Accepted Manuscript

On security challenges and open issues in Internet of Things

Kewei Sha, Wei Wei, Andrew T. Yang, Zhiwei Wang, Weisong Shi

PII: S0167-739X(17)32488-3
DOI: https://doi.org/10.1016/j.future.2018.01.059
Reference: FUTURE 3966

To appear in: *Future Generation Computer Systems*

Received date : 31 October 2017
Revised date : 27 December 2017
Accepted date : 28 January 2018

Please cite this article as: K. Sha, W. Wei, A.T. Yang, Z. Wang, W. Shi, On security challenges and open issues in Internet of Things, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.01.059

On Security Challenges and Open Issues in Internet of Things

Kewei Sha, Wei Wei, Andrew T. Yang

University of Houston - Clear Lake, Houston, TX

Zhiwei Wang

Nanjing University of Posts and Communications, Nanjing, China

Weisong Shi

Wayne State University, Detroit MI

Abstract

When Internet of Things (IoT) applications become a part of people's daily life, security issues in IoT have caught significant attention in both academia and industry. Compared to traditional computing systems, IoT systems have more inherent vulnerabilities, and meanwhile, could have higher security requirements. However, the current design of IoT does not effectively address the higher security requirements posed by those vulnerabilities. Many recent attacks on IoT systems have shown that novel security solutions are needed to protect this emerging system. This paper aims to analyze security challenges resulted from the special characteristics of the IoT systems and the new features of the IoT applications. This could help pave the road to better security solution design. In addition, three architectural security designs are proposed and analyzed. Examples of how to implement these designs are discussed. Finally, for each layer in IoT architecture, open issues are also identified.

Keywords: Internet of Things; Security; Architecture; Challenges; IoT; Open Issues

1. Introduction

Internet of Things (IoT) is becoming the largest computing platform [1]. With recent developed applications such as Smart Transportation [2], Smart City [3], Smart House [4], and Smart Grid [5], IoT technologies are significantly changing our life style [6, 7]. The pervasive interconnection of smart IoT things which are physically distributed extends the computation

Email addresses: {sha,wei,yang}@uhcl.edu (Kewei Sha, Wei Wei, Andrew T. Yang), zhwwang@njupt.edu.cn (Zhiwei Wang), weisong@wayne.edu (Weisong Shi)

and communication to IoT things with various specifications. Sensing capability of these devices helps collect real-time data from the physical world directly or remotely. The analysis of the collected data provides us the ability of building an intelligent world and making better decisions to manage it.

IoT devices are becoming pervasive and they extend the Cyber world to the physical world, which creates new types of and more complex security issues and concerns. If those security concerns cannot be adequately addressed, wider adoption of IoT applications will be greatly hindered. For example, considering two of the typical application domains of IoT, i.e., Smart Home and Smart Healthcare, it is essential to protect the sensitive information moving around the system and the critical assets in the system [8, 9, 10]. The characteristics of the IoT devices, however, make the security design in IoT more challenging than before. These characteristics include extremely large scale, low cost design, resource constraints, device heterogeneity, preference of functions over security, higher privacy requirements, and harder trust managements. To be more specific, resource constraints often include limited computation power, energy supply, and memory capacity. These features make it difficult to apply many traditional security solutions to IoT, including the widely used public key scheme and IP-based security solution. Due to insufficient IoT security design, it is often easier to compromise IoT devices than conventional computers. For example, Forbes.com reports a successful hack into a baby monitor in Houston area [11]. Someone also demonstrated how to hack and remotely control and stop a Jeep car on the road when the driver is in operation [12]. It is also reported by CNN Money that hackers have found volatilities in most smart home devices [13], including Smart Plugs [14, 15], Smart Cameras [16, 17], DVRs [18] as well as vulnerabilities revealed by researchers [19, 20, 21, 22, 23, 24, 25].

Above cases illustrate the urgent needs of improving security of IoT systems. Serious consequences can be expected from security breaches in IoT systems. For example, fatal accidents can be the result of remotely turning off a vehicle through a security breach. Current weaknesses in IoT security may be attributed to insufficient understanding of security challenges of new IoT systems. In this paper, we aim to conduct a detailed analysis of security challenges in IoT systems, because we believe an intimate understanding of IoT security challenges will pave the road to better security solution design. Moreover, the differences in security challenges between IoT systems and Wireless Sensor Networks (WSNs) are summarized and compared. Finally three architectural security designs for IoT are proposed and compared. Examples of how to implement these designs are presented and discussed. One of our findings is that, without aid of

highly capable devices, it is difficult to achieve high level of security with the low capable devices in the system. This observation necessitates the deployment of secure services in the new Edge computing paradigm [26, 27]. The contributions of the paper include in-depth analysis of IoT security challenges, proposals of security function deployment, and identification of open issues in IoT security designs.

The rest of the paper is organized as follows. Importance of security in IoT applications in the context of several typical IoT applications is discussed in Section 2. Then Section 3 overviews a typical IoT architecture. A comprehensive analysis on new IoT security challenges is presented in Section 4, which is followed by comparisons of security challenges between WSNs and IoT in Section 5. In Section 6 our proposal of architectural designs of IoT security solutions are presented and discussed. We list a set of related work in Section 7. Finally, conclusion and future work are depicted in Section 8.

2. IoT Applications and Needs of Security

IoT is becoming the largest computing platform. It has been applied in many application domains including Logistics [28], Smart Home [4], Smart City [3], Smart Health, Smart Connected Vehicles [2], Smart Grid [5], and so on [1]. In this section, we present three typical applications of IoT in the context of the importance of security in these applications.

2.1. Smart Home

Smart Home is becoming increasingly popular recently [29]. Gartner's IT Hype Cycle 2016 Report identifies that smart connected home is an emerging technology. It is predicted that a typical home could contain 500 or more smart devices by 2022 [30]. Smart Home has the vision of adding intelligence to everyday home objects, such as appliances, door locks, surveillance cameras, furniture, garage doors, and so on, and making them communicate with existing cyber-infrastructure. The addition of intelligence to physical objects offers many benefits to better human lives, including increased convenience, safety, security, and efficient usage of natural resources. For example, the Smart Home can adjust the blinds to save energy based on the environmental changes, automatically open the garage door when it senses an authorized vehicle approaching, or automatically order medical service when emergency is detected. In Smart Home, traditional physical home devices become a part of the extension of the existing Internet. If devices are compromised, the consequence can be severe. For example, successfully hacking smart lock will enable strangers to enter the house; compromising of baby monitors can scare

babies remotely by strangers; hacking microwave can cause fire at the home. Owners of Smart Home may not want to live in Smart Home if security is a concern. Instead, they may expect to improve the safety of the house by using intelligent surveillance services [4]. In addition, privacy of Smart Home owners need to be preserved. However, continuously collecting data from Smart Home devices can reveal private activities of home owners as indicated in [31, 32]. It poses serious threats to the home owners' privacy.

2.2. Smart Grid

The other typical IoT application is to build Smart Grid. Smart Grid has been designed and implemented to improve the reliability, reduce the cost, and optimize the performance of the traditional power grid systems [33]. In addition to integrating more green and renewable energy such as wind power, geothermal heat and solar power, it also aims to improve the reliability and management of the traditional power grid more efficiently. Smart grid data communication networks, which interconnect many smart grid devices, play a critical role to achieve above goals. It not only collects the energy usage data, but also monitors the status of the smart grid system. Many novel applications can be developed based on the smart grid data communication networks. For instance, based on the collected energy usage information, utility companies can distribute and balance the load more wisely. It also helps to design a fair but scaled pricing model by considering the unbalanced energy consumption in the dimension of time and space. By building smart grid status monitoring applications, it is possible to identify failures in the grid system as early as possible, and design novel fault-tolerant mechanisms to better respond to the failures. Many techniques including automated metering infrastructure (AMI) [34, 35] have been proposed to build the smart grid communication networks. Having so many data moving around this mission-critical system, security is also one of the most important concerns in building such systems. Intrusion to Smart Grid [36] and cutting electricity supply to a large area can cause huge physical and economical damage to the society. Analysing power usage data can also reveal people's daily private activities [37]. Moreover, attacks against data integrity [38, 39] and false data injection [40, 41, 42] can disturb the billing system of the smart grid and mess up start grid state estimation, torture the power flow, and delay demand response.

2.3. Smart Connected Health

Smart Connected Health is proposed to improve the efficiency of healthcare systems and to reduce healthcare costs [43]. The analysts at MarketResearch.com claim that the sector will be worth $117 billion by 2020. By embedding smart healthcare devices in the existing medical

infrastructure, healthcare professionals will be able to monitor patients more effectively, and use the data collected from these devices to figure out who needs the most attention. In other words, by making the most of this network of devices, healthcare professionals could build a system of proactive management based on the collected data, as it is believed that prevention can be more important and effective than the cure. Researchers also study techniques on how to implant sensors into human body and monitor the health condition of these people [44]. Analyzing the collected data, healthcare professionals are able to discover behavioural changes of patients with the disease and with the medicines during the treatments. In Smart Connected Health, security is also a critical concern. With networked medical devices, it is convenient to collect data and check the status of that device, but it is also risky because instructions can be sent to stop the function of the device [45]. It will be extremely dangerous to stop a medical device that is critical to the life of the patient, like heart bumps. In addition, privacy can be a significant concern in Smart Connected Health because most data collected in the system are very sensitive medical data [46].

