The current research of IoT security

1st Jian Zhang
School of Computer Science and Engineering
Tianjin University of Technology
Tianjin, China
zhangj@tjut.edu.cn

2nd Huaijian Chen
School of Computer Science and Engineering
Tianjin University of Technology
Tianjin, China
ytx0000001@163.com

3rd Liangyi Gong
School of Software and BNRist
Tsinghua University
Beijing, China
gongliangyi@gmail.com

4td Jing Cao
Tianjin Information System Security
and Confidentiality Evaluation Center
Tianjin, China
cj0000@ vip.sina.com

5th Zhaojun Gu
Information Security Evaluation
Center of Civil Aviation
Civil Aviation University of China
Tianjin, China
zjgu@cauc.edu.cn

***Abstract*—In recent years, the development of the Internet of Things technology has been very rapid. However, with the explosive growth of IoT devices, the challenges facing the IoT environment are becoming more and more serious. How to ensure the security of the IoT becomes a key issue. The primary purpose of IoT security is to protect private data and ensure the security of IoT users, infrastructure, data and devices. This paper reviews the threat challenges and IoT security models at each level of the Internet of Things in recent years and discusses some of the past and future solutions. At first, the IoT security threats are systematically introduced from the perspectives of physics, network and data. In addition, the mainstream IoT security model is introduced. Then we introduce solutions to IoT threats from three perspectives, including IoT access control, intrusion detection and distribution methods. In the end, the paper introduces the current IoT security model has not formed a unified standard and expresses a future expectation for the development of future security model.**

***Index Terms*—IoT architecture, Data security, Network security, Physical security**

I. Introduction

In recent years, cybercriminals' interest in the Internet of Things has continued to grow. In the two years of 2015 and 2016 alone, a number of large-scale IoT security incidents have occurred, highlighting the Mirai and Bashlite botnets. The research and application deployment of IoT security technologies has attracted widespread attention from governments, industry and academia.

According to estimates, the number of global IoT devices will reach 8.4 billion in 2017, surpassing the global population for the first time. It is estimated that by 2020, the number of IoT devices worldwide will reach 20.4 billion. Huawei predicts that the number of IoT devices will be close to 100 billion in 2025, and 2 million sensors will be deployed every hour. Massive IoT devices give us convenience and also pose a great security threat.

IoT network security will also be a disaster area. According to statistics, in the first half of 2018, the number of malware samples collected by Kaspersky Lab for attacking smart devices was three times that of 2017, and the number in 2017 was ten times that of 2016. Violently cracking Telnet passwords is still the most common method of self-propagation of IoT malware. In the second quarter of 2018, this type of attack was three times that of other attacks [1]. Fig.1 shows the ten countries most affected by Telnet password attacks.

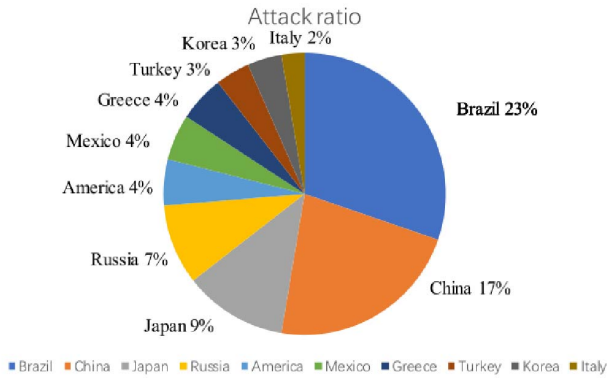

Fig. 1. Telnet password attack.

In November 2015, Hong Kong toy manufacturer VTech was invaded. Nearly 5 million adult users' names, e-mail addresses, passwords, addresses and names, genders and birthdays of more than 200,000 children were accidentally leaked. In March 2017, Spiral Toys' CloudPets series of animal-filled toys suffered data breaches and malicious customer databases were maliciously invaded. The accident disclosure information includes toy recordings, MongoDB leaked data, 2.2 million account voice messages, and database extortion information. In recent years, data privacy issues have become more and more prominent, which has threatened our lives to a large extent. Information security is an important issue that needs to be solved urgently in the security of IoT.

The security is not only the basis of the development of the IoT, the most important link of the IoT technology. The purpose of this article is to provide a comprehensive

978-1-7281-4528-0/19/$31.00 ©2019 IEEE
DOI 10.1109/DSC.2019.00059

understanding of IoT security. The focus is on an overview of recent challenge architectures and solutions. This paper will comprehensively introduce the security threats of IoT from three aspects and systematically elaborate on the latest security architecture of IoT. Finally, the paper introduces the advanced security solutions of IoT and provides some suggestions for the healthy development of IoT.

