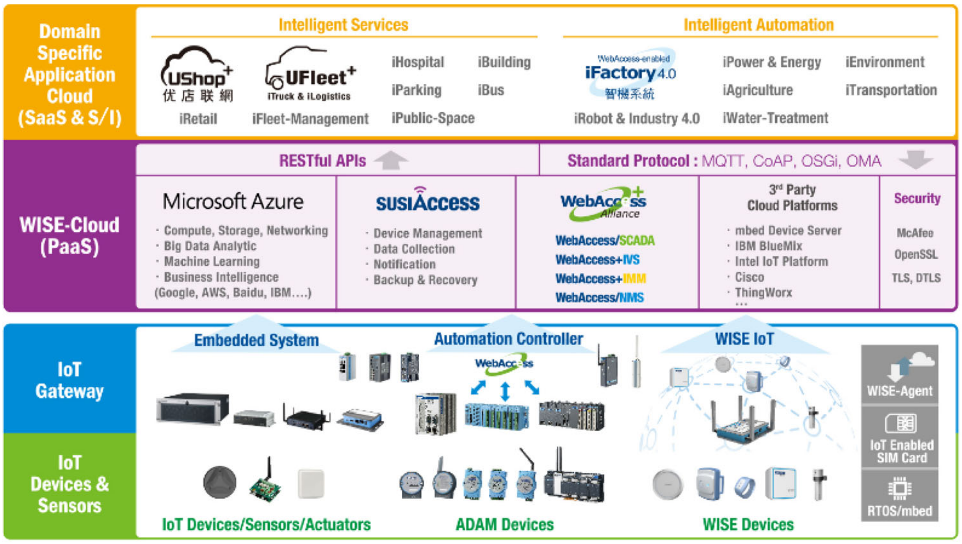
The internet of things can be divided into the public internet of things and the special internet of things. The public internet of things refers to the internet of things that connects all the goods, covers a social administrative area, and connects with the public internet. The internet of things refers to the internet of things that connects certain specific objects, covers a particular organization area, and serves as a special purpose within the organization.

Public IoTs must include public networking system and public networking technology system, public IOT system needs a standard, including goods identification technology standard system and standard system of goods information transmission technology, data processing and goods and services technical standard system. Smart city, the wisdom of the earth belongs to the public internet of things, all need a public networking technology system support, forming a public internet of things system.

Special IoTs can include special networking system and IOT system, special things can be constructed for a specific application of standard technology system, including goods identification, goods and goods information transmission, data processing and service technology system. From the point of view of expansion, the internet of things is best referred to the standards of public internet of things. However, the primary stage of network development in the special development of things inevitably leading the development of networking technology in the public, private networking standards may not be made public networking technology adoption system, so, specific for the early development of the Internet technology could be eliminated by technology. Wisdom, wisdom, wisdom campus plant hospital, smart shopping, wisdom warehouse is some special typical networking system, these things the current system is unable to realize the interconnection, intercommunication and interoperability, this is a limitation of the special IOT itself which, because of the limitation of these special things cannot have all the characteristics of things, most special things do not need to have all the characteristics of the internet of things.

Special IoTs can achieve coverage nationwide, according to an application domain objects connected to the network, the special things can also provide related information services through the Internet, such as the international transfer of the company through the logistics network, the Internet can provide quick query a current arrival position service. However, different internet of things cannot achieve interconnection and interoperability, cannot constitute the entire social needs of the internet of

Fig. 3 IBM model of the Internet of Things



things system. Therefore, only the public internet of things can serve as an infrastructure for information society and play a role similar to that of the internet.

The public internet of things can build an interconnection infrastructure for all kinds of dedicated internet of things, and can also build a public technology platform for the internet of things. Only the public technology platform can form the industrial chain, in order to promote the development of an industry. Therefore, to pay attention to the research and development of public internet of things, in order to bring the development of animal networking industry (Fig. 4).

2.4 Conceptual model of internet of things

The conceptual model of the internet of things is the basis for understanding and further studying the internet of things. The objective concept model of internet of things will guide the theoretical research and technological development of the internet of things with practical value.

In the last 20 years of the twentieth Century, human society created a virtual network world with the development of network and information technology. The human society has already can use the virtual world, to achieve online dating, online shopping, online games, online office, online booking, online education, online warehouse management, online power scheduling, online production control, online traffic monitoring etc. But some virtual world activities must rely on the physical world, for example, online shopping must depend on the support of the real-world logistics system. Some human society activities must depend on the real-time interaction between the virtual network world and the physical world, such as online storage management, online power transfer, and online production control. The separation of virtual network world from the real physical world will inevitably hinder the development of virtual network world.

NIT development has put forward the integration of the network world and the physical world. In the past ten years, the industry has put forward the combination of informatization and industrialization. This combination has not only injected vitality into the development of traditional industries, but also brought new opportunities for the development of Internet and information technology. The development of NIT will inevitably extend the scope of application to the physical world, and will apply the Internet technology, which focuses on network and information technology, to the connection of objects in the physical world. So, naturally have the demand of IOT research and achieved remarkable results in warehousing and logistics management and other aspects of the networking application, the strategic thought of development of these studies prompted the International Telecommunication Union proposed in 2005.

The internet of things was originally researched from the point of view of connecting objects, and naturally the technology of networking with things as internet of things technology. The first technique items of networking is the items of information identification, the information identification technology is the most mature and widely used is the radio frequency identification (RFID) technology, it has been widely used in warehousing and logistics. Sensor network technology for object perception is classified naturally in the internet of things technology because of its ability to identify and perceive objects.

Many applications of traditional embedded technology are to reside in man-made objects, and are often classified as internet of things technology. Thus, there is a misunderstanding between academia and industry. It seems that all the information technologies belong to the internet of things technology, and the internet of things technology can include all the information technology. Some scholars have concluded from these one-sided understanding that

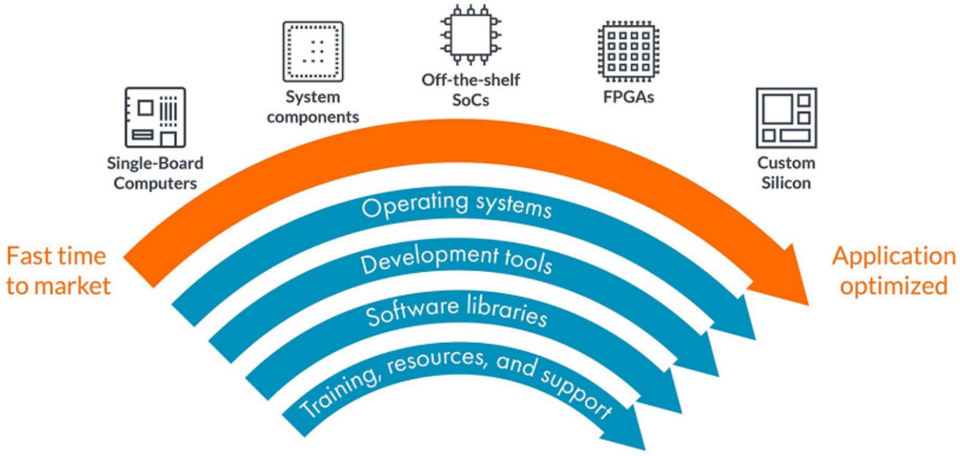


Fig. 4 Built from the ground up for internet of things applications and battery operations

the internet of things has no special technology, but only the integration of existing technologies.

