Overview of IoT Security Architecture

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

2nd Huanran Jin
School of Computer Science and Engineering
Tianjin University of Technology
Tianjin, China
358287106@qq.com

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

4rd 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 the Internet of Things, services can be provisioned using centralized architectures, where central entities acquire, process, and provide information. Alternatively, distributed architectures, where entities at the edge of the network exchange information and collaborate with each other in a dynamic way, can also be used. In order to understand the applicability and viability of this distributed approach, it is necessary to know its advantages and disadvantages not only in terms of security and privacy challenges. The purpose of this paper is to show that IoT three-layer security logic architecture and the distributed approach has various challenges that need to be solved, but also various interesting properties and strengths. It also focuses on security issues such as privacy protection and intrusion detection, etc.We also propose a high-level security management scheme based on blockchain for different IoT devices in the full life cycle. It also summarizes the main causes of the deficiencies and security problems in existing research work.**

***Index Terms*—distributed architectures, centralized architectures, security, privacy, blockchain**

I. Introduction

Since the International Telecommunication Union officially proposed the concept of Internet of Things (IoT) in 2005, technologies such as sensor networks, cloud computing, and microchips have matured over time, and the Internet of Things industry has also rapidly expanded. According to the latest statistics of the Statista portal, the number of connected devices has reached 17.6 billion in 2016 and is expected to exceed 30 billion by 2020. International Data Corporation predicts that the Internet of Things market will exceed $7 trillion by 2020. While the Internet of Things is developing at a rapid pace, its security is also facing severe challenges. At present, countries, enterprises and individuals have not established enough awareness of IoT security and privacy protection. The IoT security issue will not only bring property damage to users but also threaten the lives of users.

In the environment of the Internet of Things, a centralized architecture can be used to provide services, which essentially capture, process, and transmit information in a central entity. In addition, a distributed architecture in which entities at the edge of the network exchange information and collaborate in a dynamic manner can also be used. In order to understand the applicability and feasibility of this distributed method, it is necessary to know its advantages and disadvantages. In addition, not only the characteristics but also the threats and corresponding solutions in terms of security and privacy need to be understood in detail.Integrating the IoT with blockchain will have many advantages. For instance, adopting the decentralized architecture for the IoT system can solve many issues especially security and single point of failure, since the blockchain provides a decentralized and distributed environment where there is no need for a central authority to manage the execution of operations and control communication between various nodes in the network. This, in turn, provides a trusted environment where participating nodes are the only entities to accept or discard a transaction based on their consent Moreover, the blockchain provides better security for various IoT applications since it provides an immutable and tamper-proof ledger to protect data against malicious attacks in which any data update or modification will not be added to ledger unless the majority of participating nodes verify it.

II. Related Work

Whether it is the latest service-oriented IoT architecture or the 4 or 5 layer IoT architecture that further divides the application layer, its essence can be divided into three logical levels. From bottom to top, it is perception layer, network layer and application layer. This section introduces the level of the IoT architecture firstly, and then introduces its security issues and research status at different levels.

A. Perception Layer Security Issues and Research Status

The main task of the perception layer is to perceive external information comprehensively. Its equipment mainly includes various types of sensors (such as infrared, ultrasonic, humidity), image capturing devices (cameras), etc. And the information collected by these devices will be directly processed and applied. Security issues that may be encountered at the perception layer include the following situations, with