II. IoT Security Threats

With the continuous improvement of theoretical knowledge and the increase of practical application scenarios, the security problems exposed by IoT technology are becoming more and more prominent. The threat of IoT security has gradually attracted the research and attention of scholars at home and abroad. In the early three-layer architecture of IoT, some scholars proposed that each layer corresponding to the traditional three-layer structure corresponds to different security threats. The perception layer has the security and transmission of the IoT terminal. The perception layer includes IoT terminal security, Wireless Sensor Network security and RFID security [2], [3]. These three kinds of security involve both physical security and network security. The network layer has security issues such as security protocols and authentication, and the application layer involves the issue of customer privacy and reliability protection [4], [5].

Intuitively, the hierarchical analysis method of IoT security threats according to the traditional architecture has lost its practical significance. This method cannot fully summarize the IoT security threats encountered in the emergency phase. Therefore, researchers at this stage only regard this classification as a classification method. It is a reference. [6] Classification of security threats by active and passive attacks, and classification of threats by means of tags that are interrupted, falsified, forged, replayed, and intercepted. However, this classification method only involves information security in the IoT security domain.

Recently, some scholars have proposed some classifications of security threats for edge computing [7], and some scholars have classified them according to some characteristics of IoT structure. For example, according to the diversity of IoT, IoT security threats fall into two categories [8]. Classification according to heterogeneity and interoperability [9], [10]. These scholars have made a detailed classification of some specific threats of IoT, but they are only specific and not universal to a certain feature or structure classification. According to China's network security level protection network has been in the cloud computing security expansion requirements, the paper will introduce the IoT security threat from three perspectives: physical device threat, network communication threat, and information data threat. The main purpose is to present IoT security threats more clearly and specifically to provide better guidance for IoT security models and solutions. Table I provides a brief comparison of IoT security threats.

A. Physical Device Threats

Traditional cybersecurity threats include disguise, illegal connection, unauthorized access, denial of service, repudiation, information leakage, traffic analysis, invalid information flow, tampering, and destruction of data. The biggest difference between IoT security and traditional network security lies in it has a large number of IoT devices.

1) Device Threats: The physical device is at the bottom of IoT and is the entry point for data. Therefore, identity authentication of IoT devices is particularly important. Mutual authentication between IoT devices servers is an important part of the IoT security system [7]. With the development of IoT security and cryptography, the threat posed by this identity authentication has achieved remarkable results. However, the risk of threats caused by the huge amount of smart devices and sensors to the Internet of Things has not decreased. Radio frequency identification (RFID) is most vulnerable to physical attacks, including the physical destruction of the node itself. Attackers attack RF tags, tamper with tag content or interfere with, block communication channels [11]. The attack on the device also includes a malicious replacement device and a forged attack. The forged attack refers to the "legal user tag" of the forged electronic tag generation system being recognized by the system, and the attack method is costly and has a long period. The SDN control node is vulnerable to damage, including man-in-the-middle attacks and saturation attacks. In severe cases, the entire network state will be in a paralyzed state. In addition, in the wireless sensor network WSN, the network node has a threat of battery capacity and storage capacity.

2) Resource Constraint: Device attacks are part of the threat, and the limitations of second physical devices are also a threat. [7] pointed out that IoT devices are resource-constrained. This resource constraint will constrain the computing power of nodes, making nodes unable to perform complex calculations and ultimately threatening the development of the entire IoT technology. This kind of resource constraint is particularly prominent in the edge calculation, which is also a high-tech bottleneck restricting the development of IoT at this stage.

B. Network Communication Threats

Physical threats are part of the IoT security foundation, and network security is the most critical part of IoT security. Structurally, the IoT network has the characteristics of interoperability and operability, but it also exposes the disadvantages of weak controllability and heterogeneity. In the IoT architecture, network communication is usually in the middle layer, transmitting, storing and processing the data transmitted from the underlying layer. Different security threats are exposed during the transfer storage and processing.

1) Structure: Structurally, the biggest difference between the IoT network system and the traditional network system is that the former has the characteristics of manageability and weak controllability. This has brought great challenges to the development of the Internet of Things.

IoT needs to be connected to the Internet. The communication method between the three layers of the Internet of Things [3] is not only wired communication but also wireless link connection. It is through heterogeneous communication technologies such as Ethernet, WiFi, Bluetooth, and ZigBee. IoT connects with a huge number of heterogeneous smart devices. On the one hand, this heterogeneity makes management control of network and IoT applications extremely complex [12]. On the other hand, under the traditional three-layer system , the underlying wireless sensor network WSN exposes weak controllability. And the core network of the middle layer and the short-distance communication network reflect heterogeneity.