2.5 Conceptual model based on world integration

The integration of the network world and the physical world involves three levels: the technology layer, the social layer and the system layer. The technical level mainly involves some things related technologies, such as RF, ID, CPS and other sensor networks; social aspects mainly refers to network world and the physical world of social, economic and legal integration and privacy protection related problems; system level relates to the network world and the physical world specific integration system, such as smart traffic system, smart grid, intelligent system Home Furnishing system, smart city, smart campus.

From the physical world and the Internet world integration perspective, technology related to technology can be divided into items of information technology, which is representative of the information technology is the material technology; the items of information sensing and articles control technology, which has the characteristics of networking applications is the technology of network physical system; the items of information transmission, processing and this is the decision technology, the existing Internet does not have the technology, is a virtual network processing technology for the physical world, can be called network technology for physics.

From the point of view of the integration of the physical world and the Internet world, the internet of things systems, such as intelligent transportation systems, smart grid systems, smart cities, are all two specific systems that are integrated into the world. The networking system is only the physical world and the network world fusion one side, only from the network point of system is difficult to truly understand and grasp the essential connotation of IOT and core technology. Because the internet of things is now the result of a fusion between the physical world and the Internet world, it belongs to the image of two world integration. The integration of the two worlds involves a range of unique technologies, because the internet of things involves two technologies that integrate the world, such as PCS technology, CPS technology, information materials technology, and so on (Fig. 5).

2.6 Internet of things architecture

The network architecture studies the components of the network and the relationships among these components. Different network architectures can be divided according to the different network systems that researchers are concerned about. For example, the functional hierarchical architecture of the network can be obtained from the point of view of the functionality of the network. From the point of view of network management, network management architecture can be obtained.

The internet of things itself is a system of three dimensions. These three dimensions are information goods, autonomous networks and intelligent applications. The independent network said this kind of network has self-configuration, self-healing, self-optimization, self-protection ability, the intelligent application of intelligent control and processing ability has said this type of application, the information items said these items are marked or can sense its own information. The function of the three dimension of the internet of things is the traditional network system does not have the dimensions (including independent network dimensions) network connection items, but must have the dimensions, otherwise, things will not be able to meet the needs of the application.

The overlap of three functional components, namely, information items, autonomous networks and intelligent applications, is the internet of things (IOT) systems with the characteristics of the internet of things, which can be called the infrastructure of internet of things. In the real world, there is no internet of things system, and the internet of things is just a group of network systems that connect objects, such as intelligent transportation systems, smart grids, and smart cities, and can be collectively referred to as the internet of things. The networking infrastructure here means the support system services in specific networking systems, can provide articles including identification, feature space location and item data validation and privacy protection services in different application areas, this part of the core of the public internet of things.

The internet of things is a network of things that cannot be described by a single hierarchical structure of the traditional network architecture. The internet of things first needs to include the functional dimension of the goods, which is the dimension that the traditional network does not have. Things connected to the internet of things can be called “information goods”. The basic functions of these objects include: electronic identification, and the ability to communicate information. The autonomous network is the advanced form of the network. Once it is not self configuring, self-healing, self optimizing and self protecting, it will be simplified into a general network and can be described by a hierarchical network model [13].

Intelligent applications can be simplified into general network applications if they are processed entirely through the human–computer interaction interface [14]. If the internet of things is no longer directly connected to the object, but through the man–machine interface to enter the information of goods, then it will no longer need to identify items and automatically convey the information of goods.

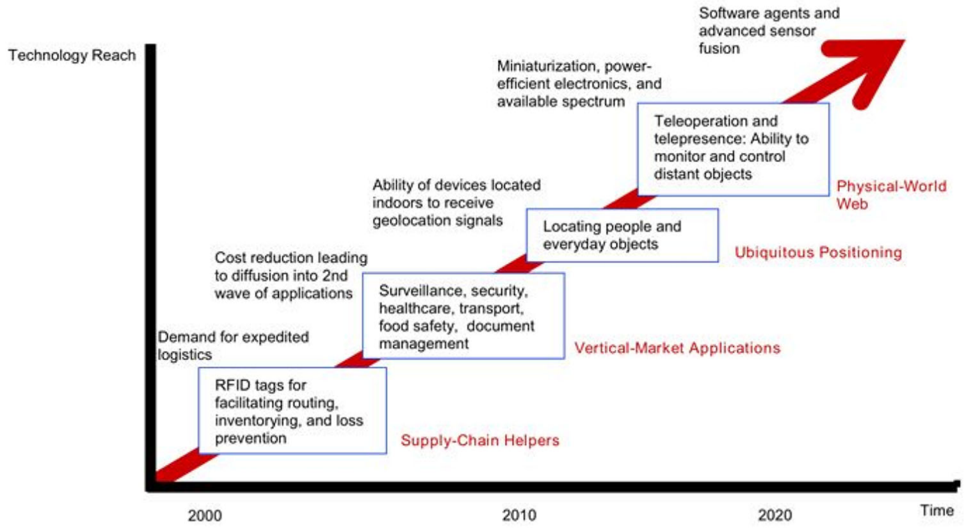

Technology Reach
Software agents and advanced sensor fusion
Miniaturization, power-efficient electronics, and available spectrum
Teleoperation and telepresence: Ability to monitor and control distant objects
Physical-World Web
Ability of devices located indoors to receive geolocation signals
Locating people and everyday objects
Ubiquitous Positioning
Cost reduction leading to diffusion into 2nd wave of applications
Surveillance, security, healthcare, transport, food safety, document management
Vertical-Market Applications
Demand for expedited logistics
RFID tags for facilitating routing, inventorying, and loss prevention
Supply-Chain Helpers
2000
2010
2020
Time

Fig. 5 Technology roadmap: the internet of things

In this way, the internet of things can be simplified into a general network system and can be described by a modern network hierarchy (Fig. 6).