978-1-7281-4528-0/19/$31.00 ©2019 IEEE
DOI 10.1109/DSC.2019.00058

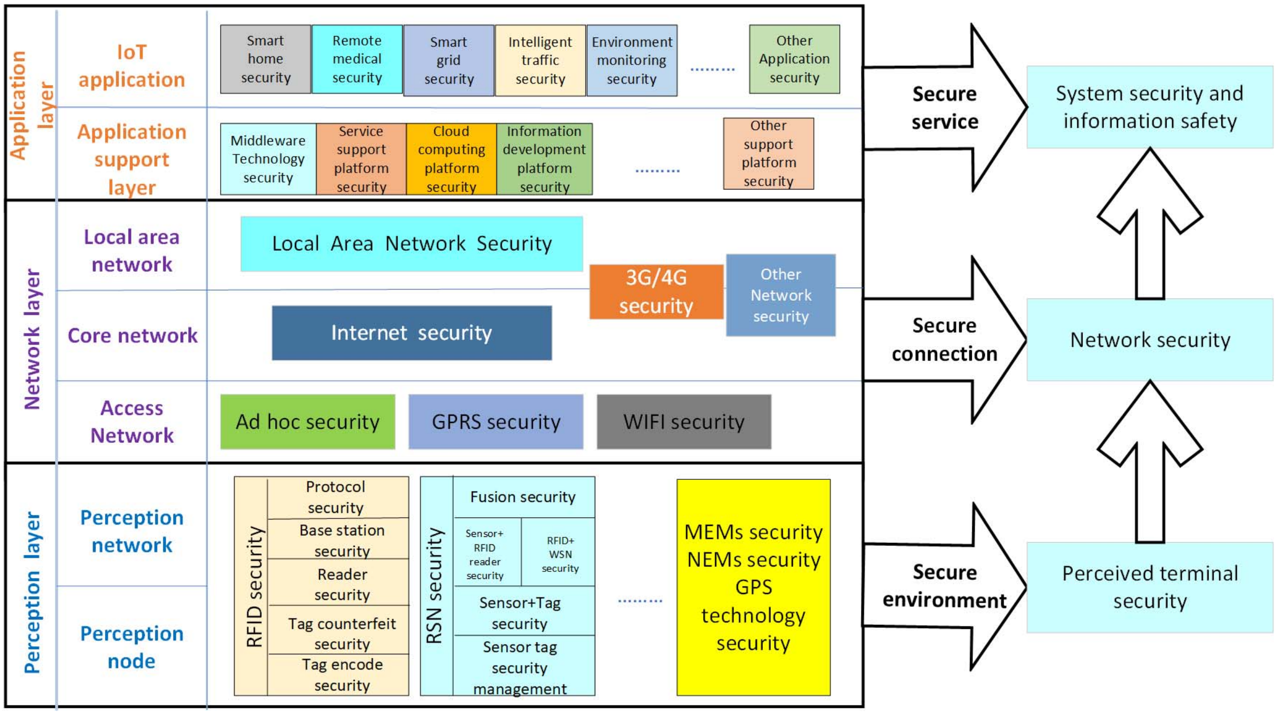

Fig. 1. Typical IoT Security Architecture.

radio frequency identification. Related issues include protocol security, base station security, tag forgery, and tag encryption security. Issues related to wireless sensors include routing protocol security, cryptographic algorithms, and trusted management of nodes. Also included are some MEMs safety and NEMS safety and so on.

Costin et al. discovered many exploitable high-risk system vulnerabilities by analyzing a large number of embedded device system firmware. Some researchers have proposed to establish a lightweight trusted execution environment in embedded systems to protect their system security, but this method has a large computational cost and limited application scope. Researchers have also designed a test framework for small embedded device systems [1], but static testing and vulnerability detection methods cannot dynamically protect the system security of embedded devices in real time. Majzoobi and Hiller's research team proposed authentication based on the unique physical characteristics of the device [2] and key generation protocol [3]. This method not only saves the device resources for storing keys separately but also effectively resists side channel attacks. Some researchers also use the characteristics of the user's human body acquired by the wearable device such as gait, sliding screen strength [4], etc. to achieve device authentication. This method can realize the dual authentication of the device and the user while saving resources.

In summary, the security requirements of the perception layer are interdependent. For example, a researcher analyzes the electrical signal information entropy based on the heart rate generation key through the side channel [5], thereby restoring the user's heart rate information and acquiring the communication key. Therefore, it is necessary to fully consider the security requirements of various aspects of the perception layer's devices and the mutual influences in order to design an effective security defense strategy.

B. Network Layer Security Issues and Research Status

The network layer is mainly responsible for transmitting the information received by the perception layer to the application layer safely and efficiently. The network layer mainly includes the network infrastructure, including the Internet, mobile networks and some professional networks (such as broadcast television networks and national power private networks). For the network layer, it can be divided into a local area network, a core network, and an access network. Among them, access to the network needs to pay attention to GPRS security and WIFI connection security.

Many researchers have defended against sensor network attacks by lightweight cryptographic algorithms and protocols [6]. However, most of these lightweight algorithms and protocols lack testing for device power and network bandwidth consumption and the applicability needs to be improved. Although the attack on the communication channel of the network layer at this stage is still dominated by traditional network attacks (such as replay, middleman, and spoofing attacks). But it is not enough to resist these traditional cyber attacks [7]. With the development of the Internet of Things, the communication protocols in the network layer will continue to