Controllability and manageability is the ability to control the dissemination and content of information. In addition to the usual form of propagation site and propagation content monitoring, the most typical example is the password hosting policy. The password hosting policy is that when the encryption algorithm is managed by a third party, it must be executed in strict accordance with the provisions of controllable. This centralized control is a good strategy for managing IoT network systems, but there are also many threat vulnerabilities in this centralized control. For example, the network-defined network SDN application in IoT security [13] is an example paradigm that reflects the controllability of the Internet of Things. However, this paradigm has not been fully matured from the present to the present. The main reason is that it faces a big threat. In the IoT system, centralized control often becomes its limitation, and in the worst case, it may become the bottleneck of the entire network. Its control node is vulnerable to damage. Once the control node is destroyed, a corrupted node (switch/host) can use this vulnerability to attack the network. These include denial of service (DoS)/DDoS attacks, data modification, repudiation attacks, black hole attacks, and side channel attacks [14]. Under the three-layer system of edge computing, the distributed middle layer exposes the disadvantage of weak controllability.

2) Protocol: Firstky, when IoT data is used for network communication, it needs to be transmitted, processed, and stored. A large number of communication protocols are used in the communication process. The IoT protocol is divided into a transmission protocol and a communication protocol. There are seven major protocols: REST/HTTP, MQTT, CoAP, DDS, AMQP, XMPP, and JMS. The protocols used for communication with the cloud server are MQTT, AMQP, XMPP, the various IoT communication protocols represented by the MQTT protocol, etc [15].

MQTT is a lightweight machine-to-machine communication protocol that acts as a low-bandwidth communication method. MQTT is very simple and promotes its widespread use. But MQTT servers are often used as firmware updates for the Internet of Things, so an attacker can install firmware updates using the malicious code. CoAP is a lightweight machine-to-machine protocol, which allows an attacker to send a small UDP packet to a CoAP client and the client will respond with a larger packet. Therefore, the CoAP protocol is vulnerable to DDoS attacks. Although the HTTP protocol itself is not a security issue, applications and servers developed using HTTP are likely to be targeted. The reason is the protocol itself does not include session management and encryption processing requirements. Both the AMQP protocol and the XMPP protocol have read object spoofing vulnerabilities.

C. Information Data Threats

Information security has five characteristics: confidentiality, integrity, availability, controllability, and non-repudiation. IoT data will reflect different security threats during transmission, processing, and storage. The main information data threats are reflected in the three characteristics of “confidentiality, integrity, and availability”.

1) Confidentiality: The confidentiality of IoT security refers to the characteristics that information is not disclosed to or used by unauthorized users, entities or processes. Specific IoT security threats are fraudulent camouflage, illegal connections, unauthorized access, information disclosure, denial of service, refusal, traffic analysis, invalid information flow, tampering or corruption of data. Identity authentication threats in IoT security refer to spoofing or mock attacks stealing authentication credentials for unauthorized service access. It can be divided into IP address spoofing, ARP spoofing and DNS service spoofing [16], [17]. IP address spoofing in the Internet of Things will also trigger DDoS attacks to form a botnet. DDoS attacks are effective by leveraging multiple compromised computer systems as a source of attack traffic. Machines that are utilized may include computers and other network resources, such as IoT devices, which derive DDoS attacks in the IoT space. Some IoT devices are infected with malware first, then turning each device into a bot. Finally, the attacker can remotely control the bot group, which is called a botnet. The crater attack associated with a fake route is to use a malicious node to use the imaginary path as the optimal routing path to direct data traffic. At the same time, the selective forwarding attack is also a data-guided attack mode [18]. The attacker selectively forwards malicious packets while discarding the real important data packets [8].

The confidentiality of data involves the privacy issues of users and developers. At this stage, IoT has given us a rich and convenient life, but also caused great trouble to our information security. In recent years, the Internet of commerce privacy data leakage incidents has occurred frequently. Our data information is now uploaded to the Internet. Some sensitive information, including the mobile phone number, is also stored in the cloud. The current network protection scheme is not perfect, and an ordinary person can also obtain us through illegal means. Sensitive data creates an unobstructed view of our private information exposed to the Internet. In the context of the Internet of Things, privacy breaches are a big problem. They refer to unauthorized access to processing information by an attacker, by attaching monitoring devices, monitoring network channels, or gaining physical access to the device. E. Bou-Harb et al. [19] described the attacker’s attempt to collect information about the target node and its vulnerabilities

TABLE I
COMPARISON OF IOT SECURITY THREATS

Name	Features	Threats
Physical Device Threats	·Resource constraint	·Identity Loss ·Destruction of Nodes ·Tamper with Label Content ·MITM attack
Network Communication Threats	·Controllability and Manageability ·heterogeneity ·Protocol	·IP Spoofing ·Side Channel Attack ·DDoS ·Vulnerablity of protocol ·Vulnerablity of Control Nodes
Information Data Threats	·Confidentiality ·Availability ·Integrality	·Replay Attack ·Data Modification

through scan connections (port scans, etc.). Once the network vulnerability information is disclosed and exploited, the side channel attack will cause sensitive information to be leaked.