Using the 3D architecture model of internet of things, we can analyze and evaluate the characteristics of an internet of things, and we can judge whether a network system belongs to the internet of things. For example, a network system only connects and perceives objects, but does not have intelligent applications, and this does not belong to a complete internet of things. Therefore, the sensor network does not belong to a complete internet of things. It only has the characteristics of information goods and autonomous networks [15].

3 Intrusion detection technology

3.1 Introduction of intrusion detection technology

Intrusion detection is an important way to protect the security of information systems. It has become the focus of security research in recent years. This paper introduces the history and current situation of intrusion detection system, expounds the classification of intrusion detection system and the framework of general intrusion detection, and discusses all kinds of intrusion detection technology in detail. With the rapid expansion of network connections, more and more systems are threatened by intrusion attacks. Therefore, the security of the computer system, the network system and the whole information infrastructure has become a pressing problem. In addition to the traditional firewall isolation technology, another important technology and research direction in security field is intrusion detection.

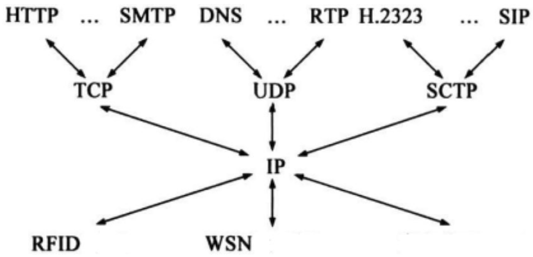


Fig. 6 Sketch map of communication protocol of IOTs

Information is one of the most valuable wealth, and the security of information system is a critical social problem, and intrusion detection is an active and important field of network security research. Research on intrusion detection can be traced back to 1980s, Aderson first proposed the concept of intrusion detection. In 1987, Denning proposed a classic intrusion detection model. Firstly, the concept of intrusion detection was proposed as a security defense measure of computer system. Then with the application of network technology, malicious attacks become more complicated and diversified, the intrusion detection technology in the rapid development accordingly, the current intrusion detection technology has become a research hotspot in the field of information security. The overall development of the intrusion detection system has gone through several stages: host based intrusion detection system and intrusion detection system based on network, the distributed intrusion detection system DIDS, and for large scale network intrusion detection system [16, 17] (Fig. 7).

3.2 Classification of intrusion detection systems

Intrusion is defined as any set of activities that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusion is usually divided into six categories:

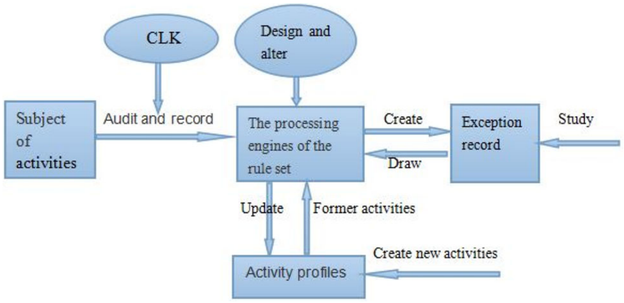


Fig. 7 Intrusion detection system

attempted intrusion, masquerade attack, security control system penetration, leakage, denial of service, and malicious use. Intrusion detection is defined as the process of identifying unauthorized people who use computer systems and who have legitimate rights to use the system but abuse privileges. The system developed for this purpose is called intrusion detection system [18].

3.3 Common intrusion detection framework

Anomaly intrusion detection refers to the establishment of a normally description file system for monitoring, any violation of the described events are considered to be suspicious, the observation activities deviate from the normal usage of the system level. Anomaly detection assumes that all intrusion are abnormal, that is to say, if we can establish a normal behavior to the file system, so in theory, it can mark the system state and all the file has been created for different intrusion attempts. However, the actual situation may be that the set of intrusions and the set of anomalous activities are just the same.

Abnormal intrusion detection based on statistical model, which is also called operation model, is to set a threshold for the number of events in a certain period of time. Once it exceeds the value, there may be an abnormal situation. The definition of anomaly threshold setting is too high, will lead to a false negative error, false negative error has serious consequences, it is not only not to detect intrusion, but also to the security administrator with a false sense of security, this is a side effect of IDS. But the definition of anomaly threshold is low, will lead to false positive judgment unbearable, false positive too much reduces the efficiency of the intrusion detection method, and will add security administrator's burden, this is because the security administrator must investigate every positive event. For example, in a given period of time, the number of password failure exceeds the set threshold, it can be considered an intrusion attempt (Fig. 8).

3.4 Mean and standard deviation model based intrusion detection

The first n observed events are denoted as follows:

$$x = \{x_1, x_2, \ldots, x_n\} \tag{1}$$

Therefore, the mean value and standard deviation can be calculated as follows:

$$mean = \frac{x_1 + x_2 + \cdots + x_n}{n} \tag{2}$$

$$stdev = sqrt\left(\frac{x_1^2 + \cdots + x_n^2}{n+1} - mean^2\right) \tag{3}$$

For a new observed event, which is denoted as x_{n+1}, if it falls beyond the confidence region $(mean \pm d \cdot stdev)$, it is considered to be anomalous, where d is the standard deviation mean parameter.

This model can be applied to the event counter, interval timer and resource metrics, it has the advantage of being able to dynamically learn about the knowledge of normal events, and shown by the confidence interval of the dynamic change. If the weights are assigned to the observed data, the closer the data weights, the better the dynamic learning ability of the model.

3.5 Intrusion detection based on multivariate model

This model is an extension of the average and standard deviation model, which is based on the correlation of two or more metrics, rather than the mean and standard deviation model, which is strictly based on a metric. Obviously, the combination of multiple correlation measures, not just a metric to detect abnormal events, which has higher accuracy and resolution.

Markov process model based intrusion detection regards event as a state variable, and then use the state transition matrix to depict the migration frequency between different states, rather than the individual state or the frequency of audit records. If the observed new event is too low for a given prior state and matrix, it is considered an abnormal event. The advantage of the model is that unusual commands or event sequences can be detected instead of single events.

Clustering analysis based intrusion detection represents the flow of events by using vectors, and then use clustering algorithms to classify them into behavior classes. Each class represents a similar activity or user's behavior, so that normal and abnormal behavior can be identified.