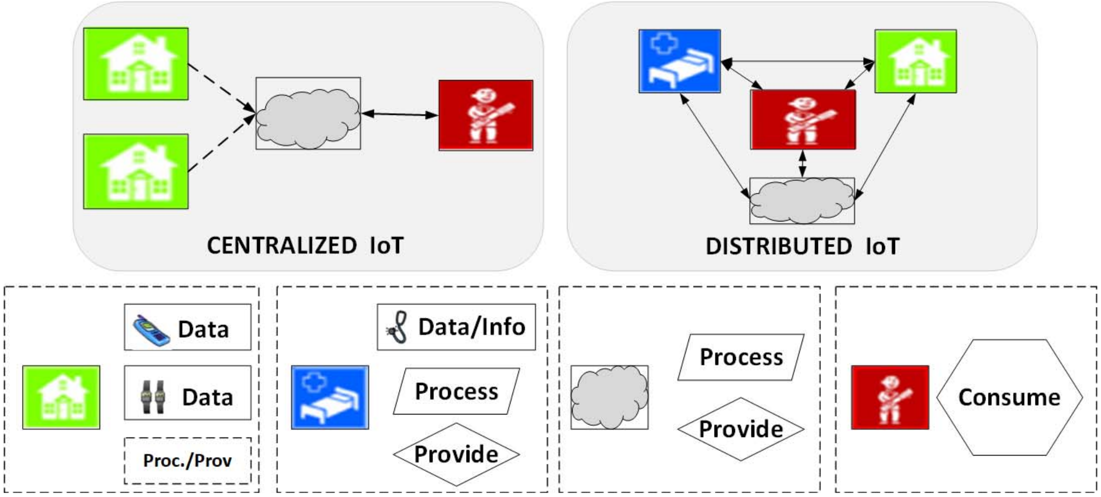

Fig. 2. Overview of The Centralized and Distribution Approaches.

increase. When data is passed from one network to another, it involves issues such as identity authentication, key agreement, data confidentiality, and integrity protection. Therefore, the security threats that will be faced will become more prominent and require more attention from researchers [8].

C. Application Layer Security Issues and Research Status

The application layer is also the core value of the Internet of Things. Typical applications such as mobile payment, smart grid, smart home and so on. The application layer can be divided into two levels to analyze, which are the IoT application and application support platform. The security that can be concerned about IoT applications includes smart grid security, telemedicine security, smart traffic security, etc. Service support platform security, middleware technology security, information development platform security, etc.

Thomas and Ned use blockchain technology for implementing anonymous sharing of IoT devices [9] worth learning. In addition, the increase in the number of IoT devices will greatly increase the scale of DDOS attacks, and the cloud server needs to improve its ability to withstand DDOS attacks [10]. For application services, it has the closest contact with users, so its most important security task is to protect user privacy information while providing services [11]. Fernandes et al. [12] found that more than 50% of applications on Samsung's smart home platform have unnecessary permissions through analysis of program source code, which may lead to user sensitive data leakage or malicious home device being maliciously controlled. Existing researchers have designed multiple access control models for sensitive operations and privacy data [13] in the protection program, but their applicability and security must be further improved.

Although the above discussion is about the security issues in the IoT architecture, the security issues at each level are not independent but interdependent. The most important aspect is the protection of data privacy. Any problem in any link will cause the user's private data to be leaked. The implementation of IoT security should include the security architecture of all IoT layers, as shown in Fig. 1.

III. Centralized and Distributed IoT Introduction

A. A Taxonomy of The Vision

In general, distributed IoT has two basic principles: 1. Intelligent location and services provided at the edge of the network. 2. Collaborate between different entities to achieve common goals.

1) Centralized Internet of Things: In this model, the data collection network is passive, and their only task is to provide data. All data will be retrieved by a central entity that will process the data into information and combine it for its customers. If the user wants to get this data, he must connect to the interface provided by this central entity by the Internet firstly.

2) Distributed Internet of Things: Under this scenario, all entities can retrieve, process, combine and provide information and services to other entities. Not only providing services locally but also working with other IoT architectures to achieve common goals. According to the electronic health example shown in the Fig. 2, following the e-health example highlighted, the IoT of a hospital can interact with the IoT located in the household of a patient, or even with the PANs of the personnel located inside the premises. Moreover, all hospitals can easily collaborate so as to obtain the overall bed occupancy. As shown in the schematic below, the house represents the intelligent family, which can generate data; the hospital bed represents the hospital, which can provide data and be able to process data; the cloud represents cloud computing, which can provide and process data; and the person represents the customers.

B. Analysis of Two Internet of Things Models

After the introduction of Section 3.1, you can see the schematic diagram of the two Internet of Things. This section

TABLE I
PROPERTIES AND REQUIREMENTS OF DISTRIBUTED AND CENTRALIZED IOT

PROP./REQ.		**CENTRALIZED IoT**	**DISTRIBUTED IoT**
Openness		High (Simple)	High (Simple)
Viability	Business Model	Already in market	Already in market
	Vendor Lock-in	Possible	Limited
Reliability	Availability	Zero if failure	Depend on resources
	Performance	Service level + latency	Service level
Scalability		Limited to cloud resources	Superior
Interoperability		Simple	High
Data management		Pull, data at cloud	Follow the push

will focus on the characteristics of the Internet of Things, as well as its advantages and disadvantages. In this analysis, we will use the various requirements and features of IoT deployments collected from existing reports and research documents. They are listed below:

Openness: In addition to providing raw data and other specialized services, the IoT platform is flexible enough to allow third parties to develop complex applications through the provided APIs.