2) Availability: In the IoT environment, information can be transmitted efficiently and reliably only by ensuring the availability of the network system. Availability refers to the feature that network information can be correctly accessed by authorized entities, which can be used normally or restored under abnormal conditions. In other words, the required information can be correctly accessed while the system is running. When the system is attacked or destroyed, can be quickly restored and put into use.

Availability is a measure of the security performance of the IoT network information system for users. When the user system is subjected to a fake route attack [19], the routing information exchanged in the target routing protocol is spoofed, modified, or replayed to generate a fictitious routing behavior. The IoT network is attacked, which may cause the routing table of the network device to be disordered, resulting in the network. Lots of waste of resources will seriously cause network paralysis. Replay attack [11] means that the attacker sends a packet that the destination host has received to achieve the purpose of spoofing the system. It is mainly used for the identity authentication process and destroys the correctness of the authentication. This kind of replay attack is difficult to resist even if it is encrypted. For example, the intruder intercepts the packet sent by Host A to Host B from the network, and sends the packet encrypted by A to B. So that Host B mistakenly thinks that the intruder is Host A, then Host B sends a message that should be sent to A to the intruder posing as A.

3) Integrity: Integrity refers to the fact that information remains non-modified, non-destructive, and non-lost during transmission, exchange, storage, and processing, that is, information is kept intact, so that information can be correctly generated, stored, and transmitted. These features pose certain challenges to information security, such as a single point of failure and network congestion. Traditional data integrity schemes include symmetric key methods and public key infrastructure (PKI). Current solutions can also ensure data integrity through distributed data authentication in blockchains.

III. IOT SECURITY MODEL

There is still a problem with the Internet of Things that do not form a security architecture, while IoT has experienced nearly 20 years of development. From the rudimentary structure of a theory to the current industrial application, this technology has undergone earth-shaking changes, but the security problems brought by this technology are becoming more and more serious. The model proposed by the security threat is also a continuous change. From the development of the IoT security model, the interesting phenomenon is that the main models at this stage are mainly three-tier architecture. Whether it is from the traditional three-tier architecture or the development to the later cloud computing-based architecture, edge computing fog computing architecture. And the SDN-based IoT architecture is a three-tier architecture-based architecture. In addition, the security architecture has evolved to date. Based on these typical architectures, IoT combined with blockchain or artificial intelligence has also been proposed [20], [21]. Each architecture has its own advantages and disadvantages, and today's IoT does not have a ubiquitous architecture, but there are unique solutions to the threats of each architecture.

A. Traditional Architecture

The traditional three-tier IoT model is divided into three layers: the perception layer, the network layer, and the application layer [3]. The sensing layer is used to identify objects and collect information, upload to the network layer for storage processing and forward to the application layer.

This traditional IoT architecture can also be extended to four layers: the perception layer, the transport layer, the processing layer, and the application layer. The transport layer of this architecture corresponds to the network layer of the above three-layer architecture, but the application layer is further divided into the processing layer and the application layer. The processing of data and the application of data are more detailed in terms of processes and methods. Frankly, the nature of the difference is no different.

The biggest drawback of this traditional three-tier architecture is that each layer corresponds to different security threats. For example, the sensing layer has RFID security, sensor network security, and terminal device security. The network

layer has wireless access security and other core network or cloud computing server security, including authentication and encryption mechanisms and security threats at the access control level. The application layer involves the privacy protection of users and the security of key management.

B. Current Mainstream IoT Architecture

Cloud and Edge Computing Paradigm: with the development of the Internet of Things, IoT devices continue to increase. Meanwhile, data at the edge of the network is gradually increasing. Cloud processing centers need to process massive amounts of data. This is not only a challenge for the processing power of cloud servers but also a high challenge for data processing and high processing efficiency. We found with the development of IoT, many new computing models are constantly being proposed because cloud computing is not always efficient. The literature [22] points out that this computational model is more efficient if we can process and analyze data at the edge nodes of the network.

The general edge calculation paradigm proposed by PeiYun Zhang et al. solves this problem well, and the architecture is shown in Fig.2 [23]. This structural feature of edge nodes consumes minimal response time, reduces network load, and ensures the privacy of user data when processing data.