There are many more IoT-based applications [6]. For example, when IoT technologies are applied in Smart Transportation, security solutions are necessary to protect the intelligent transportation systems such as navigation and safety [47, 48]. Because the focus of this paper is to investigate security issues in IoT, we only introduce the three typical IoT applications in detail as listed above. We can conclude that security is an essential component for most IoT applications, and higher level of security is required comparing with many existing networked systems since most IoT applications are critical applications that deal with persons' daily life.

3. An Architectural View of IoT

IoT is a system that interconnects a set of large-scale and heterogeneous IoT end devices. Large volume of data is collected and transferred in IoT [49]. Based on the analysis of the collected data, IoT targets to build an intelligent world [6, 50]. A typical three-layer architecture of IoT systems is depicted in Fig 1. IoT applications run on top of the three layers, i.e., the *cloud layer*, the *edge layer*, and the *things layer*. Each layer is capable of collecting, processing, and analyzing data. Two-way communication is usually supported, although generally speaking, much more data is streamed from the things layer to the cloud layer through the edge layer than the other way around.

The **things layer** contains huge number of heterogeneous things including sensors and actuators. IoT Things (also called end devices) are integrations of physical parts and cyber parts;

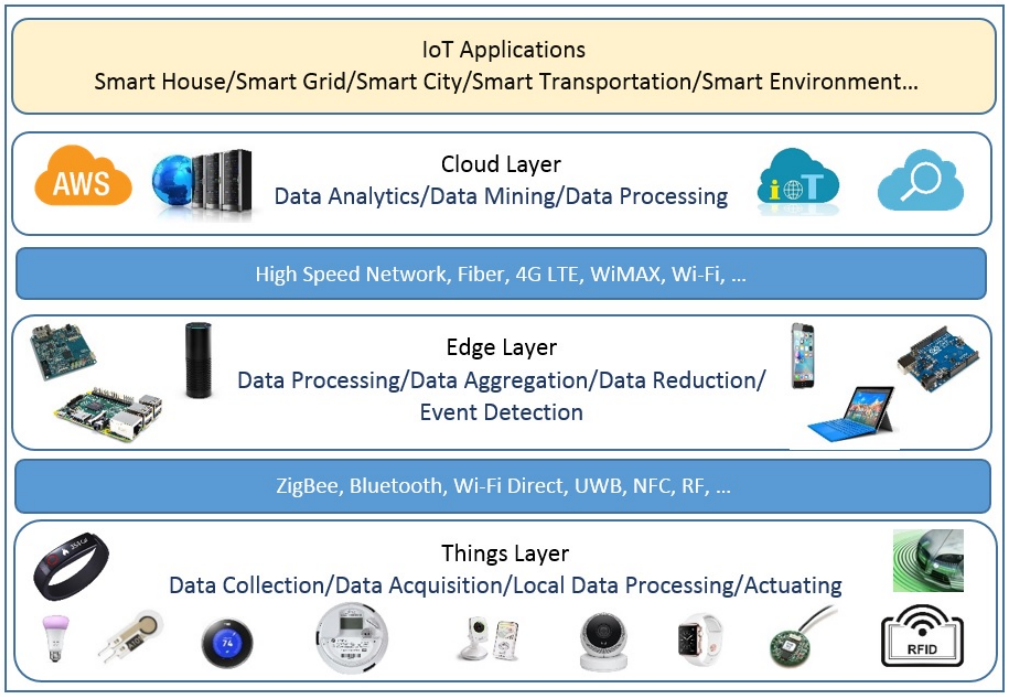

Figure 1: An architecture of Internet of Things.

Physical parts of the things reaches deeply into the physical world, while the cyber parts bring connectivity computability and storage. The things can be extremely different in specifications including computation, storage, communication, and power supply. For example, things like smart meters are powerful enough to support heavy computation, while things like smart bulb can only actuate some simple operations and almost have no computation power. In conclusion, most things are resource-constrained and energy-limited. Therefore, they are not suitable to run heavy tasks.

Not like the things layer, the **cloud layer** is very powerful and has many resources available to support heavy tasks, such as mining intelligence from a huge volume of data and implementing very complicated tasks like distributed intrusion detection. In addition, there exist many powerful tools and advanced algorithms that can be utilized to build powerful applications. The cloud and the things are connected, but they are usually located far away from each other and have no direct communication channels. It is very costly to transfer all data from things to the cloud via multiple-hop routing. Therefore, cloud is not an optimal choice to support IoT application that have features such as high real-time requirements, extensively geo-distribution or high mobility [51].

The **edge layer** (also called the *fog layer* or the *gateway* layer) is proposed to fill the gap between the resource-constrained things layer and the resource-rich cloud layer. The edge layer has become a very important layer in the IoT architecture. Usually edge devices are directly connected to or several hops away from the things. Compared with things, edge devices generally have more resources including power supply, computing power and storage spaces. Having multiple communication interfaces, they can help mask the heterogeneity of the things, and provide other services to the things such as offloading heavy tasks. Finally, the edge devices are mostly connected with the cloud via high speed Internet. They can easily utilize the powerful cloud services, or they can work together with the cloud layer on heavy tasks. Therefore, the edge layer plays a critical role in this architecture to link the things and the cloud.

In conclusion, each layer in IoT architecture has its own special characteristics. It is essential to make them work collaboratively to build an efficient IoT system. Deployment of IoT tasks can be optimized by taking into consideration the characteristics of different layers.

4. Why Security is more Challenging in IoT?

Security is a must for IoT systems to protect the sensitive data and critical physical infrastructures [52]. Without a good level of protection, users may not adopt many IoT systems and applications. Security in traditional networked systems remains challenging while IoT systems bring many more challenges to researchers because of several special characteristics of IoT systems. A thorough understanding of these challenges is essential to develop novel security solutions. In this section, we discuss these security challenges in depth.

4.1. Integration with the Physical World

In a typical IoT application, the cyber world is tightly coupled with the physical world. The coupling poses extra security concerns since the physical world now can be compromised or controlled through the cyber world, which could generate extremely detrimental consequences. The following discussion explains some of those concerns.

Many IoT systems are mission-critical and non-interruptible, such as the SCADA systems used in oil and gas industry. Conventional security rescue mechanisms are often not applicable in those scenarios. For instance, the turn off, reset, and then reboot sequence simply cannot work because the production processes cannot halt. In addition, an IoT system consists of the necessary cyber parts and the physical parts. These two parts must be compatible for the system to function properly, which may be problematic. Imagine a legacy physical device that uses a

driver that only works with an old operating systems that is no longer supported and updated by the vendor. Obviously, the old OS has to stay but it becomes a serious vulnerability. The whole system may be compromised through this weakest link.

In addition, with the tight coupling of the physical system and the cyber world, compromising one can put the other at great risks and negative impact can propagate both ways. For example, compromising the cyber part of the systems allows the attackers to control the physical system. What may be in jeopardy is no longer just the sensitive and private data and information, but possibly the physical devices as well. Considering the IoT applications such as Smart Grid or Smart Health, there could be both financial loss and human life loss. On the other hand, captured IoT devices could provide attackers access to coupled cyber parts. Not like more sophisticated traditional computing devices, many IoT devices are not sufficiently safeguarded. Once gaining access to those vulnerable and unprotected devices, attackers can further invade and compromise the cyber systems [53, 54].

The ultimate goal of IoT is to build an intelligent world based on analysis results of data gleaned across the systems. Typically, control messages are often sent from the cloud or edge layer to the actuators or end devices to control the physical world. Along this path, the cyber system could be compromised at multiple points-including all the three layers plus the communication network. Therefore, in the IoT security design, we need to compartmentalize compromised systems so negative impacts will not propagate. To achieve this, we need to study granularity access control models and mechanisms that restrict proliferation of security breaches [55].

4.2. Heterogeneous Devices and Communications

The value of IoT technology lies greatly in its versatility and applicability. When used for different application domains, IoT systems often adopt various devices with disparate hardware and software specifications. Take Smart Home as an example, the system power usage is monitored by low capable sensors that can only conduct simple calculations and provide readings occasionally. On the contrary, home security surveillance systems need to provide monitoring of the home area in real-time. They also need to run detection algorithms to detect abnormal activities. In addition, in Smart Homes, we can also see very powerful devices such as smart TV and gaming consoles that need to perform complicated computation tasks. In summary, we see many IoT devices that run on a wide range of operating systems using various communication channels. These heterogeneities make traditional security solutions not applicable to IoT systems.

