Internet Of Things Security From Data Perspectives: A Survey

[1] Shejina N M [2] Shabna K A [3] Dr. S Brilly Sangeetha

[1] Assistant Professor, Computer Science and Engineering [2] Assistant Professor, Computer Science and Engineering [3] Associate Professor, Computer Science and Engineering, IES College Of Engineeering

Abstract*— The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. It consists of all the web-enabled devices that collect, send and act on data they acquire from their surrounding environments using embedded sensors, processors and communication hardware. The Rapid growth of IoT is constrained by resource use and fears about privacy and security. Data collected and shared in the IoT plays an important role in the significance of the IoT. This survey analyzes various a framework for IoT security observation that takes both the typical IoT architecture and the IoT data life cycle into account, which outlines IoT security in three dimensions, i.e., the one-stop dimension, the multi-stop dimension and the end-application dimension. This paper mainly focusing on methods for IoT Security from data perspectives.

Index Terms— Data life cycle, Forencis ,Internet of things ,Privacy, Safety, Security.

IoT is creating a giant network where all the devices are connected to each other and providing them with the capability to interact with each other. This is driving the automation to a next level where devices will communicate with each other and make decisions on their own without any human interventions. It is a marvel of technology development, which enhances more and more pervasive connectivity around the world. It expands the communication capability of information and communication technologies (ICTs) from “Any TIME”and “Any PLACE”to “Any THING”[1] . However, on the other hand, it makes the security situation more and more severe.

Obviously, the IoT stimulates an explosive growth of data. The Norwegian research organization SINTEF pointed out that over the past two years, 90 percent of the world’s data had been generated at a speed of over 205,0 0 0 gigabytes per second, which was approximately equivalent to 150 million books [2] . IoT provides smart services by extracting vital information from differents kinds of data collected by IoT end-point devices, which has a significant impact on social production and people’s life. IoT is incomplete without the consideration of data.

An IoT end-point device is not only a simple data collecting device. Most importantly, it has mandatory communication capabilities. It is a kind of data source in some sense, which may provide data to back-end servers on the Internet. Standalone devices such as smart watches or smart meters are counted as IoT devices. However, IoT devices are usually embedded in large systems, such as electronic control units (ECU) in networked vehicles [3] .

A great value of the IoT is that it can capture and make use of a variety of data concerning natural environments as well as human beings. Data makes the IoT alive. Observing data in an IoT environment may help to understand the security of the IoT, likewise blood in a human body is useful to have insights into people’s health.

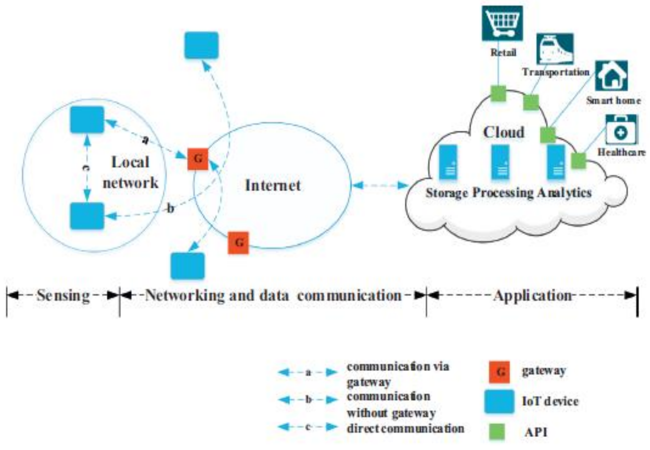

Fig. 1. An overall architecture of an IoT system.

This survey consider a framework that takes both IoT architectures and data life cycles into account. As shown in Fig. 1 , one of the typical IoT architectures describes the IoT as a multi- layered network, which consists of a sensing layer, a networking and data communication layer and an application layer [15] . It can be divided into three dimensions, which are named as one-stop dimension, multi-stop dimension and end-application dimension. These dimensions have their focuses on a single IoT device, IoT entity groups and IoT applications, respectively. This survey paper explores IoT security through these dimensions. From the one-stop dimension, data on one IoT device is observed. From the multi-stop dimension, data moving in a group of IoT entities is observed. From the end- application dimension, data used in IoT applications is observed. With the one-stop dimension, IoT security is explored based on data that is captured by an end-point device and sent out to the Internet or that is received by the end-point device from the Internet. With the multi-stop dimension, IoT security is discussed in consideration of data flowing among a group of IoT entities. With the end-application dimension, IoT security is analyzed according to the usage of data in IoT applications. Put together, investigations from the whole framework may present a holistic landscape of IoT security.