General edge computing structure is divided into three layers: cloud layer, edge computing layer and terminal layer. Between the cloud layer and the edge computing layer, a core network provides network services. Each edge node is connected to the cloud, and each device is connected to the edge node. The edge nodes can communicate with each other to form a honeycomb. The terminal layer consists of mobile and fixed IoT devices (media, machines, and smartphones). Each device is connected to an edge node, and the locally collected data is sent to the edge node first. The edge computing layer is located at the edge of the network and consists of a large number of edge nodes (including routers, gateways, access points, base stations, etc.). The layer aims to extend cloud computing to the edge of the network and has certain computing and storage capabilities. The cloud is the center of the network, a remote control management center for complex but not urgent tasks. In the whole architecture, the edge node sends a request to the cloud center, and the cloud center returns relevant data to the edge node.

With the continuous research on the edge calculation, the concepts of fog calculation, mobile edge calculation, and mobile cloud computing are proposed. Paper [24] points out the differences between these architectures. Fog calculation is currently a hotspot area for researching the Internet of Things. It is also a three-layer architecture. The edge device layer is called the fog layer in the fog computing structure. At this time, the edge node is also called the fog node. The fog node has short storage capacity and has higher storage and buffering capacity than the edge. When calculating a complex and long-period calculation, the fog node is sent data through various communication technologies(eg 4G, 5G, WIFI, etc.) to the clouds. This structure is characterized by geographical distribution, low latency, emergency processing, and location awareness.

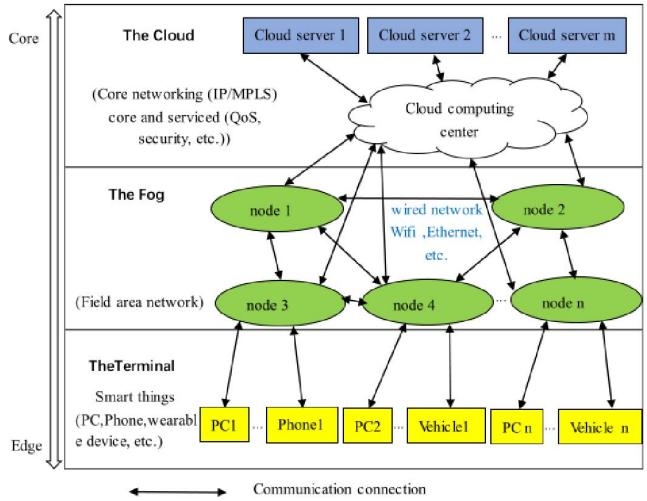

Fig. 2. General Edge Computing Paradigm.

C. Edge Computing Extended Architecture

1) SD-IoT Architecture: The paradigm of edge computing has not been widely used at this stage. The main reason is its resource constraint. The computing resources of the edge device layer have limited storage resources and load capacity, and can only execute lightweight algorithms. In this regard, Kalkan, Kubra et al. [25] proposed architecture of SDN technology. SDN is a new network architecture with data control separation and software programming. It is also a three-layer network architecture consisting of a control plane, data plane, and control management plane. The centralized control plane and the distributed forwarding plane are adopted. SDN flexibly defines the forwarding function of the network device by writing software and includes multiple interface protocols. The southbound interface protocol implements the interaction between the SDN controller and the SDN controller. Use the northbound API to implement the interaction between the application and the SDN controller. Since the SDN architecture is a distributed structure in the forwarding plane, it can be perfectly integrated with the geographically distributed edge computing architecture.

Fig.3 is a new architecture for SDN and edge computing architecture, called SD-IoT architecture [26]. This framework is divided into three layers: application layer, control layer, and infrastructure layer. The control layer is the core of the architecture. A number of SD-IoT controllers form a control pool, and the controller is responsible for centralized control of the IoT logic. The control pool is divided into the vertical control architecture of the main control layer and the basic control layer. The main control layer is responsible for resource management and controls some controllers of the basic control layer. The underlying control layer is responsible for load balancing, each controller is connected to an edge

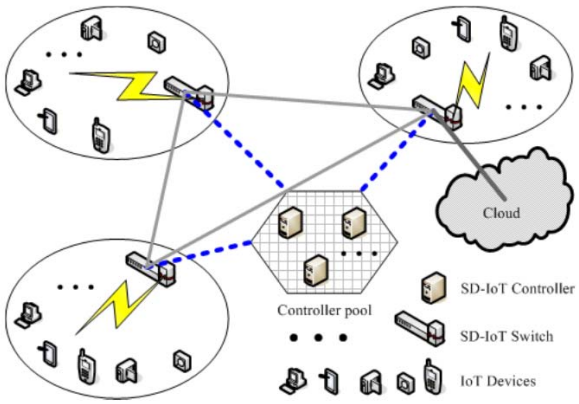

Fig. 3. General Edge Computing Paradigm.

node. The load balancing algorithm is used to coordinate the messages in the master to achieve load balancing of the IoT. Although this architecture can reasonably alleviate some resource-constrained shortcomings, it also brings some more threats. For example, this architecture is vulnerable to DDoS attacks.