Traditional security solutions often assume certain types of software systems and communication methods. Therefore, security solutions that work in Window systems may not work for other operating systems such as Android, iOS, TinyOS, Contiki, and mbed. In addition, IP based security solutions including IPSec, SSL, HTTPS, and SSH cannot work in low-capable devices such as smart meters and sensors that do not support IP-based protocols directly. As a result, we will see different levels of security for different parts in a single IoT systems. The least secure device becomes the most vulnerable point-of-entry and it determines the overall level of security of the IoT systems. Once it is compromised, other devices may be exploited as well.

In conclusion, when designing IoT security solutions, we need to adapt security algorithms and protocols to the hardware and software specifications of the devices. Security of low capable devices needs to be enhanced through facilitation from more capable devices. Compared to Bring Your Own Device (BYOD) concept and its corresponding security issues [56], IoT brings a far more challenging computing environment that calls for effective security solutions, in which the core should be a novel security abstraction independent of device specification, operating systems, and communication channels.

4.3. Resource Constraints

To drive down the development and manufacturing cost, vendors often equip the IoT devices with limited capabilities. This results in low capable devices with various resource constraints such as small memory space, low computation capability, low communication bandwidth and limited power supply. For example, a typical IoT device may run an 8-bit or 16-bit system. These resource constraints directly contribute to many of the IoT insecurities because traditional security solutions often cannot work on low capable devices.

National Institute of Standards and Technology (NIST) defined the high level goals of security as data integrity, availability, and confidentiality. Mechanisms including encryption, authentication, access control, intrusion detection, and firewalls are used to help achieve those goals. However, the inherent resource constraints of IoT greatly narrowed the possible choices of security solutions because many established security mechanisms cannot be carried out by low capable devices. For instance, most IoT devices cannot use asymmetric key based encryption algorithms because the computation cost is prohibitive, even for some relatively powerful Smart Meters such as GE I-210 [57]. In turn, for those devices, any security solution that involves public-private key scheme, such as PKI-based security solutions and digital signature based authentication, are not feasible either. For some even lower capable devices such as RFID tags [58],

the situation is even worse because the tags cannot even support symmetric key based cryptographical algorithms such as AES, DES, and 3DES. As far as authentication is concerned, only symmetric key based authentication or other lighter approaches can be used by IoT systems. For example, digital signature based authentication is not applicable because it needs to use the public-private key scheme. The other candidate, Kerberos, has its own limitations such as scalability issues and the fact that it mainly works with IP-based networks. In addition, it requires a trusted path through which passwords are entered. Furthermore, there are also challenges to the key distribution and key management tasks. Neither the traditional certificate authority (CA) nor the Diffie-Hellman key exchange algorithm would work because they require asymmetric key scheme. In terms of access control, intrusion detection systems, and firewalls, their application to IoT systems are also greatly limited due to the resources constraints since they are often more computationally expensive than cryptographic algorithms. Take role-based access control protocols as example, they often need to work with a big policy library, which cannot be stored in the end devices or even some edge devices. The same applies to intrusion detection systems firewalls. In summary, effective security design for IoT systems must be mindful of the resource constraints and focus on being lightweight and applicable.

4.4. Privacy

As large scale IoT systems often generate, collect, and analyze large volume of data to derive intelligence, privacy becomes a great concern. When used in a medical domain, IoT may pose threats to the privacy of people's medical information. When used in smart home, IoT may expose one's personal life to the outside world, which can be potentially dangerous. For example, recent research [59] has revealed that based on utility readings, one can infer the daily activities of the users, including private activities such as when they take showers, when they cook, and when they leave and come home. Other personal details such as whether they have kids or what types of diseases do they have can also be derived. IoT systems need to utilize data to achieve its functions, but privacy also needs to be preserved to a satisfactory level. The dilemma is obvious and calls for solution.

There also exists a tradeoff between privacy and security. Higher privacy demand tends to require weaker identity. Algorithms like k-anonymity [60] was designed for such purpose. On the other hand, strong security often demands strong identity especially in authentication. Considering intrusion detection and firewalls, both need information traceability and linkability to function. But these are exactly what privacy tries to avoid. Aggregation is another approach

often taken to enhance privacy. But aggregated data often fails to provide the necessary details required for certain security analysis. In design of IoT security solutions, privacy needs to be emphasized, but how to achieve the most optimal balance between privacy and security is an open-ended question that needs to be answered.

4.5. The Large Scale

The ever-increasing scale complicates the challenges of designing security solutions for IoT systems. First of all, the huge amount of interaction between all the devices increase the security deployment cost significantly. Second, it is difficult to apply key management schemes that are already plagued with scalability issues to large scale IoT systems [61]. Third, post-deployment system administration will be very challenging as well [62]. For example, people may fail to view IoT devices (such as TVs, refrigerators, ACs, etc.) as devices that involves computing and need to be secured. On the other hand, trying to manage all the IoT devices the same way we do with traditional computing devices is impractical, both financially and technically. A potential consequence is that necessary security updates will not take place in a timely manner [63]. Finally, the large number of connected IoT devices greatly increases the attack space, and each device may become the next target of certain attacks. Therefore, we conclude that the ideal IoT security solutions should be scalable, distributed, and automatically configurable. The solution should also be hierarchical and isolable.

4.6. Trust Management

Trust computing is an essential component in security design [64]. With a big portion of the IoT systems organized as peer-to-peer or ad hoc networks, trust management remains a significant challenge in IoT as it is a challenging issue in any peer-to-peer or ad hoc networks [65]. In addition, high mobility, no global identity, and temporary relationship among IoT devices further complicate the design for an efficient trust solution. Finally, IoT systems usually do not have a central administration and lack a good infrastructure to record the behavior of IoT devices. Therefore it is difficult to generate reputation ratings for the devices. Study on novel trust models are required to evaluate the reputation of IoT devices [66].

4.7. Less Preparation for Security

Last but not the least, IoT security breaches are caused by little security preparation in people's mindset in IoT device design and manufacture; however, it is challenging to change the people's mind. Firstly, a lot of current IoT device manufacturers do not have the same

level of understanding about cybersecurity as traditional cyber device manufactures. Thus, it is difficult for them to produce high secure IoT devices in the short run; for example, many IoT devices will still use simple default configurations. Because of that, attackers can hack devices by using simple hacking techniques to obtain the username and password. Secondly, because functionality and usability are easier to sell, they are usually preferred over security and it is hard to persuade people to invest in security. Therefore, limited security budget does not allow to build strong security for a lot of IoT devices. A study from OEM Hub at Bitdefender [67] confirms above observations by pointing out that security seemed to be one of the first things to be cut off. Moreover, many security solutions may not be considered by the market and the users because they degrade the functionality and usability. Finally, IoT devices may be treated as physical dummy devices and can be poorly administrated by users. Considering the fact that so many successful security breaches in the traditional networked systems are resulted from insufficient security design and weak security configuration at the current level of security administration, we will see more security problems in a less administrated system like IoT with so many mental difficulties. How to efficiently educate and train the IoT designers, users and administrators needs to be explored.

5. Security Challenges: IoT vs. Wireless Sensor Networks

Wireless Sensor Network (WSN) is one of the major enabling technologies of IoT [68, 69]. Security is also an important design challenge in WSN mainly caused by constrained available resources at each sensor and the scale of sensors [70, 71]. Besides common challenges of security design in both WSN and IoT, several differences between IoT and WSN, however, indicate that security issues in IoT are more challenging than those in WSN because of the different characteristics of WSN and IoT as well as the different targeted applications. Detailed comparisons in terms of characteristics of IoT and WSN are summarized in Table 1.

First, WSNs are mostly used in data collection applications, such as environmental monitoring [72] and surveillance [73]. The data is typically collected by sensors and transmitted to sinks via reliable multihop routing protocols [74]; therefore, the communication is mostly one direction, although the other direction is also used to disseminate control messages, which is used to manage the sensors. In addition, these messages usually do not intend to control the physical world, but are used to instruct sensors. Consequently, the impact of WSN to the physical world is not as significant as IoT to the physical world. The tight coupling between the physical world and the cyber world in IoT systems makes it essential to consider the safety of

Table 1: Comparison of different characterises of IoT and WSNs.

Characteristics	**IoT**	**WSNs**
Physical coupling	Tightly coupled	Monitoring the physical world
Communication	Two-direction communication	Mostly one-direction communication
Constraints	Computation and storage and energy	More on energy
Heterogeneity	Heterogeneous communications and devices	Mostly homogeneous devices
Scalability	Very large scale	Large scale
Privacy	Very High privacy expectation	Some privacy expectation

the physical system as a part of security design.