Viability: This attribute contains two concepts, the business model (whether this technology is feasible) and the vendor lock-in (whether a company can rely on a particular vendor for a long time).

Reliability: The IoT architecture must not only be large enough to ensure a certain level of availability, but also provide performance that is tailored to the specific needs of the application.

Scalability: In the entire IoT system, the devices generated and processed by these devices are expected to grow exponentially, so we must consider scalability and scalability.

Interoperability: Even though the IoT itself is heterogeneous, all its components must be able to interact with each other. Therefore, it is necessary to implement service and semantic interoperability as well as other functions.

Data Management: Since different elements of the Internet of Things can generate large amounts of data through perception or processing, we must make certain design decisions: where the data should be stored and how it should be accessed.

Security issues: In order to implement a trusted and fault-tolerant Internet of Things, you must examine various security issues, how to maintain communication, how to manage authentication and access control in billions of things, and the privacy of users and the security of data generated by things.

Table I gives a summary of the attributes and requirements of the two IoT models. We can deduce why the centralized approach is the first to enter the market. In terms of openness, centralized solutions typically provide most of the proprietary APIs to capture and provide data. In this way, application developers can use these APIs to develop rich and complex IoT applications. In terms of availability, most companies build infrastructure through cloud companies, which typically have very good uptime. In terms of interoperability: all data sources will interact with the APIs provided by the centralized system, so you only need to create one adapter for each data source. The existence of the last profitable company proves the feasibility of this business model.

The distributed IoT approach is also important. There are some new aspects that need to be explicitly mentioned. For example, in terms of data management, the provisioning of data can follow the 'push' model (provide only when it is needed), as it is not necessary to provide all data to a central system. In terms of availability, the service uptime is more depended on how many resources are invested in maintaining the underlying IoT infrastructures, but a failure in one element of the infrastructure will not affect the whole system. As for the business model, it might be less well-defined in comparison to the model of a centralized IoT, but there are some approaches that can be taken, such as maintenance fees or management of open source services.

IV. SPECIFIC CHALLENGES

Once the analysis of the threat and attacker models is complete, we can examine the main challenges in the design and deployment of security mechanisms. In this study, we will not only introduce existing IoT security mechanisms but we will also introduce ways to provide security in a distributed IoT environment.

1) Identity and Authentication: It is important to consider how to manage identity and authentication in the Internet of Things because of multiple entities (such as data sources, service providers, information processing systems) need to authenticate each other to create trusted services. In defining these security mechanisms, we must also consider some of the inherent characteristics of the Internet of Things. Since the interactions may be dynamic, the network entity may not even know in advance which partners can be used to create a service. The Internet of Vehicles is an example: cars not only provide data to roadside equipment but also provide data to other cars.

In the centralized IoT, if there is a data provider with its own identity provider, it will be no scalability issue because such an identity provider can establish a trust relationship with the central entity (N-to-1 scheme). For distributed Internet of Things, it also meets the principles of collaboration and edge intelligence. In this scenario, a dynamic N-to-N scenario occurs where the data provider is no longer passive and can acquire and process information from other sources.

TABLE II
FEATURES OF CENTRALIZED AND DISTRIBUTED INTERNET OF THINGS IN SIX SECURITY AREAS

Security challenges	**Centralized IoT**	**Distributed IoT**
Identity and Authentication	N-to-1	N-to-N
Access control	Homogeneous policies	Heterogeneous policies
Protocol and Network Security	Known centralized provider	Unknown peers
Privacy	Less flexible	More flexible
Trust management	Holistic point of view	More detailed information
Governance	Less flexible, more simple	More flexible, more complex
Fault tolerance	Holistic point of view	Detailed point of view

2) Access Control: Specific services are built by aggregating multiple services and data sources from different locations and contexts (e.g. hospitals that retrieve information from home patients and ambulances). All these information providers have their own access control policies and the lifecycle (creation, execution, maintenance, translation) of each task needs to be managed. For example, in the event of an accident, everyone at the scene of the accident can access my blood type, but only certified doctors and nurses can access my vital signs.

With authentication, access control policies are easier to manage in a centralized IoT architecture, and all access control policies are stored in a central entity for management. As a side effect of this configuration, both the data provider and the information consumer must fully trust the central entity. On the other hand, the purely distributed IoT architecture needs to address all the aforementioned challenges: management of heterogeneous policies, multiple implementations.