2) Fog Orchestration Architecture: The three-layer fog calculation orchestration architecture proposed in [26] makes the edge computing architecture specific and enables the IoT architecture to implement the decentralization process. Hsu, Ruei-Hau et [27] proposed a reconfigurable security framework based on edge computing, which implements the field of Internet of Things by applying GKMS (Global Key Management System), AAA system (authentication, authorization, and accounting), key management and authorization authentication functions.

3) Local Difference Privacy Obfuscation : The six-layer edge computing intrusion detection model proposed by Lin, Fuhong et al. in [36], describes the computing resource allocation scheme of edge computing nodes. They address the challenge of edge computing resource allocation and proposes general edge computing IDS architecture. [37] proposed a local differential privacy confusion framework, which aggregates and refines IoT data information on the edge side without revealing user sensitive data. Each edge server applies the LDPO framework to the data to protect the privacy, then extracts the data and sends it to the cloud server. Although these architectures are perfect, they only stay in the architecture stage, and the implementation is still facing certain difficulties. Because of the security model of edge computing, there are three major security threats at present: physical equipment threats, network communication threats and lack of effective tools for data security defense.

4) New Architecture: In order to solve the problem of traffic security authentication in the Internet of Things, the edge computing security model based on the combination of SDN and blockchain has also been proposed by [38] . They see a new blockchain-based distributed cloud model that takes four steps on top of the SD-IoT three-tier architecture: selecting resource providers, providing services, registering transactions, and paying for data [26]. After delivering, they used Software Custom Network (SDN) enables controller edge nodes at the network edge to meet design requirements such as reduced latency, transmission efficiency, and efficient matching scheduling. With the combination of blockchain, [39] proposes a comprehensive model of human artificial intelligence. The model proposed by them is mainly aimed at the future of the explosive growth of IoT data, because the traditional intrusion detection model is no longer practical. They use the bat algorithm's group partitioning and binary differential variability to select typical features and use a random forest adaptive algorithm to classify traffic to achieve intelligent attack detection. The security model requires interoperability, adaptability, decentralization, and contextualization. The model proposed by Pierre et al. [40] adapts to these security requirements and proposes a self-managing security unit security model SMSC (Self Managed Security). This is a service-oriented architecture that stays in the architectural theory phase and is not easy to implement. The literature [41] proposes a novel dynamic defense mechanism: Artificial Immune System (AIS) artificial immune system, which simulates the defense mechanism of immunology compared with the traditional network security model and is applied in the field of information security.

This section reviews the traditional three-tier architecture, edge computing architecture, SD-IoT architecture, and other architectures, and compares the strengths and weaknesses of these architectures to the conclusion that the IoT architecture is not fully mature. Security threats are the premise of the IoT architecture, and this is the trend of IoT architecture in the future.

IV. Solutions

The IoT security model does not currently have a truly unified architecture. On the one hand, it has the same threats for different architectures, such as DDoS attacks, privacy leaks, etc. There are also some security threats unique to the model, such as resource constraints of the edge computing architecture, node replacement threats, etc. On the other hand, the characteristics of IoT security have the same confidentiality, integrity, availability, and controllability as traditional network features. But IoT has resource-constrained physical characteristics and heterogeneous network features unique to IoT security. The literature [8] proposes some solutions based on these characteristics, but this review method is not comprehensive. For example, access control may involve both confidentiality and controllability. The defense of DDoS attacks may also involve resource constraints. There are two aspects of physical threats and heterogeneous network characteristics. Therefore, in order to better explain the current research of IoT security, this section will analyze the three aspects of access control and privacy protection, intrusion detection, and traffic detection methods and resource constraints and allocation schemes.

TABLE II
COMPARISON OF IOT SECURITY SOLUTIONS

Ref	Solutions	Methods
[28], [29]	Access control and privacy protection	Control methods: network access control, permission control, directory level security control,attribute security control, server security control, independent access control,mandatory access control androle-based access control and Mandatory access control and role-based access control Privacy issues:Physical security, smart tags, and encryption
[30]–[33]	Intrusion detection and traffic detection methods	Intrusion detection methods: Misuse detection, anomaly detection, specification detection, mixed detection and semi-supervised fu -zzy mean value (ESFCM) methods Intrusion Detection System : mIDS, BMIDS,MDSClone,Exception based IDS,Signature based IDS,Behavior -based IDS Real-time extraction flow time series: Anonymous Data Transfer Flow Detection Method, Linear search LS, Recursive Search DStrie, Collection Clip DStries, Respectively Based On Host and Network-based Architecture Classify Log File Suspicious Packages
[34]–[36]	Resource constraint and allocation plan	Distribution methods: on-demand security configuration technology, load balancing scheme, edge node computing resource allocation and remote security management server.Lightweight algorithms: ultra -lightweight cryptographicalgorithms, hardware parallelizable light -weight cryptographic algorithms, software parallelizable lightweight cryptographic algorithms, lightweight public key cryptographic algor -ithms, unbalanced public key cryptographic algorithms, and some lightweight security protocols.DDoS solutions: target IP address entropy based DDoS attack detection scheme, cosine similarity rate algorithm, DPPC algorithm, flow control, anomaly based detection scheme.