Second, both sensors in WSNs and end devices in IoT suffer from constrained resources; sensors, however, may have more concerns on energy constraints [71], while some end devices in IoT systems may have more concerns on computation capability and storage spaces because of the low-cost design of these devices, even comparing with typical sensor boards. Sensors in a WSN are mostly homogeneous, but device and communication heterogeneity are more common in IoT systems. Above heterogeneity not only brings significant challenges in interconnection, but also makes it difficult to design a general solution that can be applied in many heterogeneous devices. For example, in an IoT system that consists of low-capable end devices, such as RFID and smart bulbs, which barely support any encryption algorithm, the design of the encryption algorithms, secure communication protocols and even architectural security designs all need to be reconsidered.

Third, WSNs are peer-to-peer ad hoc networks. One WSN is mostly isolated from other WSNs, and one WSN is usually designed for one specific application. Contrarily, IoT, as the extension of the existing Internet, intends to connect many domain specific autonomous systems including ad hoc networks like WSNs. System-wide key management is much more challenging in IoT than in WSNs because of the larger scale of IoT as IoT connects more number of devices and cover more heterogeneous devices than that in connected autonomous subsystems. Random key distribution [75, 76, 77, 78] is a widely adopted key management mechanism in WSNs, but because it requires a centralized key pool and has good but still limited scalability. It is hard to apply random key distribution mechanism in IoT, considering the large scale and lacking of central management in IoT. Polynomial based key predistribution [79, 80] also has limitations of higher memory usage and computational overhead. It requires to design complicated key-

distribution mechanism for various IoT applications.

Last but not the least, comparing typical IoT applications, such as smart home and smart grid systems, with typical WSN applications such as environmental monitoring and industrial monitoring, more human-related data is collected in IoT applications than in WSN applications. Analyzing collected human-centric data, sensitive activities of people's daily life will be discovered. Privacy becomes a much more significant concern in IoT systems than in WSNs. It can even be one of the biggest obstacles of deployment and adaptation of IoT systems.

Based on the above analysis, security requirements are higher in IoT and it is more challenging to design efficient security solutions in IoT than in WSNs.

6. Architectural Security Design for IoT

From previous sections, we can see that it is challenging to satisfy security requirements of IoT applications. Novel security solutions are needed to achieve a high level security in IoT, including designs of lightweight security algorithms and protocols, efficient privacy-preserving algorithms and protocols, safety mechanisms to protect the physical systems, and many automatous approaches to manage and configure security settings of IoT devices. Among them, architectural security design is of the most importance and should be considered first, because other security solutions are embedded in IoT's new architecture as depicted in Section 3, which is different from the architecture of existing Internet based systems and WSNs. In other words, the architectural security design can guide other novel security designs for IoT. In the rest of this section, we present three typical architectural security designs, including End-to-End security at things, security service deployed at the edge, and a distributed security model. These designs can be used to model future security solution designs like security protocols for IoT. Moreover, for each type of architectural security design, we discuss the advantage and limitations of each design and present examples that illustrate how to implement these designs. Moreover, we identify a set of open issues for the design of each layer.

6.1. End-to-End Security at Things

End-to-End communication is essentially important in networked systems [81], including both traditional Internet and IoT. Protocols such as IPv6 [82] and 6LoWPAN [83] have been designed to support End-to-End communication in IoT. Similarly, End-to-End security at Things is also of great interests [84]. Although resource constraints at this layer limit the choices of available security techniques, there exist necessities of deploying End-to-End secuity. First of

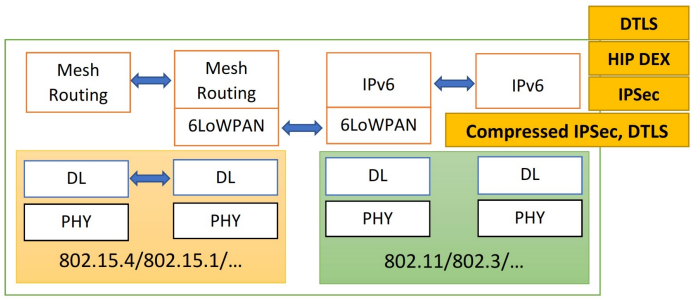

Figure 2: End-to-End security at Things.

all, to ease trust management, it is better to let end devices manage security by themselves. Moreover, enabling End-to-End security among end devices or between the end device and other devices is important for many IoT applications. For instance, End-to-End security is needed in a Vehicular Network application [85], where vehicles need to work together to accomplish collaborative tasks like driving safety enhancement. Furthermore, when End-to-End security is achieved at the Things layer, many existing Internet based applications can be naturally extended to be IoT applications. Finally, end devices may want to manage security and privacy by themselves.

One solution to support end-to-end security in IoT systems is to increase the available resources such as memory and computational power at IoT devices so that they can utilize traditional security solutions. The other solution is to add extra security-related hardware like Physically Unclonable Function (PUF) [86], which is a hardware based solution, working as a digital fingerprint and serves as a unique identity for a device. With PUF, authentication can be implemented like that are demonstrated in [87, 88]. The advantage of PUF technology exists that it only requires less or comparable size of hardware (digital gates) to implement PUF compared with other commonly used cryptographic algorithms including popular secure hash functions (such as MD5 and SHA) and symmetric encryption algorithms like AES [89]. Therefore PUF technology has great potential when it is implemented in IoT systems, but there are also limitations of PUF. Firstly, not so many existing IoT devices are equipped with PUF hardware, so we cannot assume the existence of PUF when we design IoT security solutions for a large scale IoT system. In addition, many PUF-based IoT devices require enough memory to store all the challenge/response pairs [89]. It may significantly increase the cost of each IoT device. Generally speaking, the PUF-based security solutions are attractive in end-to-end security solution design for IoT systems, but there are still extra hardware cost to have PUF in

IoT devices. Finally, PUF still has problem of modeling attacks and side-channel attacks [90, 91].

Besides the above hardware-based solutions, End-to-End security protocols for IoT have also been studied in the literature. Most of them are extensions of the existing IP-based security solutions. Two categories of protocols are most common, including IPv6 based security solutions [92, 93] and 6LoWPAN [83] based security solutions [94, 95]. When IP is supported by the end devices as shown at the right part of Figure 2, IP-based security solutions can be naturally extended to end devices, although the computational overhead can still be high for these devices. Several efforts have been made to make the IP-based security protocols lightweight. Hummen *et al.* tailors HIP DEX protocol [92] for IoT applications. In their design, a comprehensive session resumption mechanism is used to reduce the heavy cost in the handshaking caused by the public key based encryption. A DTLS based End-to-End security architecture has also been proposed to support two-way authentication [93].

To interconnect end devices that do not support IP stack as shown at the left part of Figure 2, 6LoWPAN [83] is designed to support End-to-End communication among devices supporting various networking technologies. Security can also be integrated into the design of the 6LoWPAN [83] protocol. Hennebert and Santos [94] review several security protocols that have been integrated into the 6LoWPAN protocol stack. Working with 6LoWPAN, security can be supported at different layers, such as at the link layer and at the network layer. In IEEE 802.15.4-2011 [96] and its amendment [97], three fields have been added to the frames for security purposes, including frame control, auxiliary security header and frame payload. Auxiliary security header specifies security control to identify security mode; frame counter is used to prevent replay attack, and key identifier is utilized to define the key used in the communication. In the network layer, IPsec has been adapted by compressing IPsec header into 6LoWPAN frame [98]. Similarly, DTLS protocol has been considered to be compressed into a 6LoWPAN frame [93].

From above analysis, we can see that to support End-to-End security, end devices are required to be capable of supporting IPv6 protocol or 6LoWPAN protocol. Both cases require end devices to have reasonable rich resources, although lightweight algorithms and protocols have been studied. For example, most existing End-to-End security solutions utilize public key schemes in the protocol design. ECC [99] has been utilized to reduce the overhead of the public key based security solutions. Other lightweight security protocols such as symmetric key based protocols could also be explored. Many end devices, however, may still be not powerful enough to support these lightweight protocols. End-to-End security at Things has several advantages. First, the

end devices do not need to trust any other devices because they do not rely on other devices to achieve security goals. Second, the system architecture is a kind of flat architecture. It reduces management cost. Third, privacy of end devices can be better protected because they can decide how much information to share.

Although many research efforts have been made to achieve End-to-End security, there are still many open research problems. Firstly it is difficult to address safety issues of end devices because of little protection can be delivered [100]. Secondly lightweight protocols that enable End-to-End security need to be designed. Thirdly, novel protocols are needed to handle the heterogeneity in IoT devices. Finally, how to extend existing IP network to cover more IoT end devices can be studied.