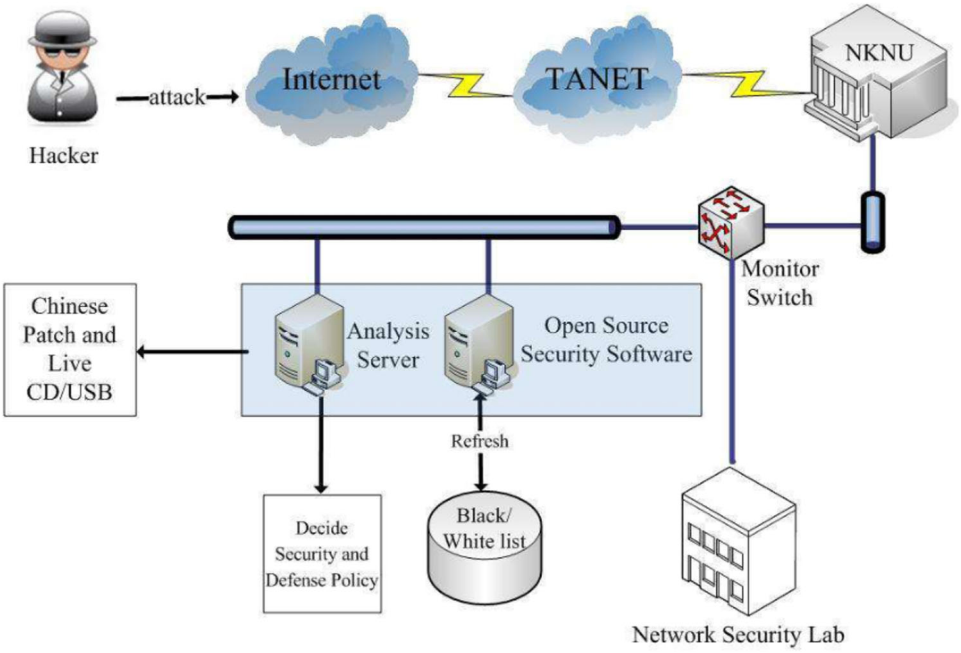


Fig. 8 The process of intrusion detection

Unsupervised clustering intrusion detection method without the need of training set standard and strict filtering, but also in the real network data to detect the unknown intrusion also has a good effect, so the algorithm has wide application prospect in the field of intrusion detection.

Neural network based intrusion detection uses a network that contains many computing units to perform complex mapping functions that interact by using weighted join. A neural network of knowledge is encoded into a network structure based on the connection between units and their weights, and the actual learning process is done by changing weights and adding or removing connections. The neural network processing is divided into two stages. Firstly, the network is trained by normal system behavior, and its structure and weight are adjusted. Secondly, the system inputs the observed events into the network, and then judges whether these events are normal or abnormal. At the same time, the system can also train the observed data so that the network can learn some changes in system behavior. The advantage of this approach is that it does not rely on any statistical assumptions about the type of data, and can handle noisy data better. Its inadequacy is that the topology of the network and the allocation of weights to each element must be determined by repeated attempts and failures. The neural network, however, does not provide any explanation for any anomalies they find, which hampers the ability of the user to obtain illustrative information or to seek the root cause of the intrusion security problem (Fig. 9).

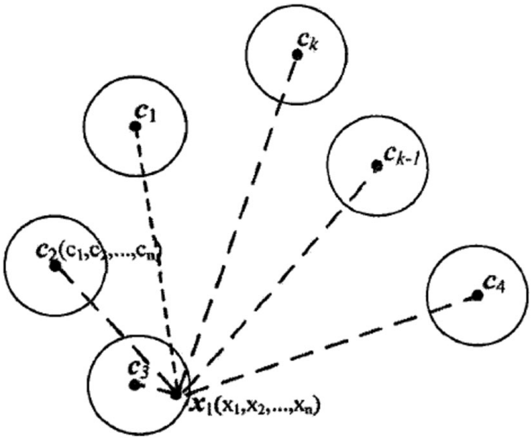


Fig. 9 Compute the sum of distances between the data samples

3.6 Data set conversion

In order to measure the distance of different samples in feature space, Euclidean distance function is needed. For two different sample sets, Euclidean distance between them can be calculated as follows:

$$x = (x_1, x_2, \ldots, x_n) \tag{4}$$

$$c = (c_1, c_2, \ldots, c_n) \tag{5}$$

$$dis(x_i, c_i) = \sqrt{(x_1 - c_1)^2 + \cdots + (x_n - c_n)^2} \tag{6}$$

In a dataset that has been divided into k disjoint clusters, one distance equation of x_1 is calculated as follows:

$$dis = dis(x_1, c_2) + \cdots + dis(x_l, c_k) \tag{7}$$

Specifically, the distance between the training set D_R and the data sample x_1 is defined as:

$$Dist(x_i, c_j) = \sum_{i=1}^{k} dis(x_i, c_j) - dis(x_i, c_j), (i = 1, 2, \ldots, m; j = 1, 2, \ldots, k) \tag{8}$$

where m is total data samples of D_R.

3.7 Classification model construction and data classification

K dimensional data set obtained by DSFE conversion is denoted as follows, and a classification model will be established as a training set.

$$D'_R = \left[x'_1, \ldots, x'_m\right] \tag{9}$$

In the data classification phase, we can obtain a new data set D'_E. For the sample data $\overline{x_i}$, its k distances can be calculated by the following formula:

$$Dist(\overline{x_i}, c_j) = \sum_{i=1}^{k} dis(\overline{x_i}, c_j) - dis(\overline{x_i}, c_j), (i = 1, 2, \ldots, s; j = 1, 2, \ldots, k) \tag{10}$$

where s represents total data sample.

3.8 Risk function of information security model

We are looking for a mapping component that minimizes misclassification risk.

$$\begin{cases} g : X \to Y \\ R(g) = \int |y - g(x)| p(x, y) dx = \Pr(y \neq g(x)) \end{cases} \tag{11}$$

In practical applications, real valued functions are used instead of binary functions. At the same time, joint probability distribution function is often difficult to predict, so the proper classification function can only be obtained by tagging sample points. This action is minimized by empirical risk function, as follows:

$$R_{emp}(f) = \frac{1}{l} \sum_{i=1}^{l} |y_i - \mathrm{sgn}(f(x_i))| \tag{12}$$

However, empirical risk minimization does not mean misclassification is the least risky. We can obtain a better generalization error bound by finding the largest function between the samples in the training set. Namely, for all $1 \leq i \leq l$, there is a constant γ, which satisfies $y_i f(x_i) \geq \gamma$. Binary loss function is as follows:

$$c(x, y, f(x)) = |y - \mathrm{sgn}(f(x))| \tag{13}$$

We can convert it into interval type loss functions, such as soft interval loss functions:

$$c(x, y, f(x)) = \max(0.1 - yf(x))^s, s \geq 1 \tag{14}$$

However, minimizing such loss functions remains difficult and may lead to poor generalization capability. Therefore, we need to control the admissible function type so as to obtain the rule risk function.

$$R_{reg}(f) = R_{emp}(f) + \lambda\Omega(f) = \frac{1}{l} \sum_{i=1}^{l} c(x_i, y_i, g(x_i)) + \lambda\Omega(f) \tag{15}$$

where $\lambda > 0$ is rule constant which determines complexity of function minimization

3.9 Network based intrusion detection system

The network based intrusion detection system uses the original network packet as the data source. Network based IDS usually monitors and analyzes all communication services over the network using a network adapter running in a random mode. Attack identification module which is usually use four kinds of commonly used techniques to identify the attack flag: mode, expression or byte frequency or cross matching; threshold; correlation between low-level events; detection of abnormal phenomenon on the statistical significance. Once an attack is detected, the IDS response module provides multiple options to notify, alert, and respond to an attack.