Table II compares these solutions. Access control is the main strategy for network security prevention and protection. Its main task is to ensure that network resources are not illegally used. It is one of the most important core strategies for ensuring network security. It has access control, access control, directory-level security control, role-based access control and more. This is the first pass for IoT information security. Data encryption is the second defensive line for information security, involving some lightweight encryption algorithms. The intrusion detection method is the most important part of the entire IoT security category. This solution not only detects system vulnerabilities after the intrusion but also prevents the attack source from being attacked before the attack occurs. The resource constraints mentioned in the previous section are one of the biggest challenges in deploying the distributed IoT security model at this stage. In response to the resource constraints of IoT devices, in addition to using lightweight algorithms, the rational allocation of resources is also a solution. The IoT security threats are both physical and network-level. Only when the requirements of these three levels are resolved, the IoT security is guaranteed.

V. CONCLUSION

Based on a review of a large number of related literature, this paper synthesizes the mainstream IoT security model at the present stage. We analyze the threats and challenges of IoT security from the perspectives of IoT physical and network characteristics. From the perspective of privacy protection, intrusion detection, and distribution schemes, some solutions that are effective at this stage are proposed. With the combination of edge computing, SDN technology and AI, IoT security problems will be more and more easy to solve. In order to develop IoT steadily, it is necessary to pay more attention to the security of the Internet of Things. Especially at this stage, the main structure of the Internet of Things is in full bloom, and there is no unified critical period. The standardization of the IoT security model plays a decisive role. As computing moves closer to the underlying device to process information in real time, edge computing architectures will increasingly dominate. The combination of SDN and edge computing is a good example of IoT security architecture. Then combined with Docker container technology, the lightweight algorithm is applied to the Internet of things gateway [42]. This kind of data plane distributed control plane centralized and lightweight algorithm implementation, not only in academia but in the Industrial Internet of Things will also be a perfect example of the combination.

VI. ACKNOLEDGE

We would like to thank all of the team members and those who has helped this work. This work is supported by the National Key R&D Program of China (2016YFB0800805), the Major Projects of Science and Technology Service Industry in Tianjin (16ZXFWGX00140), the Open Project Foundation of Information Security Evaluation Center of Civil Aviation, Civil Aviation University of China (NO. CAAC-ISECCA-201501), and the Natural Science Foundation of Tianjin (No. 18JCQNJC69900).

REFERENCES

[1] T. I. Murphy, "Line spacing in latex documents," http://www.sohu.com/a/254853203_804262/, accessed April 4, 2010.

[2] H. Zhang and L. Zhu, "Internet of things: Key technology, architecture and challenging problems," in *2011 IEEE International Conference on Computer Science and Automation Engineering*, vol. 4. IEEE, 2011, pp. 507–512.

[3] L. Li, "Study on security architecture in the internet of things," in *Proceedings of 2012 International Conference on Measurement, Information and Control*, vol. 1. IEEE, 2012, pp. 374–377.

[4] J.-H. Han, Y. Jeon, and J. Kim, "Security considerations for secure and trustworthy smart home system in the iot environment," in *2015 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2015, pp. 1116–1118.

[5] M. Schiefer, "Smart home definition and security threats," in *2015 ninth international conference on IT security incident management & IT forensics*. IEEE, 2015, pp. 114–118.

[6] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. D. Hai, "Recent challenges, trends, and concerns related to iot security: An evolutionary study," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2018, pp. 405–410.

[7] M. Alrowaily and Z. Lu, "Secure edge computing in iot systems: Review and case studies," in *2018 IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE, 2018, pp. 440–444.

[8] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," *IEEE Communications Surveys & Tutorials*, 2019.

[9] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[11] J. Kim and H. Kim, "Security vulnerability and considerations in mobile rfid environment," in *2006 8th International Conference Advanced Communication Technology*, vol. 1. IEEE, 2006, pp. 801–804.

[12] I. Bedhief, M. Kassar, and T. Aguili, "Sdn-based architecture challenging the iot heterogeneity," in *2016 3rd Smart Cloud Networks & Systems (SCNS)*. IEEE, 2016, pp. 1–3.

[13] K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Communications Magazine*, no. 99, pp. 1–7, 2017.

[14] L. Sidki, Y. Ben-Shimol, and A. Sadovski, "Fault tolerant mechanisms for sdn controllers," in *2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. IEEE, 2016, pp. 173–178.