6.2. Edge Layer Security Service

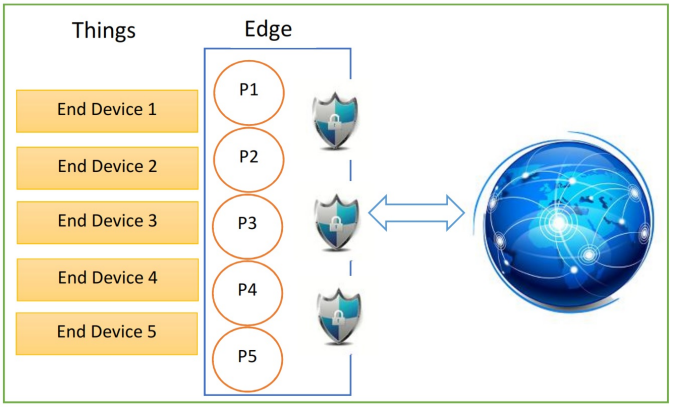

Figure 3: Deploy security service at edge.

Many end devices such as smart bulbs and RFID tags do not have sufficient resources to support End-to-End security. Instead of having end devices handle security by themselves, security management tasks may be offloaded from low capable end devices to more powerful edge devices. In this scenario, the end device may have to chooses to trust the edge layer, and use the edge layer as the security agent to manage its security needs. Figure 3 illustrates how the edge layer can be used to enhance the security of the end devices. In the figure, edge device creates a security profile for each end device. Any access to end device or instruction sent to end devices is taken care of by the edge layer on behalf of these end devices through well-designed security checking mechanism. For example, representing the end device, the edge device makes use of an authentication protocol to mutually authenticate a third device that

wants to communicate with the end device. Authorization can also be managed by the edge device that decides which other devices have the right to access the data collected by the end device or can send control commands to it. In addition, with more data available at the edge device and the available computation capability, the edge device can run intrusion detection algorithms to detect attacks so that the intrusion can be controlled as early as possible.

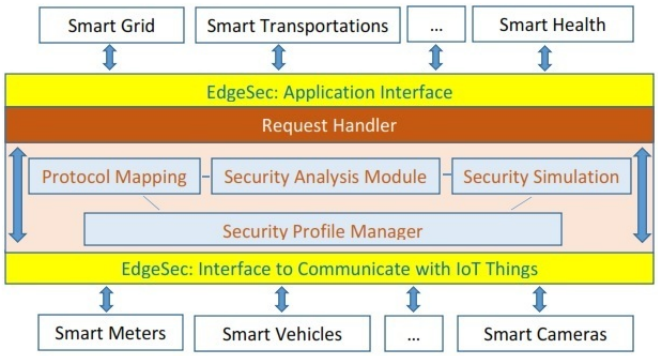

Figure 4: The architecture of EdgeSec.

EdgeSec [26] presents an example of such a design. The architecture of EdgeSec is shown in Figure 4. From the figure, EdgeSec consists of seven major function components, including Security Profile Manager, Security Analysis Module, Protocol Mapping, Interface Manager, Security Simulation Module, Request Handler, and User Interface. Security Profile Manager registers end devices to EdgeSec. It creates a security profile and also collects security requirements of each end device. Based on device security profile and requirements, Security Analysis Module decides if a specific security function will be deployed at the edge layer. Then the Protocol Mapping module chooses appropriate protocols to satisfy the security requirements based on security function deployment decisions. Interface Manager is designed to mask communication heterogeneity in end devices. After Request Handler receives the request of accessing the end devices, Security Analysis Module will be contacted to analyze potential security risks of the requests. Moreover, if the request is a critical request, e.g., it may cause physical damages to the IoT system, it will first simulate the execution of the request using Security Simulation Module. Finally, User Interfaces allows administrators and users to interact with EdgeSec components.

The advantages of deploying security at the edge layer are as follows. First, with more resources available at the edge layer, it can leverage these resources to offload computation-intensive tasks, such as data encryption, key generation, and intrusion detection, from end

devices. This is critical for end devices with very constrained resources, such as passive RFID tags and smart bulbs. Second, edge devices are physically close to end devices. This not only reduces the communication cost significantly but also improves real-time performance of IoT applications. Third, the Edge layer has more information than end devices about the whole system; thus it is possible to deploy more optimized security management at the Edge layer. Fourth, the relatively stable relationship between edge devices and end devices is very beneficial to establish trust between them by designing novel trust models. Fifth, the Edge layer can be used to protect the privacy of end devices by utilizing secure aggregation algorithms or other k-anonymity algorithms [60]. Finally, the Edge layer usually has high-speed connection with Cloud and it is cost-effective for them to get security support from Cloud as needed. One limitation of this approach is that the end device has to fully trust the edge device. In addition, novel security solutions are needed to enhance the security level of the edge layer. Furthermore, how to secure the communication between the end device and the edge device remains a challenge.

Edge based security solutions attract more attention recently. Open research issues include how to build a secure and efficient edge layer, i.e., security design to secure edge devices, how to securely connect the edge layer with end devices using a lightweight protocol, how to organize edge devices to collaboratively perform complicated security functions, and how to build novel trust models for edge and end communications. In addition, research issues such as edge-based intrusion detection and threats analysis will be of great interests.

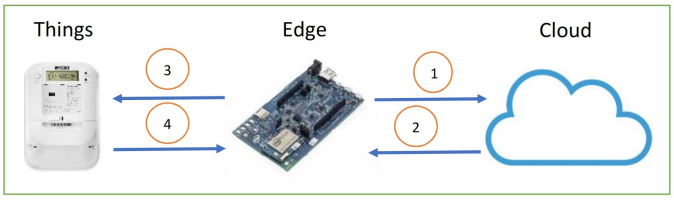

Figure 5: Distributed security model for IoT.

6.3. Distributed Security Model for IoT

Above edge based security solution requires end devices to trust edge devices. This can be risky in many cases. Authentication can be utilized to build the trust between end devices and edge devices. Most existing scalable authentication protocols depend on public key or symmetric key schemes, but end devices may not have sufficient resources to support these needed operations. Compared with temporary connected edge devices, the permanent available cloud services are more trustable to end devices in most cases. With this level of trust, the

cloud can provide credentials to edge devices so that the edge device can win the trust from end devices by presenting the verifiable credential from the cloud. This idea can be implemented in four steps as shown in Figure 5. In the first step, before the edge device starts its communication with the end device, the edge device sends a request asking access to a specific end device to the cloud. Then the cloud verifies the trustworthiness of the edge device either based on an authentication and authorization check or based on the trust score calculated from a trust model available at the cloud. Next, the cloud issues credentials to the edge device. In the third step, the edge device presents the credentials from the cloud to the end device and the end device verifies the credentials. If above steps are all successful, the end device can start trusting the edge device at the fourth step.

The secure framework to read isolated smart meter [101, 59] presents an example that implements the above design by designing a two-phase authentication protocol. In [59], the smart meters are the IoT things, resource-constrained devices that can support neither asymmetric cryptographic algorithms nor the IP based security solutions. The utility cloud needs to securely read data from smart meters to build smart grid applications, but it cannot securely communicate with the smart readers directly. Therefore, a smart reader is used as an edge device that connects the utility cloud and the smart meters. It also helps to securely read data from the smart meter and send them to the utility cloud. The above goal is achieved by designing a two-phase authentication protocols that involves all three parties. In the first phase of the framework, after receiving the data reading request from the smart reader, the cloud verifies the legitimation of the smart reader using a digital signature based authentication protocol and the cloud database also confirms the legitimation of the task by checking the job schedule. Then a credential is sent from the cloud to the smart reader. It is used to generate a one-time shared key between the smart reader and the smart meter. In the second phase of the framework, the smart reader completes a symmetric key based authentication using the generated one-time shared key and wins the trust from the smart meter. Therefore, the smart meter will allow the smart reader to read the collected data.

Besides the trust management, cloud can help in many other perspectives of security solution design. For example, although edge devices are generally powerful, they still may not have sufficient resources to handle very heavy tasks. In these cases, the cloud can be very helpful in implementing security solutions by offloading heavy computation and storage needs at the edge layer to the cloud layer. For instance, intrusion detection mechanisms can be more powerful when they are implemented in the cloud in that the cloud has the capability to store and process

a huge volume of data. Like what is indicated in [102], the intrusion can be detected as early as possible based on the analysis of the collected data in the cloud. In addition, the cloud can be a better choice to manage key distribution and help to manage the security of edge layer [103].

In the above design, the end device, the edge device and the cloud work together to achieve a high level of security. Therefore we name this architectural security design as distributed security model for IoT. The advantages of distributed security model are three folds. First, cloud layer service is usually more trustable than edge layer service. It can lower the risk of trusting the edge layer. Second, with the available resources in the cloud, many complicated security solutions can be supported, i.e., the cloud can be compliment to other layers in security solution design. Third, it is beneficial to distribute the security workload to multiple layers; in other words, distributing the storage of security information helps to enhance the security. One problem of using cloud in IoT security design is that the cloud is usually located far away from the end devices and they may not be able to communicate directly with the end devices. Several performance related requirements such as the real-time requirement are not easy to be satisfied. Moreover, using cloud to improve the security at end devices can make the security solution design more complicated. More types of communication make it necessary to secure all the communications. Finally, there are also requirements like that the end device should be reasonably powerful to support necessary security functions such as symmetric key algorithms and secure hash functions like in [59].