3) Protocol and Network Security: A secure communications channel is, in most cases, a byproduct of a successful authentication (e.g. server authentication or mutual authentication using protocols such as TLS/DTLS). There are some additional challenges related to the computational resources available to things. When opening a secure channel, devices should be able to negotiate the actual parameters of that channel, such as algorithms (e.g. RSA vs. ECC), strength (AES-128 vs. AES-256), and protection mechanisms (only integrity vs. confidentiality and integrity). The first reason is obvious: constrained devices might not be able to implement certain configurations. There is another reason, though: adaptability. Depending on various factors such as the level of criticality of the data, it might not be necessary to apply strong protection mechanisms to a particular information flow (e.g. confidentiality and the on/off status of a streetlight). Another challenge is the need to analyze the number of security protocols that can be implemented within a constrained device.

4) Privacy: So far, distributed data architectures require more sophisticated security mechanisms. However, distributed Internet of Things offers immediate benefits in one area: data management and privacy. For centralized IoT architectures, including those that follow the principles of collaboration, data providers can also decide whether to share a particular data stream. If the centralized architecture conforms to the edge intelligence principle, another approach can be used: since data providers and recipients of information can communicate directly, they may negotiate a set of keys to protect their information. However, in this case, the central entity cannot process the data, so it becomes a simple storage system unless it implements an advanced encryption mechanism that can manipulate encrypted data, such as homomorphic encryption.

5) Trust and Governance: In a centralized IoT, uncertainty comes from interactions with data providers, and the overall view of the central entity can help calculate the credibility of other entities (for example, if all nearby sensors provide lower values, the radiation sensor Cannot issue a warning). However, if different central entities collaborate with each other, they must be able to exchange trust information in order to fix inconsistencies in reputation values. In a distributed Internet of Things, there is uncertainty as to whether it interacts with the data provider or with the service provider. Distributed infrastructure makes trust management more complex: how to calculate and share reputation and trust? Which ontology should be used? Can you trust reports from other systems?

6) Fault Tolerance: Many things can go wrong and stop working, but they can also send fake or even manipulated data. Therefore, in the context of the Internet of Things, it is necessary to consider fault tolerance. In a centralized IoT architecture, this task is much simpler because the central entity will access all data streams. For a distributed IoT architecture, a discovery mechanism that accurately locates the relevant data streams needs to be developed. A centralized system can analyze the consistency of data and pinpoint which data providers are behaving irregularly. Distributed systems can utilize additional information retrieved at the local level (such as network information) or apply advanced intrusion detection systems in interaction with other entities.

The prescriptiveness and heterogeneity of distributed methods increase the complexity of most security mechanisms (identity and authentication, access control, protocol and network security, trust management, and fault handling). Table II also summarizes the characteristics of these two programs in various fields.

V. APPROACHES

1) Identity and Authentication Approaches: As mentioned above, it is important to manage the identity of things in a scalable manner. Therefore, devices should be able to use their own attributes and tag their identity in the environment they belong to. In an environment, the local identity provider can manage the identity of these devices and can also establish trust relationships with related external resource providers (e.g. common patients, other hospitals). For example, Guinard et al. [14] proposed an intelligent gateway infrastructure (social access controller, or SAC) that allows users to retrieve data from local sensors using their social network (e.g. Facebook). Note that this approach may not work if humans do not interact directly with the IoT entity. In this case, it is necessary to develop an agent mechanism that can represent human users. Another example is the concept of digital shadows [15], where users can delegate their credentials (including access control credentials) to multiple objects or virtual entities.

2) Access Control Approaches: The distributed IoT access control strategy has made little progress in management. In fact, it is not easy to apply existing access control methods to a fully distributed environment. For example, there are scalability and consistency issues when storing user lists and their associated access rights in an access control list. When things belong to a certain category, various simple strategies can be used. For example, the access control logic can be pushed to a specific trusted entity, and RBAC policies using attribute certificates [16] need to allow such certificates to be verified in a cross-domain environment. However, please note that due to the specific nature of the Internet of Things, certain factors can be considered as part of the access control model. Therefore, there is sufficient technical support, certain policies (for example, only authenticated users who are close to me during business hours can access today's reports) can be easily implemented. In addition, an access control logic can be pushed to specific trusted entities that will act as token-granting services in Kerberos (one thing will be granted access with a valid signature created by a trusted entity).

3) Protocol and Network Security Approaches: In fact, the security of IoT-designed Web transport protocols such as CoAP (Restricted Application Protocol) relies heavily on the implementation of these security protocols, and some protocols can be implemented without any major modifications. However, due to the complexity of its design, other prototypes need to be adjusted. Such a protocol must compromise between simplicity and compatibility. For example, one approach attempts to apply IPsec to a constrained environment by balancing link layer security and IPsec security [17].

For the distribution of certificates, any contents belonging to a particular local group may have one or more entities responsible for managing and distributing credentials. These protocols can provide good features, such as high resiliency to attacks [18]. In addition to optimization, many researchers are looking to implement fast and compact cryptographic algorithms, from designing new hash functions and symmetric algorithms [19] to optimizing existing primitives.