The host intrusion detection system has high detection efficiency based on the analysis of the cost analysis of small, high speed, can quickly and accurately locate intruders, the behavior characteristics and can be combined with the operating system and the application of the intrusion for further analysis. In the real time, sufficiency and reliability of data extraction, intrusion detection system based on host log is better than network-based intrusion detection system. Many organizations of network security solutions are based on both host based and network based two intrusion detection systems.

3.10 Mapping UML model and large relational database model

ERP database uses large relational data. In order to use the object-oriented technology in the database field, we need to use UML to get the object-oriented data model. Because there are differences between UML model and large relational database, some skills should be dealt with, and UML model and large relational database model can be mapped by object relation method. In the process of mapping, we should solve the problem of reference consistency, trigger problem, stored procedure problem and database access interface problem.

Rose can model the applications of ERP systems, and can model the database of ERP systems. Rose supports the generation of object models from data models and the generation of data models from object models. There are many differences between the data model and the object model, which are determined by the nature of the model itself. The object model focuses on behavior and data, while the data model focuses on data. The object model in most statements supports inheritance, and the data model does not support inheritance. To handle these own differences, when creating the ERP data model, separate the creation of the object model from the creation of the data model. Since the ERP system development of the circulation enterprise starts from the existing MIS data model, we must first use the data model in Rose, including the logical view and the component view. In the logical view, a structure is created that contains stored procedures. Also create tables that contain fields, restrictions, triggers, primary keys, indexes, relationships, and so on.

It is assumed that the behavior of all intrusions is different from normal behavior. Establish a normal activity document, which is considered as a choice of suspicious behavior and features when the subject activity violates its statistical rules. In practice, however, the set of intrusions may overlap with the set of unusual behavior, which is not exactly the same, and there are two desired results: false positives and missing reports. Among them, false positives are non intrusive behaviors which lead to abnormal occurrence and are labeled as intrusions. Omission refers to the occurrence of an invasion, but no abnormal results are recognized as normal behavior by the system. The main advantage of exception detection is that they can detect previously unknown attacks, and the disadvantage is that they are prone to fail to report. At present, there are many kinds of intrusion detection methods based on Anomaly Intrusion detection.

Statistical methods: is a kind of intrusion detection method is relatively mature, it makes the intrusion detection system can learn the main daily behaviors between those with normal activities of the statistical errors of the signs for abnormal activity. In the statistical approach, first select the statistical data and effective measurement points, the session can reflect the theme feature vector is generated, and the data was analyzed by statistical method, to determine whether the current activity conforms to the historical behavior of the theme. With the continuous operation of the system, the behavior characteristics of the learning corpus and the updating of the history record, the main advantage is that the user behavior can be learned adaptively.

Prediction model generation: this method is based on events that have occurred and try to predict what will happen in the future. Compared with pure statistical methods, it increases the analysis of sequence and correlation of events, thus detecting abnormal events that statistical methods cannot detect. The main advantage of this method is that it can detect abnormal events which are not easily detected by traditional methods. The system built with this model has highly adaptive ability.

Artificial neural network: training a neural network to predict the next activity or operation of a user. The specific operation is to train the neural network through a series of normal user operations. In the training process, by adjusting its structure and weight, it can match the actual operation as much as possible. Then, the observed event stream is input into the network to determine whether these events flow normally. The main advantages of using neural networks are that they can handle noise data well and do not rely on any statistical assumptions about the data type.

3.11 Misuse intrusion detection

Using a known attack pattern or system weakness to match and identify attacks, this method detects many known attack patterns and tries to recognize known bad behavior. The main problem is how to find all possible intrusion pattern features, which can make the real intrusion and normal behavior to distinguish, so the intrusion pattern expression directly affects the ability of intrusion detection. Its main advantage is low false positive rate, and the disadvantage is that only known attacks in the database can be found. Due to misuse intrusion detection cannot detect new or unknown attacks and intrusion detection are often unable to detect internal attacks, so the intrusion detection system using any of these methods are not desirable, an ideal choice is to use two kinds of detection methods. At present, there are many kinds of intrusion detection methods based on Misuse Intrusion detection.

Expert system: in an expert system, intrusion behavior is encoded into expert system rules, which identify individual audit events or represent an intrusion behavior, a series of events. The expert system can explain the audit records of the system and determine whether they satisfy the description rules. The disadvantage is that the use of expert systems to represent a series of rules is not straightforward, and the rules must be updated by experts.

Based on pattern matching, the known intrusion signatures are encoded into patterns consistent with audit records, and when the new audit events occur, the method will search for the known intrusion patterns matching it. The main problem with this model is that it can detect only events based on known authorization behavior.

Model of intrusion detection based on intruder often uses a behavioral sequence in the attack when a system, this kind of behavior has a certain sequence consisting of behavior model, according to the behavior characteristics of this model represents the attack intention, can detect malicious attack. The advantage of this method is that it improve the uncertainty reasoning based on mathematical theory, it can only detect some of the major audit events, after these events, and then began to record detailed audit, audit events so as to reduce the processing load.

3.12 The development trend of intrusion detection technology

With the rapid development of network technology, intrusion detection technology is also developing, but generally speaking, intrusion detection technology is still very imperfect, and will face many challenges. Some promising research directions are put forward below. Data selection is an important part of intrusion detection technology, and is also the key to identify intrusion events effectively. Data selection sensor technology may be integrated into the daily computer environment in the future and become part of the operating system.

Once the intrusion detection system is controlled by an intruder, the security line of the whole system will be faced with the risk of the collapse of the front line. Therefore, an effective strategy must be adopted to ensure the absolute security of the intrusion detection system. As the network attacks step by step, this research will be an important direction.