The end layer, the edge layer and the cloud layer working together on security solutions is of great interests, but there are still open research issues, such as how to distribute security functions to each layer, how to minimize the complexity of the security solutions when all three layers are involved, how to maximally utilize the cloud layer resources for security design, and how to preserve privacy when all three layers are involved in security solution design. Moreover, how to produce distributed log files and conduct distributed security analysis across multiple layers is the other open research issue.

In conclusion, three options of architectural security designs are available. If the end devices are powerful enough to support necessary security functions and have the appropriate networking capability, it is preferred to have end-to-end security at IoT things. It is necessary, otherwise, to offload security related tasks to the edge devices and the cloud that have enough computational and storage capacity to support security functions. Then a certain level of trust to either the edge layer or to the cloud layer is needed. Each above design has its advantages and limitations. Applications need to choose the most suitable architectural security design based

on their security requirements and available resources.

7. Related Work

IoT has attracted lots of attentions in the recent years. There exist many efforts that focus on how to secure the IoT systems. In this section, we lists a set of work related to this paper. A comprehensive survey of IoT is presented in [104]. The authors not only summarize the architecture, application and enabling techniques for IoT, but also provide a discussion on security and privacy issues. Roman *et. al.* [105] present features and challenges of security and privacy in distributed IoT. In their paper, the authors classify IoT systems into four types: centralized IoT, collaborative IoT, connected IoT, and distributed IoT. After analyzing the features of each type of IoT systems, they list a set of security challenges in terms of the traditional security requirements and discuss promising approaches to address these challenges. Similarly, work by Jing *et. al.* [106] surveys security in different layers including perception layer, transportation layer and application layer. The paper discusses security issues in RFID, Wireless Sensor Networks, and in network communication protocols as well as application layer protocols. Suo *et. al.* present a review of security in IoT [107]. They analyze security issues in each layer of IoT systems in a general IoT architecture and give a review of the existing security tools. Security challenges are discussed briefly. Security and privacy issues are also examined in [108] and [109]. They summarize the challenges from the viewpoint of traditional security requirements and present a brief review of the existing technologies. Similarly, Hossain *et. al.* review security issues and challenges in IoT from the viewpoint of limitations in hardware, software and networks [110]. Security challenges in the IP-based IoT system are studied in [81]. The paper reviews the architecture design of a IP-based IoT and presents a list of security challenges in the context of standard IP-based security protocols. IoT security challenges are also reviewed in [111]. Our work extends [111] and differs from all above listed related work by presenting a comprehensive analysis on the new challenges and analyzing the security deployment problem in IoT systems. Several open security issues are identified at each layer in the IoT architecture.

Weber provides a review of privacy issues in IoT systems from the legal point of view [112]. A list of attack models are discussed as well. In [113], Covington and Carskadden present a list of attacks that can be launched against the IoT systems. Zhang *et al.* [114] describe various communication scenarios in IoT systems and analyzes several authentication schemes for their application in IoT. As an important layer in the IoT architecture, security issues in the fog/edge layer are analyzed in [115]. The authors investigate the security and privacy issues in the Fog

computation paradigm and study the man-in-the-middle attack. Similarly, cloudlet mesh is used to secure mobile clouds in [116]. There are also many other papers working on a specific security problem and proposing solutions for that problem like Sybil attack [117].

8. Conclusion

With increasing deployments of IoT systems, security becomes a key component to protect both the cyber and the physical world. This paper first analyzes the new security challenges presented by the features of IoT systems, especially by resource-constrained IoT end devices and the tight coupling of the cyber and physical world. Then three architectural security designs are summarized to guide future security protocol and algorithm design. Advantages and limitations of each design are analyzed in detail. Examples of how to implement each design are presented. Based on our analysis, low capable end devices need help from the levels above in order to achieve a good level of security of the whole IoT system.

Acknowledgments

This research is partially supported by the National Natural Science Foundation of China under Grant No:61672016.

References

[1] A. L. L. Atzori, G. Morabito, The internet of things: A survey, Computer networks 54 (15) (2010) 2787–2805.

[2] S. Greengard, Smart transportation networks drive gains, Communications of the ACM 58 (1) (2015) 25–27.

[3] G. Pan, et al., Trace analysis and mining for smart cities: issues, methods, and applications, IEEE Communications Magazine 121 (6) (2015) 120–126.

[4] A. GhaffarianHoseini, et al., The essence of future smart houses: From embedding ict to adapting to sustainability principles, Renewable and Sustainable Energy Reviews 24 (1) (2013) 593–607.

[5] M. Amin, W. Bruce, Toward a smart grid: power delivery for the 21st century, IEEE Power and energy Magazine 3 (5) (2005) 34–41.

[6] J. Gubbi, et al., Internet of things (iot): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (7) (2013) 1645–1660.

[7] Z. Liu, K.-K. R. Choo, M. Zhao, Practical-oriented protocols for privacy-preserving outsourced big data analysis: Challenges and future research directions, Computers & Security 69 (2017) 97–113.

[8] H. J, G. W. B, C. K.-K. R, Medical device vulnerability mitigation effort gap analysis taxonomy, Smart Health in press (2018) https://doi.org/10.1016/j.smhl.2017.12.001.

[9] A. Anjum, et al., An efficient privacy mechanism for electronic health records, Computers & Security 72 (2018) 196–211.

[10] V. Casola, A. Castiglione, K.-K. R. Choo, C. Esposito, Healthcare-related data in the cloud: Challenges and opportunities, IEEE Cloud Computing 3 (6) (2016) 10–14.

[11] Baby monitor hacker still terrorizing babies and their parents.
URL http://www.forbes.com/sites/kashmirhill/2014/04/29/baby-monitor-hacker-still-terrorizing-babies-and-their-parents/#5b91ff7717e2

[12] Previous next black hat usa 2015: The full story of how that jeep was hacked.
URL https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/

[13] Your hackable house.
URL http://money.cnn.com/interactive/technology/hackable-house/

[14] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, X. Fu, Security vulnerabilities of internet of things: A case study of the smart plug system, IIEEE Internet-of-Things (IoT) Journal pp (99) (2017) 1–1.

[15] C. Osborne, Vulnerable smart home iot sockets let hackers access your email account, [http://www.zdnet.com/article/vulnerable-smart-home-iot-sockets-act-as-bridge-to-take-down-full-networks/], online; accessed 24-October-2017.

[16] M.-A. Russon, Hackers turning millions of smart cctv cameras into botnets for ddos attacks, [http://www.ibtimes.co.uk/

hackers-turning-millions-smart-cctv-cameras-into-botnets-ddos-attacks-1525736], online; accessed 24-October-2017.

[17] T. Fox-Brewster, How hacked cameras are helping launch the biggest attacks the internet has ever seen, [https://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#705007235899], online; accessed 24-October-2017.

[18] KrebsOnSecurity.com, Hacked cameras, dvrs powered todays massive internet outage, [https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/], online; accessed 24-October-2017.

[19] C. D'Orazio, K.-K. R. Choo, L. T. Yang, Data exfiltration from internet of things devices: ios devices as case studies, IEEE Internet of Things Journal 4 (1) (2017) 524–535.

[20] C. D'Orazio, K.-K. R. Choo, A technique to circumvent ssl/tls validations on ios devices, Future Generation Computer Systems 74 (2017) 366–374.

[21] C. J. D'Orazio, R. Lu, K.-K. R. Choo, A. V. Vasilakos, A markov adversary model to detect vulnerable ios devices and vulnerabilities in ios apps, Applied Mathematics and Computation 293 (2017) 523–544.

[22] C. D'Orazio, K.-K. R. Choo, Circumventing ios security mechanisms for apt forensic investigations: A security taxonomy for cloud apps, Future Generation Computer Systems 79 (2018) 274–261.

[23] Q. Do, B. Martini, K.-K. R. Choo, Is the data on your wearable device secure? an android wear smartwatch case study, Softw., Pract. Exper. 47 (3) (2017) 391–403.

[24] Q. Do, B. Martini, K.-K. R. Choo, A data exfiltration and remote exploitation attack on consumer 3d printers, IEEE Trans. Information Forensics and Security 11 (10) (2016) 2174–2186.

[25] Q. Do, B. Martini, K.-K. R. Choo, Exfiltrating data from android devices, Computers & Security 48 (2015) 74–91.

[26] R. Errabelly, K. Sha, W. Wei, T. A. Yang, Z. Wang, Edgesec: Design of an edge layer security service to enhance internet of things security, in: Proceedings of the First IEEE International Conference on Fog and Edge Computing (ICFEC 2017), 2017.

[27] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet of Things Journal 3 (5) (2016) 637–646.

[28] D. X. Li, W. He, S. Li, Internet of things in industries: A survey, IEEE Transactions on industrial informatics 10 (4) (2014) 2233–2243.

[29] A. Jacobsson, P. Davidsson, Towards a model of privacy and security for smart homes, in: Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT 2015), 2015.