4) Privacy Approaches: The distributed IoT approach facilitates the implementation of privacy design principles because all entities can manage their own data directly. As far as people are concerned, aspects such as the availability of the user interface (such as what can be accessed and to what extent) should be considered [20].It is also necessary to study the applicability of existing secure distributed data mining algorithms. For example, some privacy enhancement technologies (PETs), such as multiparty computing [21], can be used to provide protection for eco-operational protocols.

In short, input and output items need to be scanned for rogue devices and malware that could threaten user privacy. A framework like uTRUSTit might help in this regard. In addition, existing research on monitoring systems such as CCTVs [22] may also provide clues to the specific legal challenges that our society will face after the Internet of Things becomes a reality.

5) Trust and Governance Approaches: A promising approach is to establish a circle of user-managed trusts, as described by Robinson et al. in the shoppingLense system. The system increases user trust in the Internet of Things by including trusted metadata in the information flow. In particular, patterns (such as QR codes) located in an environment (such as a shopping mall) are digitally signed and owned by a user-defined group. Members of this group can also add ratings to a standard mode. In this way, if the user trusts a particular group, information can be obtained from the mode, or a trusted rating can be obtained from other users. Finally, uTRUSTit [23] has achieved promising results in this area in terms of user trust in the system. In particular, the framework developed by this project not only provides a directory of local devices connected to the Internet of Things but also enables users to understand their own state and allow the creation of a mental model of the virtual world.

6) Fault Tolerance Approaches: There are also a variety of theoretical platforms designed to provide service discovery, discovery and synthesis mechanisms for the Internet of Things. Using a local cluster can help with this task: if the entities are clustered in a local group, the cluster can incorporate mechanisms that not only provide up-to-date information about local things, but also support different through specialized middleware [24]. Service discovery protocol interactions, in addition, all these services can take advantage of the functionality provided by existing security mechanisms, such as trust management. Implement a new detection mechanism that takes into account the specific attack model of the distributed Internet of Things. In addition, the experience can be learned from existing distributed intrusion detection systems that are implemented in similar environments, such as smart grids [25].

VI. Blockchain Based IoT Security Architecture

Blockchain has been applied to the IoT in the last two years. Now block chains have been used in the Internet of Things. These works use the advantage of blockchain centralization to design a fair and credible management platform or key distribution platform without third party. It break through the limitations of the third party centered, and achieve the high efficiency of processing. However, these works do not consider the threat traceability of IoT terminal life cycle. Furthermore, the life cycle of IoT terminal devices (e.g., different sensors or mobile devices) is different. Thus, in the life cycle of these

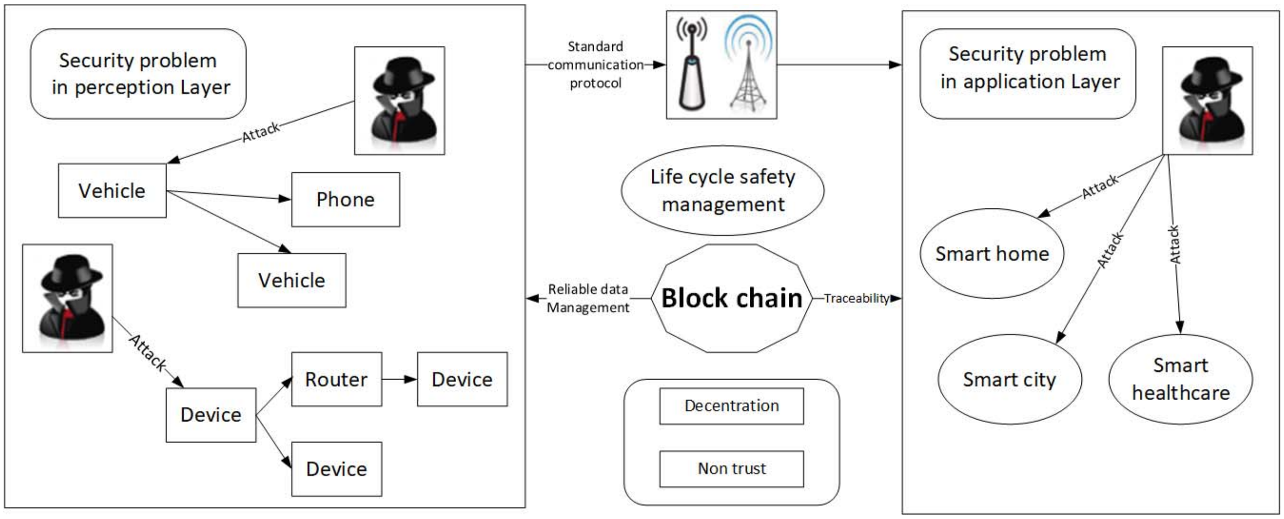

Fig. 3. Blockchain Enhanced IoT Security Architecture.

terminals, how to achieve effective threat traceability can help to avoid unnecessary leakage of security and privacy issues in the actual deployment of devices for IoT. However, due to the different terminal life cycle, centralization is usually used to trace the source, which leads to the waste of resources. Therefore, how to use blockchain to deal with it is a challenge problem.