Evaluation method of intrusion detection. Users need to evaluate the scope of detection, the system resource occupation and the reliability of the intrusion detection system. It is an important research direction of IDS to design a test and evaluation platform for general intrusion detection system.

Attack behavior tracking and security incident diagnosis technology. In order to provide basis for treatment of intrusion events, real-time tracking and recording attacks related technology needs is a promising direction, the main research may include recording attacks, attacks network technology and network attack obtained evidence related to deception. In order to deal with events, and use security incident diagnosis technology to determine attack types, the main research in this part includes the techniques of obtaining and analyzing the characteristics of cyber attacks and the classification and determination techniques of attacks.

Network intrusion detection and attack protection. The target is real-time detection, real-time tracking of the invasion of users, and automatically prevent network intrusion, the implementation of security protection. This part mainly focuses on the problem of intrusion detection in high-speed networks and the adaptive problem of intrusion detection, which is a hot research area.

4 Block chain information security model

4.1 The problems of block chain technology

Block chain technology is still in the initial stage of development, and there are many problems. The problem of data volume in distributed bookkeeping. The distributed accounting book records all transaction records of the whole block chain network from birth to the current time node, and brings storage and synchronization problems while ensuring that the block chain data cannot be tampered with. As mentioned above, the current amount of bitcoin data has exceeded 60 GB, huge amount of data. According to the increasingly active trend of bitcoin, the book is too large is an urgent need to solve the problem.

Block chain as a technology, it is to point to be based on some algorithms, add a new data in the Shared database, must first obtain some node recognition, after approved, the new data to form a new block, and can be identified by other data in the database, and the ability of self-management, these blocks without human management, the blocks can also through the public key and the original block chain link [19–21]. The interlinks between these blocks are known as blockchains that should host the following three major aspects of the features. (1) It can be said that the current bitcoin, Nasdaq Linq trading platform and Edgelogic diamond registration account are the specific applications of blockchain technology, rather than the block chain technology itself. It is important to note that most of the current block chain technology involved in the collection of individual technology, in the corresponding area are relatively mature technology, how many innovation does not exist, but overall caused by the currency block chain technology through the organic combination of existing technology to create the infrastructure of a certain value, its essence is a kind of integrated innovation [22–24]. (2) Bitcoin blockchain technology on the one hand, the construction of democratic network using P2P protocol to open source, to the center, so that each node of the information real-time broadcast spread to other nodes in the network, and each node can store all complete information; on the other hand, the use of asymmetric encryption and the identification information the owner, the individual can prove their ownership in the anonymous network. (3) The Bitcoin blockchain technology uses a "block + chain" data structure, the "block" of the "block" stores data, and the "block" of "block" stores the reference of the previous "block", in fact The link from the current "block" to the previous "block" is formed [25, 26].

Synchronous time problem. So far, 430 thousand blocks of bitcoin networks have been mined, and the time has taken for new nodes to synchronize with their books. If there is no improvement scheme, with the passage of time, the new node will be more expensive, and even block the expansion of the block chain network.

Transaction efficiency problem. Regarding of bitcoin, for example, only 7 transactions can be dealt with in one second, while the determined transaction will have to wait for the next block, averaging 10 min. The force proof leads to the inequality of nodes. In theory, the block chain of each node in the network to be treated equally, but in order to obtain economic returns to mining, hardware competition, between nodes is not equal to [27–29]. At present, using CPU to dig bitcoin, the theoretical probability is almost equal to 0. The randomness of the block accounting rights is undermined, which violates the original intention of the design.

For this system, we should discuss from the following aspects [30–32]. (1) To the center of the center of the management mechanism does not exist in the network, the network structure of the end but a distributed end to, each node in the network access equivalence; (2) The autonomy: the consensus protocol based on the specification and all nodes can trust environment freely and safely the exchange of data; (3) Security: on the transaction data encryption using asymmetric cryptography technology, at the same time with the proof of work mechanism to ensure data theory is difficult to tamper; (4) Transparency: all transactions recorded in the whole network is open and transparent, to break the information asymmetry.

Although block chaining technology adopts cryptography related technology, it has high security, but the whole block chain network still has weak link in privacy and security. Data privacy issues. Bitcoin transactions using the address, which is anonymous, but the transaction is completely open, all the transaction records of an address can be found, once the address associated with the true identity, the consequences are very serious.

Use security issues. Block chaining technology is highly secure, and its security and effectiveness are guaranteed by using asymmetric key mechanism. But for the use of the private key and save the situation is worrying, even if the private key performance of 256 bit to 50 characters in length, is still difficult to memory, use other software to aid trading is an inevitable choice, but the security of this kind of software is questionable.

4.2 Combination of internet of things and block chain

At present, a combination of things with the block chain has been used in the medical and health applications such as networking platform, which realizes the combination of electronic medical records and medical insurance, banking and insurance, in order to ensure personal health assessment and identification, protection of personal health information privacy and security cannot be tampered with. The internet of things is a technology intensive industry, and it also collides with all kinds of things and laws and regulations. Although the internet of things is complex, difficult, involving a wide range of related things, but its application and development, or let us look forward to. We need to achieve the transformation and rejuvenation through industrial upgrading, and the internet of things technology is able to help achieve its goals through technical integration, cross-border integration and the creation of ecological systems.

In view of the complexity of the internet of things, the development of the internet of things, first of all, the industry as the main, one by one to establish, and then there is an association between industries, and gradually form an ecological system. The internet of things is the system of social attributes, the importance of the ecosystem of internet of things, and the development of internet of things needs collaboration, sharing and patience. The ultimate form of the internet of things security is to build a trust system to re-establish the social trust mechanism through the extensive interconnection between people and things, so as to make our world a better place.

5 Experiment and construction of information security model

Information security risk assessment is based on the international and domestic technical standards for information and information processing facilities threat, impact, vulnerability and the possibility of the three assessment.

Table 1 Risk grade matrix

Criticality	Damage degree		
	High(100)	Medium(50)	Low(10)
High (1.0)	100	50	10
Medium (0.5)	50	25	5
Low (0.1)	10	5	1

Risk is a potential threat to the loss or damage of assets by the use of an asset or a set of vulnerabilities, that is, the combination of the likelihood and the outcome of a particular threat. Risk formation consists of five aspects: origin, mode, approach, receptor and consequences.

5.1 Risk grade matrix and description

The risk of information systems is determined by the following two aspects. Threat sources exploit system vulnerabilities under existing controls. The degree of damage resulting from the system being attacked.