[30] Gartner, Gartner says a typical family home could contain more than 500 smart devices by 2022, [http://www.gartner.com/newsroom/id/2839717], online; accessed 13-September-2016.

[31] I. Rouf, et al., Neighborhood watch: security and privacy analysis of automatic meter reading systems, in: Proceedings of the 2012 ACM conference on Computer and communications security, 2012.

[32] X. Pan, Z. Ling, A. Pingley, W. Yu, K. Ren, N. Zhang, X. Fu, How privacy leaks from bluetooth mouse?, IEEE Transactions on Dependable and Secured Computing (TDSC) 13 (4) (2016) 461–473.

[33] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid - the new and improved power grid: A survey, IEEE Communications Surveys and Tutorials 14.

[34] S. Depuru, L. Wang, V. Devabhaktuni, Smart meters for power grid: Challenges, issues, advantages and status, Renewable and sustainable energy reviews 15 (6) (2011) 2736–2742.

[35] S. Karnouskos, O. Terzidis, P. Karnouskos, An advanced metering infrastructure for future energy networks, in: Proceedings of NTMS 2007 Conference, 2007.

[36] M. Faisal, Z. Aung, J. Williams, A. Sanchez, Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study, IEEE Systems Journal 9 (1) (2015) 31–44.

[37] A. Molina-Markham, et al., Private memoirs of a smart meter, in: Proceedings of the Second ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, 2010.

[38] Q. Yang, D. An, R. Min, W. Yu, X. Yang, W. Zhao, On optimal pmu placement-based defense against data integrity attacks in smart grid, IEEE Transactions on Information Forensics and Security 12 (7) (2017) 1735–1750.

[39] X. Zhang, X. Yang, J. Lin, G. Xu, W. Yu, On data integrity attacks against real-time pricing in energy-based cyber-physical systems, IEEE Transactions on Parallel and Distributed Systems (TPDS) 28 (1) (2017) 170–187.

[40] J. Lin, W. Yu, X. Yang, On false data injection attack against multistep electricity price in electricity market in smart grid, IEEE Transactions on Parallel and Distributed Systems (TPDS) 27 (1) (2016) 286–302.

[41] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, W. Zhao, On false data-injection attacks against power system state estimation: Modeling and countermeasures, IEEE Transactions on Parallel and Distributed Systems (TPDS) 25 (3) (2014) 717–729.

[42] X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, W. Zhao, A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems, IEEE Transactions on Computers (TC) 64 (1) (2015) 4–18.

[43] G. Leroy, H. Chen, T. Rindflesch, Smart and connected health, IEEE Intelligent Systems 29 (3) (2014) 2–5.

[44] M. Hartman, Tools for the vision impaired [opinion], IEEE Technology and Society Magazine 34 (2) (2015) 16–17.

[45] M. Rahman, B. Carbunar, M. Banik, Fit and vulnerable: Attacks and defenses for a health monitoring device, arXiv preprint arXiv (1304) (2013) 5672.

[46] J. L. Fernandez-Aleman, et al., Security and privacy in electronic health records: A systematic literature review, Journal of biomedical informatics 46 (3) (2013) 541–562.

[47] N. Ekedebe, W. Yu, C. Lu, H. Song, Y. Wan, Securing transportation cyberphysical systems, CRC Press, Boca Raton, 2015.

[48] J. Lin, W. Yu, N. Zhang, X. Yang, L. Ge, On data integrity attacks against route guidance in transportation-based cyber-physical systems, in: Proceedings of the 14th IEEE Annual Confernece in Consumer Communications and Networking Conference (CCNC 2017), 2017.

[49] Y. Sun, et al., Constructing the web of events from raw data in the web of things, Mobile Information Systems 10 (1) (2014) 105–125.

[50] Y. Sun, A. Jara, An extensible and active semantic model of information organizing for the internet of things, Personal and Ubiquitous Computing 18 (8) (2014) 1821–1833.

[51] F. Bonomi, et al., Fog computing: A platform for internet of things and analytics, Springer International Publishing, 2014.

[52] K. Sha, W. Wei, A. Yang, W. Shi, Security in internet of things: Opportunities and challenges, in: Proceedings of International Conference on Identification, Information & Knowledge in the Internet of Things (IIKI 2016), 2016.

[53] S. Boyer, SCADA: supervisory control and data acquisition, International Society of Automation, 2009.

[54] C. Lin, G. Wu, Enhancing the attacking efficiency of the node capture attack in wsn: a matrix approach, The Journal of Supercomputing 66 (2) (2013) 989–1007.

[55] M. Alramadhan, K. Sha, An overview of access control mechanisms for internet of things, in: Proceedings of the 26th International Conference on Computer Communications and Networks (ICCCN 2017), 2017.

[56] B. Morrow, Byod security challenges: control and protect your most sensitive data, Network Security 2012 (12) (2012) 5–8.

[57] I-210+c smart grid enables consumer friendly metering.
URL http://www.gegridsolutions.com/smartmetering/catalog/i210plusc.htm#i210c2

[58] R. Wang, The magic of RFID, ACM Queue 2 (7) (2004) 41–48.

[59] K. Sha, N. Alatrash, Z. Wang, A secure and efficient framework to read isolated smart grid devices, IEEE Transactions on Smart Grid 8 (6) (2017) 2519 – 2531.

[60] L. Sweeney, k-anonymity: a model for protecting privacy, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10 (5) (2002) 557–570.

[61] J. Qi, et al., Security of the internet of things: Perspectives and challenges, Wireless Networks 20 (8) (2014) 2481–2501.

[62] Z. Wan, et al., Skm: Scalable key management for advanced metering infrastructure in smart grids, IEEE Transactions on Industrial Electronics 61 (12) (2014) 7055–7066.

[63] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, C. Xu, Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things, in: Proceedings of the 14th ACM Workshop on Hot Topics in Networks, 2015.

[64] Z. Yan, P. Zhang, A. V. Vasilakos, A survey on trust management for internet of things, Journal of network and computer applications 42 (4) (2015) 120–134.

[65] Q. Han, H. Wen, G. Feng, B. Wu, M. Ren, Self-nominating trust model based on hierarchical fuzzy systems for peer-to-peer networks, Peer-to-Peer Networking and Applications 9 (6) (2016) 1020–1030.

[66] S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Computer Networks 76 (1) (2015) 146–164.

[67] Why iot security will be a nightmare for everyone.
URL http://oemhub.bitdefender.com/why-iot-security-will-be-a-nightmare-for-everyone

[68] C. Kruger, G. Hancke, Implementing the internet of things vision in industrial wireless sensor networks, in: Proceedings of the 12th IEEE International Conference on Industrial Informatics (INDIN 2014),, 2014.

[69] Z. Song, M. T. Lazarescu, R. Tomasi, L. Lavagno, M. A. Spirito, High-level internet of things applications development using wireless sensor networks, in: Internet of Things, Springer, 2014, pp. 75–109.

[70] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Communications of the ACM 47 (6) (2004) 53–57.

[71] G. A. Y. Wang, B. Ramamurthy, A survey of security issues in wireless sensor networks, IEEE Communications Surveys and Tutorials 8 (2) (2006) 2–23.

[72] L. Larkey, L. Bettencourt, A. Hagberg, In-situ data quality assurance for environmental applications of wireless sensor networks, Tech. Rep. Report LA-UR-06-1117, Los Alamos National Laboratory (Oct. 2006).

[73] T. Bokareva, et al., Wireless sensor networks for battlefield surveillance, in: Proceedings of Land Warfare Conference 2006, 2006.

[74] K. Sha, J. Gehlot, R. Greve, Multipath routing techniques in wireless sensor networks: A survey, Wireless personal communications 70 (2) (2013) 807–829.

[75] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: Proceedings of ACM CCS'03, 2003.

[76] W. Du, J. Deng, Y. Han, P. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in: Proceedings of ACM CCS'03, 2003.

[77] K. Sha, Y. Xi, W. Shi, L. Schwiebert, T. Zhang, Adaptive privacy-preserving authentication in vehicular networks, in: Proceedings of the International Workshop on Vehicle Communication and Appliations, 2006.

[78] Y. Xi, K. Sha, W. Shi, L. Schwiebert, T. Zhang, Enforcing privacy using symmetric key-set in vehicular networks, in: Proceedings of the 8th International Symposium on Autonoumous Decentralized Systesms, 2007.

[79] M. Anita, R. Geetha, E. Kannan, A novel hybrid key management scheme for establishing secure communication in wireless sensor networks, Wireless Personal Communications 82 (3) (2015) 1419–1433.

[80] D. Liu, P. Ning, R. Li, Establishing pairwise keys in distributed sensor networks, ACM Transactions on Information and System Security (TISSEC) 8 (1) (2005) 41–77.

[81] T. Heer, et al., Security challenges in the ip-based internet of things, Wireless Personal Communications 61 (3) (2011) 527–542.