Utilizing blockchain to enhance the security of IoT is shown in Fig. 3. We can see that the blockchain is applied to the threat traceability of the IoT devices, which involves the interaction between IoT devices and network. transmission, as well as between IoT devices and cloud. For the IoT devices and network transmission, the problems include how to identify malicious hot spots, malicious terminal access, abnormal traffic monitoring, etc. For the IoT device and cloud, the problems include how to achieve identity authentication, etc. In view of the above problems, the implementation of traditional security measures usually requires trusted third party, which results in resource consumption. Therefore, the technology of blockchain can be applied to realize the implementation of the above security policy without the third party. For example, the identity authentication mechanism between the IoT device and the cloud may require third parties to distribute the key.

However, with the increase of IoT devices, there are massive IoT terminals. Therefore, plenty of computing power at terminals would necessarily be consumed based on traditional blockchain technology. As for IoT, problems such as computational efficiency, privacy protection, and supervision for distributed node data management in blockchain must be solved. Therefore, the establishment of blockchain based cloud platform for IoT devices management in the full life cycle can be considered, depending on the distributed cloud computation. This platform composes of IoT devices, application software, platform providers, and union nodes interconnect to each other through the high speed network. With this blockchain platform, a more efficient cryptographic algorithm will be adopted, thus guaranteeing the requirements of low latency and high throughput in data management for IoT devices. On the other hand, in terms of connections between the IoT devices and the blockchain database, device identification-based key algorithm will be adopted to guarantee security and reliability.

To summarize, currently, the works addressing the application of blockchain technology in IoT have covered only partial aspects of security. The research is still in its beginning. In Table III, we provide a comparison of the solutions based on blockchain technology. We note that the solutions deal efficiently with scalability and heterogeneity issues compared to previous approaches such as SDN and cryptographic tools. We believe that this technology will bring a lot of benefits to IoT security.

VII. Conclusion

The main purpose of this paper is to clearly analyze the characteristics and security challenges of the IoT distributed approach to understanding the status of the Internet of Things in the future Internet. Many challenges must be addressed to ensure interoperability, implement business models, and manage devices for authentication and authorization. Data is managed by distributed entities that not only push/pull data when needed, but also implement specific privacy policies. In addition, you can create additional altruistic fault tolerance mechanisms for this approach. These and other benefits show that this approach is useful and applicable to the real world. Then, we introduced blockchain based IoT security system. The design issues of this security solving methods is asset management for devices in the full life cycles based on blockchain. We study the management requirements for IoT devices, and then blockchain platform can be utilized to solve it. With the interaction between the IoT devices and the blockchain database, a device identification-based key

TABLE III
CLASSIFICATION OF BLOCKCHAIN BASED SECURITY SOLUTIONS IN IOT APPLICATIONS.

Applications	Challenges					
	Computation complexity	Communication complexity	Memory	Mobility	Heterogeneity	Scalability
Smart Grids	[26]	-	-	[26]	-	[26], [29]
Smart Cities	[9], [26], [27]	[9], [26], [27]	[9], [26], [27]	[26]	[9], [26]	[9], [26]
Transport	[26], [27]	[27]	[26], [27]	-	-	[26], [27]
Manufacturing	[9], [26], [28]	[9], [27], [28]	[9], [27], [28]	-	[9]	[9], [27], [28]
Healthcare	[9], [26]	[9], [26]	[9], [26]	[9], [26]	[9]	-

algorithm will be adopted to guarantee security and reliability. In the future, it is necessary to make suggestions on the distributed and centralized Internet of things patterns, the types of challenges and corresponding solutions on the basis of the three-layer architecture.

ACKNOWLEDGMENT

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 Natural Science Foundation of Tianjin (No. 18JCQNJC69900).

REFERENCES

[1] V. Sachidananda, J. Toh, S. Siboni, A. Shabtai, and Y. Elovici, “Poster: Towards exposing internet of things: A roadmap,” in Acm Sigsac Conference on Computer & Communications Security, 2016.

[2] M. Rostami, M. Majzoobi, F. Koushanfar, D. S. Wallach, and S. Devadas, “Slender puf protocol: A lightweight, robust, and secure authentication by substring matching,” in IEEE Symposium on Security & Privacy Workshops, 2012.

[3] M. Hiller, A. G. Önalan, G. Sigl, and M. Bossert, “Online reliability testing for puf key derivation,” in International Workshop on Trustworthy Embedded Devices, 2016.