[15] Z. Shi, K. Liao, S. Yin, and Q. Ou, "Design and implementation of the mobile internet of things based on td-scdma network," in *2010 IEEE International Conference on Information Theory and Information Security*. IEEE, 2010, pp. 954–957.

[16] A. W. Atamli and A. Martin, "Threat-based security analysis for the internet of things," in *2014 International Workshop on Secure Internet of Things*. IEEE, 2014, pp. 35–43.

[17] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[18] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," in *2009 7th International Conference on Information, Communications and Signal Processing (ICICS)*. IEEE, 2009, pp. 1–5.

[19] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber scanning: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1496–1519, 2014.

[20] D. Fakhri and K. Mutijarsa, "Secure iot communication using blockchain technology," in *2018 International Symposium on Electronics and Smart Devices (ISESD)*. IEEE, 2018, pp. 1–6.

[21] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. D. Hai, "Recent challenges, trends, and concerns related to iot security: An evolutionary study," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2018, pp. 405–410.

[22] L. S. Guan Xin, Li Lu, "Research on edge computing for internet of things," 2018.

[23] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Generation Computer Systems*, vol. 88, pp. 16–27, 2018.

[24] M. L. R. S. L. F. An Xingshuo, Cao Gui, "Intelligent edge computing security review," *Science of Telecom*, vol. 34, no. 7, pp. 135–147, 2018.

[25] K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Communications Magazine*, no. 99, pp. 1–7, 2017.

[26] D. Yin, L. Zhang, and K. Yang, "A ddos attack detection and mitigation with software-defined internet of things framework," *IEEE Access*, vol. 6, pp. 24 694–24 705, 2018.

[27] R. H. Hsu, J. Lee, T. Q. S. Quek, and J. C. Chen, "Reconfigurable security: Edge-computing-based framework for iot," vol. 32, no. 5, 2017.

[28] L. Lin, T.-T. Liu, S. Li, C. M. S. Magurawalage, and S.-S. Tu, "Priguarder: A privacy-aware access control approach based on attribute fuzzy grouping in cloud environments," *IEEE Access*, vol. 6, pp. 1882–1893, 2018.

[29] T. Hänel, A. Bothe, R. Helmke, C. Gericke, and N. Aschenbruck, "Adjustable security for rfid-equipped iot devices," in *2017 IEEE International Conference on RFID Technology & Application (RFID-TA)*. IEEE, 2017, pp. 208–213.

[30] P. J. H. Rathore, Shailendra, "Semi-supervised learning based distributed attack detection framework for iot," 2018.

[31] P.-Y. Lee, C.-M. Yu, T. Dargahi, M. Conti, and G. Bianchi, "Mdsclone: multidimensional scaling aided clone detection in internet of things," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2031–2046, 2018.

[32] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.*, vol. 3. IEEE, 2005, pp. 253–259.

[33] F. Anjum, D. Subhadrabandhu, S. Sarkar, and R. Shetty, "On optimal placement of intrusion detection modules in sensor networks," in *First International Conference on Broadband Networks*. IEEE, 2004, pp. 690–699.

[34] S. Yoon and J. Kim, "Remote security management server for iot devices," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2017, pp. 1162–1164.

[35] D. Puthal, R. Ranjan, A. Nanda, P. Nanda, P. P. Jayaraman, and A. Y. Zomaya, "Secure authentication and load balancing of distributed edge datacenters," *Journal of Parallel and Distributed Computing*, vol. 124, pp. 60–69, 2019.

[36] F. Lin, Y. Zhou, X. An, I. You, and K.-K. R. Choo, "Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of internet of things devices," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 45–50, 2018.

[37] C. Xu, J. Ren, D. Zhang, and Y. Zhang, "Distilling at the edge: A local differential privacy obfuscation framework for iot data analytics," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 20–25, 2018.

[38] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[39] J. Li, Z. Zhao, R. Li, H. Zhang, and T. Zhang, "Ai-based two-stage intrusion detection for software defined iot networks," *IEEE Internet of Things Journal*, 2018.

[40] P. De Leusse, P. Periorellis, T. Dimitrakos, and S. K. Nair, "Self managed security cell, a security model for the internet of things and services," in *2009 First International Conference on Advances in Future Internet*. IEEE, 2009, pp. 47–52.

[41] C. Liu, Y. Zhang, and H. Zhang, "A novel approach to iot security based on immunology," in *2013 Ninth International Conference on Computational Intelligence and Security*. IEEE, 2013, pp. 771–775.

[42] M. Alam, J. Rufino, J. Ferreira, S. H. Ahmed, N. Shah, and Y. Chen, "Orchestration of microservices for iot using docker and edge computing," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 118–123, 2018.