[82] C. Huitema, IPv6: the new Internet protocol, Prentice Hall PTR Upper Saddle River, NJ, USA, 1996.

[83] Z. Shelby, C. Bormann, 6LoWPAN: The wireless embedded Internet, Vol. 43, John Wiley & Sons, 2011.

[84] R. Roman, P. Najera, J. Lopez, Securing the internet of things, Computer 44 (9) (2011) 51–58.

[85] J. Cui, W. Xu, K. Sha, H. Zhong, An efficient identity-based privacy-preserving authentication scheme for vanets, in: Proceedings of 13th EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2017), 2017.

[86] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, Physical unclonable functions and applications: A tutorial, Proceedings of the IEEE 102 (8) (2014) 1126–1141.

[87] M. Rostami, M. Majzoobi, F. Koushanfar, D. S. Wallach, S. Devadas, Robust and reverse-engineering resilient puf authentication and key-exchange by substring matching, IEEE Transactions on Emerging Topics in Computing 2 (1) (2014) 37–49.

[88] A. Aysu, E. Gulcan, D. Moriyama, P. Schaumont, , M. Yung, End-to-end design of a puf-based privacy preserving authentication protocol, in: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems, 2015.

[89] L. Bolotnyy, G. Robins, Physically unclonable function-based security and privacy in rfid systems, in: Proceedings of Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07), 2017.

[90] J. Delvaux, I. Verbauwhede, Side channel modeling attacks on 65nm arbiter pufs exploiting cmos device noise, in: Proceedings of 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2013.

[91] X. Xu, W. Burleson, Hybrid side-channel/machine-learning attacks on pufs: a new threat?, in: Proceedings of the conference on Design, Automation and Test in Europe, 2014.

[92] R. Hummen, et al., Tailoring end-to-end ip security protocols to the internet of things, in: Proceedings of the 21st IEEE International Conference on Network Protocols (ICNP), 2013.

[93] T. Kothmary, et al., A dtls based end-to-end security architecture for the internet of things with two-way authentication, in: Proceedings of the IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops), 2012.

[94] C. Hennebert, J. D. Santos, Security protocols and privacy issues into 6lowpan stack: a synthesis, IEEE Internet of Things Journal 1 (5) (2014) 384–398.

[95] K. Krentz, H. Rafiee, C. Meinel, 6lowpan security: adding compromise resilience to the 802.15. 4 security sublayer, in: Proceedings of the International Workshop on Adaptive Security, 2013.

[96] I. S. Association, et al., Ieee std 802.15. 4-2011, ieee standard for local and metropolitan area networks-part 15.4: Low-rate wireless personal area networks (lr-wpans) (Sep 2011).

[97] G. Patti, G. Alderisi, L. Bello, Introducing multi-level communication in the ieee 802.15. 4e protocol: the multichannel-lldn, in: Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA), 2014.

[98] S. Raza, et al., Securing communication in 6lowpan with compressed ipsec, in: Proceedings of the 2011 International Conference on Distributed Computing in Sensor Systems (DCOSS'11), 2011.

[99] S. Chatterjee, A. K. Das, An effective ecc-based user access control scheme with attribute-based encryption for wireless sensor networks, Security and Communication Networks 8 (9) (2015) 1752–1771.

[100] V. G. Cerf, P. S. Ryan, M. Senges, R. S. Whitt, Iot safety and security as shared responsibility, Journal of Business Informatics 35 (1) (2016) 7–19.

[101] K. Sha, C. Xu, Z. Wang, One-time symmetric key based cloud supported secure smart meter reading, in: Proceedings of the 23rd International Conference on Computer Communications and Networks (ICCCN 2014), 2014.

[102] S. Raza, L. Wallgren, T. Voigt, Svelte: Real-time intrusion detection in the internet of things, Ad Hoc Networks 11 (8) (2013) 2661–2674.

[103] J. Singh, T. Pasquier, J. Bacon, H. Ko, D. Eyers, Twenty security considerations for cloud-supported internet of things, IEEE Internet of Things Journal 3 (3) (2016) 269–284.

[104] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IIEEE Internet-of-Things (IoT) Journal pp (99) (2017) 1–1.

[105] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013) 2266–2279.

[106] Q. Jing, et al., Security of the internet of things: Perspectives and challenges, Wireless Networks 20 (8) (2014) 2481–2501.

[107] H. Suo, Others, Security in the internet of things: a review, in: Proceedings of the IEEE International Conference on Computer Science and Electronics Engineering, 2012.

[108] M. Abomhara, G. Koien, Security and privacy in the internet of things: Current status and open issues, in: Proceedings of the IEEE International Conference on Privacy and Security in Mobile Systems, 2012.

[109] X. Xu, Study on security problems and key technologies of the internet of things, in: Proceedings of the 5th International Conference on Computational and Information Sciences, 2013.

[110] M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: Proceedings of the 2015 IEEE World Congress on Services, 2015.

[111] K. Sha, W. Wei, A. T. Yang, W. Shi, Security in internet of things: Opportunities and challenges, in: Proceedings of 2016 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI'16), 2016.

[112] R. Weber, Internet of things-new security and privacy challenges, Computer Law & Security Review 26 (1) (2010) 23–30.

[113] M. Covington, R. Carskadden, Threat implications of the internet of things, in: Proceedings of the 5th IEEE International Conference on Cyber Conflict (CyCon), 2013.

[114] Z. Zhang, M. Cho, S. Shieh, Emerging security threats and countermeasures in iot, in: Proceedings of 10th ACM Symposium on Information, Computer and Communications Security, 2015.

[115] P. Panciatici, G. Bareux, L. Wehenkel, Operating in the fog: Security management under uncertainty, IEEE Power and Energy Magazine 10 (5) (2012) 40–49.

[116] Y. Shi, S. Abhilash, K. Hwang, Cloudlet mesh for securing mobile clouds from intrusions and network attacks, in: Proceedings of the 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2015.

[117] K. Zhang, et al., Sybil attacks and their defenses in the internet of things, IEEE Internet of Things Journal 1 (5) (2014) 372–383.

Kewei Sha is an Associate Director of Cyber Security Institute and Assistant Professor of Computer Science at University of Houston - Clear Lake (UHCL). Before he moved to UHCL, he was the Department Chair and Associate Professor in the Department of Software Engineering at Oklahoma City University (OCU). He received Ph.D. in Computer Science from Wayne State University in 2008. His research interests include Internet of Things, Cyber-Physical Systems, Edge Computing, Network Security and Privacy, and Data Management and Analytics. His research has been supported by NSF, NSFC, UHCL and OCU. He received 2018 Albert Nelson Marquis Lifetime Achievement Award and IEEE Outstanding Leadership Award in 2015. He is a Senior member of both ACM and IEEE.

Wei Wei is an Assistant Professor in Computer Information Systems at the University of Houston-Clear Lake (UHCL). She received her Ph.D. in Management Information Systems from the University of Arizona, Tucson, United States (2010). She also works at the Cyber Security Institute at UHCL. Her research interests include network security, cybersecurity education, and big data analytics for various purposes such as security intelligence and public relation management.

T. Andrew Yang earned his Ph.D. in Information Science from the University of Minnesota, and is currently with the faculty of the Computing Science Department in the University of Houston-Clear Lake. His research interests include computer security, network security, wireless and ad hoc networks, information system education, and cybersecurity curricular design. His research and development work have been sponsored by various federal, state, and local agencies.

Zhiwei Wang is an associate professor of the School of Computer at Nanjing University of Posts and Telecommunications from 2009 to now. His research interests include applied cryptography, security and privacy in mobile and wireless systems, clouding computing and fog/edge computing. He has published over 40 journal articles and referred conference papers.

Weisong Shi is a Charles H. Gershenson Distinguished Faculty Fellow and a professor of Computer Science at Wayne State University. His research interests include Edge Computing, Computer Systems, energy-efficiency, and wireless health. Hereceived his BS from Xidian University in 1995, and PhD from

the Chinese Academy of Sciences in 2000, both in Computer Engineering. He is a recipient of the National Outstanding PhD dissertation award of China and the NSF CAREER award. He is an IEEE Fellow and ACM Distinguished Scientist.

When Internet of Things (IoT) applications become pervasive in daily life, security issues in IoT have caught significant attention in both academia and industry. Compared to traditional computing systems, IoT systems have more inherent vulnerabilities, and meanwhile, could have higher security requirements. However, the current design of IoT does not effectively address the higher security requirements posed by those vulnerabilities. Many recent attacks on IoT systems have shown that novel security solutions are needed to protect this emerging system. This paper studies security challenges and issues in IoT and makes the following contributions that advance the field.

1) We analyze security challenges resulted from the special characteristics of the IoT systems and the new features of the IoT applications.
2) We propose three architectural security designs and analyze the strength and weakness of each design. Examples of how to implement these designs are discussed.
3) We identified a set of open security issues in the context of different layers in IoT architecture.