The possibility of the threat is related to the ability and motivation of the threat source, the vulnerability of the information system and the control measures implemented by the system. The calculation of information system risk should be carried out through the risk grade matrix. Table 1 is a standard risk grade matrix structure where the risk of an information system is multiplied by the likelihood of occurrence and the hazard level. Table 1 is a matrix of 3 × 3, and can be used in the matrix of 4 × 4 or 5 × 5 depending on the complexity of the organization. The larger the matrix, the greater the risk level. The calculated risk level values indicate the degree of risk.

We can qualitatively divide the risk grade matrix into several risk levels according to the specific circumstances of the organization to obtain an intuitive risk profile [33, 34].

5.2 Risk grade matrix and description

The operational steps for quantitative information security risk assessment are as follows. A combination of threat sources, motivational levels, and threat capability levels generates a threat level that represents the potential of the threat itself, as shown in Table 2.

Table 2 Combination of threat sources motivational levels and threat behavior abilities

Threat level		1(Low)	2(Medium)	3(High)
Threat behavior capability	1(Low)	1	2	3
	2(Medium)	2	3	4
	3(High)	3	4	5

Table 3 Threat level and vulnerability utilization level combination

Threat/vulnerability level		Threat level				
		1	2	3	4	5
The level in which vulnerability is exploited	1	1	2	3	4	5
	2	2	3	4	5	6
	3	3	4	5	6	7

The threat level is combined with the vulnerability utilization level to generate a threat/vulnerability level, indicating the potential to exploit vulnerabilities, as shown in Table 3.

Table 4 Threat level and vulnerability utilization level combination

Asset/impact level	Asset value level		
	1(Low)	2(Medium)	3(High)
Impact level	1	2	3
	2	3	4
	3	4	5

The combination of the asset value level and the impact level produces the asset/impact level, indicating the importance of the asset, as shown in Table 4.

5.3 Classification problem

Intrusion detection belongs to a classification problem, the goal is to classify each audit record into a discrete classification set. Given a set of records, each of which has a class flag, the classification algorithm can compute a model that uses the most distinguishing feature value to describe each flag. In order to make the classifier effective, it is necessary to obtain features with high information and reduce entropy, as shown in Table 5.

A security scanner is run on a LAN with a network load of 10 Mb/s, and a simulated attack is sent to 15 hosts in the LAN using different scanning methods, as shown in Table 6.

Table 5 Telnet record of intrusion detection

Label	Service	Flag	Hot	Failed	Compromised	Root	Su	Duration
Normal	Telnet	SF	0	0	0	0	0	10.2
Normal	Telnet	SF	0	0	0	3	1	2.1
Guess	Telnet	SF	0	0	0	0	0	26.2
Normal	Telnet	SF	0	0	0	0	0	126.2
Overflow	Telnet	SF	3	0	2	1	0	92.5
Normal	Telnet	SF	0	0	0	0	0	2.1
Guess	Telnet	SF	0	0	0	0	0	13.9
Overflow	Telnet	SF	3	0	2	1	0	92.5
Normal	Telnet	SF	0	0	0	0	0	1248

Table 6 Telnet record of intrusion detection

Number of attacks launched	Detect attack quantity	Effectiveness of attack	Analyze message quantity	Packet loss
39,522	39,017	0.9872	15,120,304	0.17%

The system effectively detects some variant attacks, denial of service attacks and password guessing attacks in simulation attacks, which cannot be detected by the system. Using protocol analysis method for intrusion detection, good results are obtained in the overall, accuracy and efficiency of intrusion detection.

6 Conclusion

This paper systematically introduces the principle, technology and application of block chain technology. It is a summary of current block chain technology research results. At present, the basic theory and technology of block chain technology is still in the initial stage, although there are a lot of using the block chain technology of commercial products, but the lack of theoretical research, to support the product, is not conducive to long-term development of block chain technology. This paper introduces the information security model of block chain based on Intrusion Detection Technology in the internet of things. We apply intrusion detection technology to the protection of block chain information security, and analyze the detection technology based on different models. At the same time, the combination of things with the block chain is also the application of hot issues, in view of the complexity of the *internet of things*, the development of the internet of things first in the industry as the subject, and then related to the industry, and gradually formed the ecological system.

Block chain technology may be a way to implement artificial intelligence, and intelligent contracts are designed to become more automated, intelligent and complex. The development and application of block chain technology have produced important influence all over the world, and more and more achievements have been made. As a new technology, block chain technology is still in the development stage, the current application of the block chain more still in the theoretical research and verification stage, based on real block chain technology for commercial application or the product is not much. In view of the possible problems in the management of logistics information resources in block supply chain, the countermeasures are put forward. The block chain is introduced into the supply chain logistics information ecosystem construction, is conducive to grasp the flow of supply chain logistics information resources, information resources optimization of logistics supply chain management, improve the supply chain logistics information ecological environment, realize the innovation and development of industrial clusters.

Acknowledgements This research is financially supported by the Project of Macau Foundation (No. M1617): The First-phase Construction of Big-Data on Smart Macao.

References

1. Zheng, X., Ge, B.: The evolution trend of information management of supply chain in China under the information environment. Inf. Sci. **10**, 128–133 (2016)
2. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. o
3. Ping, Z., Yu, D., Bin, L.: Chinese Block Chain Technology and Application Development White Paper. Ministry of Industry and Information Technology, Beijing (2016)
4. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc, Sebastopol (2015)