[4] R. A. Scheel and A. Tyagi, “Characterizing composite user-device touchscreen physical unclonable functions (pufs) for mobile device authentication,” in International Workshop on Trustworthy Embedded Devices, 2015.

[5] I. Vasyltsov and S. Lee, “Entropy extraction from bio-signals in healthcare iot,” in Acm Workshop on Iot Privacy, 2015.

[6] H. Holisaz, S. Shamshiri, F. Baharvand, and S. M. Fakhraie, “A lightweight secure provenance scheme for wireless sensor networks,” in IEEE International Conference on Parallel and Distributed Systems, 2012.

[7] Y. Zhu, J. Yan, Y. Tang, L. S. Yan, and H. He, “Joint substation-transmission line vulnerability assessment against the smart grid,” IEEE Transactions on Information Forensics & Security, vol. 10, no. 5, pp. 1010–1024, 2017.

[8] Y. Zhang, Y. Xiang, X. Huang, and L. Xu, “A cross-layer key establishment scheme in wireless mesh networks,” Lecture Notes in Computer Science, vol. 8712, pp. 526–541, 2014.

[9] T. Hardjono and N. Smith, “Cloud-based commissioning of constrained devices using permissioned blockchains,” in Acm International Workshop on Iot Privacy, 2016.

[10] C. Altmeier, C. Mainka, J. Somorovsky, and J. Schwenk, “Adidos – adaptive and intelligent fully-automatic detection of denial-of-service weaknesses in web services,” in International Workshop on Data Privacy Management, 2015.

[11] M. Q. Ali and E. Al-Shaer, “Configuration-based ids for advanced metering infrastructure,” in IEEE Power & Energy Society General Meeting, 2013.

[12] E. Fernandes, J. Jung, and A. Prakash, “Security analysis of emerging smart home applications,” in Security & Privacy, 2016.

[13] P. Fremantle, B. Aziz, J. Kopecky, and P. Scott, “Federated identity and access management for the internet of things,” in International Workshop on Secure Internet of Things, 2014.

[14] D. Guinard, M. Fischer, and V. Trifa, “Sharing using social networks in a composable web of things,” in Proc of the Pervasive Computing & Communications Workshops, 2010.

[15] A. C. Sarma and J. Girão, Identities in the Future Internet of Things, 2009.

[16] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, “Identity management framework towards internet of things (iot): Roadmap and key challenges,” 2010.

[17] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, “Secure communication for the internet of things—a comparison of link-layer security and ipsec for 6lowpan,” Security & Communication Networks, vol. 7, no. 12, pp. 2654–2668, 2015.

[18] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, “Key management systems for sensor networks in the context of the internet of things,” Computers & Electrical Engineering, vol. 37, no. 2, pp. 147–159, 2011.

[19] “Browse by series: Ecrypt ii european network of excellence in cryptology ii.”

[20] K. Beznosov, P. Inglesant, J. Lobo, R. Reeder, and M. E. Zurko, “Usability meets access control: challenges and research opportunities,” in Acm Symposium on Access Control Models & Technologies, 2009.

[21] V. Oleshchuk, “Internet of things and privacy preserving technologies,” in International Conference on Wireless Communication, 2009.

[22] M. Button, “Setting the watch privacy and ethics of cctv surveillance,” International Journal of Law Crime & Justice, vol. 39, no. 4, pp. 215–217, 2011.

[23] C. Hochleitner, C. Graf, P. Wolkerstorfer, and M. Tscheligi, “utrustit – usable trust in the internet of things,” in International Conference on Trust, 2012.

[24] T. Teixeira, S. Hachem, V. Issarny, and N. Georgantas, “Service oriented middleware for the internet of things: A perspective,” in European Conference on Towards A Service-based Internet, 2011.

[25] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, “Distributed intrusion detection system in a multi-layer network architecture of smart grids,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 796–808, 2011.

[26] K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology, in: 2016 IEEE 18th International Conference on High Perfor- mance Computing and Communications; IEEE 14th International Confer- ence on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2016, pp. 1392–1393, doi: 10.1109/ HPCC- SmartCity- DSS.2016.0198 .

[27] K. Gaurav , P. Goyal , V. Agrawal , S.L. Rao , Iot transaction security, in: 5th Inter- national Conference on the Internet of Things (IoT), Seoul, S. Korea, 2015 .

[28] S.H. Hashemi, F. Faghri, P. Rausch, R.H. Campbell, World of empowered iot users, in: 2016 IEEE First International Conference on Internet-of-Things De- sign and Implementation (IoTDI), IEEE, 2016, pp. 13–24, doi: 10.1109/IoTDI. 2015.39 .

[29] L. Kokoris-Kogias , L. Gasser , I. Khoffi, P. Jovanovic , N. Gailly , B. Ford , Managing identities using blockchains and cosi, 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016), EPFL-TALK-220210, 2016 .