5. Zhao, H., Li, X.F., Zhan, L.K., et al.: Data integrity protection method for icroorganism sampling robots based on blockchain technology. J. Huazhong Univ. Sci. Technol. **43**(Z1), 216–219 (2015)
6. Swan, M.: Block chain thinking: the brain as a decentralized auto nomous corporation. IEEE Technol. Soc. Mag. **34**(4), 41–52 (2015)
7. Godsiff, P.: Bitcoin: bubble or blockchain. In: The 9th KES International Conference on Agent and Multi-Agent Systems: Technologies and Applications (KESAMSTA), vol. 38, pp. 191–203 (2015)
8. Wilson, D., Ateniese, G.: From pretty good to great: enhancing PGP using Bitcoin and the blockchain. In: The 9th International Conference on Network and System Security, New York, pp. 358–379 (2015)
9. Kypriotaki, K.N., Zamani, E.D., Giaglis, G.M.: From Bitcoin to decentralized autonomous corporations: extending the application scope of decentralized peer-to-peer networks and block chains. In: The 17th International Conference on Enterprise Information Systems (ICEIS2015), pp. 280–290 (2015)
10. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
11. President's Council of Advisors on Science and Technology. Leadership Under Challenge. Information Technology R&D in a Competitive World, An Assessment of the Federal Networking and Information Technology Program[EB/OL] (2017). https://www.ostpgov/pdf/nitrd_review.pdf
12. International Telecommunication Union. ITU Internet Reports 2005: The Internet of Things (2005)
13. Petrovic, D., Shah, R.C., Ramchandran, K.: Data funneling: routing with aggregation and compression for wireless sensor networks. In: Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (SNPA'03). Seattle, USA, pp. 140–168 (2003)
14. Yuan, Y., Kam, M.: Distributed decision fusion with a random access channel for sensor network applications. IEEE Trans. Instrum. Meas. **53**(4), 1239–1320 (2004)
15. Tan, H., Korpeoglu, I.: Power efficient data gathering and aggregation in wireless sensor networks. ACM SIGMOD Record **32**(4), 50–89 (2003)
16. Anderson, J.P. Computer security threat monitoring and surveillance. Technical Report, James P Anderson Co., Fort Washington, Pennsylvania (1980)
17. Denning, D.E.: An intrusion -detection model. IEEE Trans. Softw. Eng. **13**(2), 220–235 (1987)
18. Aurobindo, S.: An introduction to intrusion detection. ACM Crossorads **2**(4), 3–7 (1996). http://www.acm.org/crossroads/xrds2-4/intrus.html
19. Chen, Q., Zhang, G., Yang, X., et al.: Single image shadow detection and removal based on feature fusion and multiple dictionary learning. Multimed. Tools Appl. (2017). https://doi.org/10.1007/s11042-017-5299-0
20. Desai, A.S., Gaikwad, D.P.: Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA. In: 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), pp. 291–294 (2016)
21. Aburomman, A.A., Reaz, M.B.I.: A novel SVM-kNN-PSO ensemble method for intrusion detection system. Appl. Soft Comput. **38**, 360–372 (2016)
22. Zhang, Y., Wang, H., Xie, Y.: An intelligent hybrid model for power flow optimization in the cloud-IOT electrical distribution network. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-1270-0
23. Anwar, S., Mohamad Zain, J., Zolkipli, M.F., Inayat, Z., Khan, S., Anthony, B., Chang, V.: From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms **10**(2), 39 (2017)
24. Haider, W., Hu, J., Slay, J., Turnbull, B.P., Xie, Y.: Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. J. Netw. Comput. Appl. **87**, 185–192 (2017)
25. Sedjelmaci, H., Senouci, S.M., Ansari, N.: Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a Bayesian game-theoretic methodology. IEEE Trans. Intell. Transp. Syst. **18**(5), 1143–1153 (2017)
26. Cai, Z., Deng, L., Li, D., et al.: A FCM cluster: cloud networking model for intelligent transportation in the city of Macau. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-1216-6
27. Bostani, H., Sheikhan, M.: Modification of supervised OPF-based intrusion detection systems using unsupervised learning and social network concept. Pattern Recogn. **62**, 56–72 (2017)
28. Zhang, S., Wang, H., Huang, W.: Two-stage plant species recognition by local mean clustering and weighted sparse representation classification. Clust. Comput. **20**, 1517 (2017). https://doi.org/10.1007/s10586-017-0859-7
29. Wang, H., Wang, J.: An effective image representation method using kernel classification. In: IEEE 26th International Conference on Tools with Artificial Intelligence (ICTAI), pp. 853–858 (2014)
30. Nair, R., Nayak, C., Watkins, L., Fairbanks, K.D., Memon, K., Wang, P., Robinson, W.H.: The resource usage viewpoint of industrial control system security: an inference-based intrusion detection system. In: Cybersecurity for Industry 4.0, pp. 195–223. Springer, New York (2017)
31. Dhillon, H.S., Huang, H., Viswanathan, H.: Wide-area wireless communication challenges for the Internet of Things. IEEE Commun. Mag. **55**(2), 168–174 (2017)
32. Pramudianto, F., Eisenhauer, M., Kamienski, C.A., Sadok, D. and Souto, E.J.: Connecting the internet of things rapidly through a model driven approach. In: IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 135–140 (2016)
33. Deng, L., Li, D., Yao, X., Cox, D., Wang, H.: Mobile network intrusion detection for IoT system based on transfer learning algorithm. Clust. Comput. 1–16 (2018)
34. Li, D., Deng, L., Gupta, B.B., Wang, H., Choi, C.: A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. Inf. Sci. (2018)

Daming Li is currently a research fellow at Post-doctoral Programme of China (Hengqin) Pilot Free Trade Zone and Information Centre of Hengqin New Area. He is also a course consultant of City University of Macau. He has received his doctor degree in City University of Macau in 2014. He is the membership of International System Dynamics Society of the State University of New York. His research interests focus on the big data technology, smart city, and quantitative analysis.

Zhiming Cai PhD, Professor at City University of Macao. Prof. Cai Zhiming received his Bachelor, Master and PhD at Hefei University of Technology in China, and experienced postdoctoral at University of Toronto of Canada. He has been working in universities of China, Germany, Canada and Macao, with positions: assistant, lecturer, associate professor, professor; duty director of department, duty dean of faculty, head of academic affairs office and graduate office of university, and director-general of Macao Software Association. He published 6 books and more than 50 papers. He has taught Software Engineering, Operating Systems, Discrete Math., etc. His research interests are in Big Data, Software Engineering, Visual Modeling, Decision Supporting System and Distributed System.

Lianbing Deng is the director and general manager of Zhuhai Da Hengqin Science and Technology Development Co., Ltd. And he is also the director of Post-doctoral Programme of China (Hengqin) Pilot Free Trade Zone and the director of Information Centre of Hengqin New Area. He has received his doctor degree in Huazhong University of Science and Technology. His researches are in the field of big data, project management, and economic research. He is the vice chairman of China Big Data Council of MIIT of the People's Republic of China.

Xiang Yao is currently an architect in China (Hengqin) Pilot Free Trade Zone and Information Centre of Hengqin New Area. He was received his bachelor degree in Heilongjiang Institute of Technology in 2007. His research interests focus on the Cloud, Big Data, IoT, Block Chain, ML technology and System analysis.

Harry Haoxiang Wang is currently the director and lead executive faculty member of GoPerception Laboratory, NY, USA. His research interests include multimedia information processing, pattern recognition and machine learning, remote sensing image processing and data-driven business intelligence. He has co-authored over 50 journal and conference papers in these fields on journals such as Springer MTAP, Cluster Computing; Elsevier Computers & Electrical Engineering, Optik, Sustainable Computing: Informatics and Systems, Journal of Computational Science, Pattern Recognition Letters, Information Sciences, Future Generation Computer Systems and conference such as IEEE SMC, ICPR, ICTAI, CCIS, ICACI.