Observed from its whole life cycle, data may exist anywhere in the IoT environment, including on an end-point device, on the Internet, or in a cloud. IoT data may flow from IoT end-point devices through the Internet to a cloud, or vice versa. Obviously, IoT security related to IoT data must be investigated with consideration of the whole IoT environment. However, the most IoT-specific points of IoT security that call for IoT-specific solutions are lying in the space from IoT end-point devices to the border of the Internet. Therefore, the paper focuses on this domain, which we call the end-point domain for brevity. It makes an in-depth analysis of the latest development in IoT security from data perspectives, summarizes open issues, and suggests promising directions for further study and applications of IoT security.

The rest of the paper is organized as follows. In Section 2 , In Sections 3, and 4 , present discussions of IoT security from each dimension, respectively. Finally, concluded with Section 5.

2. IOT SECURITY FROM ONE STOP DIMENSION

This section explore IoT security by analyzing data on an IoT end-point device. Data may be collected and sent out to the Internet by an end-point device, or may be received by the end- point device from the Internet. Data flowing to and from an end- point device, i.e., input data and output data, which has interaction effects between the device and the Internet, should be considered for IoT security.

2.1 Output data related security

Massive IoT end-point devices are collecting a large volume of data and uploading it to the Internet for IoT applications. Some sensory data collected by IoT devices is sensitive and highly valuable, which is potential gains for attackers and commercial competitors. So IoT end-point devices should ensure the confidentiality requirement of data provided to the Internet. Additionally, the authenticity of output data has a direct impact on the reliability of services involving industry, economy, and social life. Therefore, it is important for IoT devices to ensure the confidentiality and authenticity of output data to guarantee the security of IoT applications and services.

2.1.1 Confidentiality

A general method for ensuring data confidentiality is encryption. IoT devices are usually dedicated devices with limited resources such as low computing power (e.g., 8-bit microcontroller), limited battery supply, small (gate) area, and limited storage [16]. General encryption algorithms that consume excessive resources may not be applicable to resource-constrained devices. In IoT, the overhead of encryption algorithms should be reasonable for device performance when providing a sufficient level of security [16]. There is an urgent need for lightweight ciphers to ensure the confidentiality of IoT data throughout its life cycle.

2.1.2 Authenticity

Data sensed and generated by IoT devices should be trustworthy to reflect the real-world environment precisely. The authentic ity of output data has a significant impact on the security of IoT applications. An IoT device is usually unattended and lacks physical protection. Physical attacks on a device, including node copying, replacement, and hijacking, may compromise the integrity of the device. Considering the authenticity of output data generated by an IoT device, it is extremely important to verify the integrity of the device. Generally, attestation techniques are widely used to verify the integrity of devices with the dedicated hardware(e.g., TPM). Traditional attestation methods designed for resource-rich devices may not be suitable for direct application to IoT devices to verify whether the device has been tampered. IoT devices call for lightweight attestation methods.

2.2 Input data related security and safety

IoT bridges the gap between the cyber world and the physical world, so that hacking into a device in the cyber world can bring threats to the real-world and vice versa. Changes in the physical state of the device can affect its computing system, and data changes in the network or computing system can also affect the physical state of the device [8].

Safety means “freedom from accidents or losses”[8] . Some de vices may execute operations based on data received from the Internet input data, coupling security and safety concerns in IoT. Leveraging input data, including the false data generated by the system itself and the malicious data sent by adversaries due to the vulnerabilities of systems, attackers may compromise the devices. Unsafe and insecure operations on IoT devices may result in a real loss of services and even the loss of life. For example, adversaries can send malicious control data to medical equipment to speed up the pacemaker or the drug infusion pumps, endangering user’s life.

2.3 Open issues

For confidentiality, current research on lightweight encryptions achieves a high degree of overhead reduction. Now, essential considerations of confidentiality on end devices should be more about practical applications of algorithms in the real world, including speed optimization and latency reduction.

For authenticity, more research on attestation for a group of devices is expected. Large scale usually implies heterogeneity, which increases the complexity of attestation. An IoT device can switch from online to offline at any time, which makes it dynamic and indeterminable. It’s difficult to obtain the real status of a device swarm. The issues about how to improve efficiency, robustness, and accuracy of swarm attestation have not been solved well.

Furthermore, IoT devices lack a common update mechanism due to heterogeneous computing systems. It is hard to apply timely updates for all end devices. Thus, vulnerabilities exposed for a long time can still be seen on most IoT devices. They are around our daily lives but quite vulnerable to exploitation, which is both a technical and social concern.

3. IoT SECURITY FROM THE MULTI-STOP DIMENSION

In this section, investigating IoT security by observing data that may flow among a group of IoT entities. Secure communica tion, authentication and access control related to interactions of IoT entities will be covered. Interconnectivity is a fundamental charac teristic of IoT entities that can directly or indirectly interact with the Internet. To ensure the interactions of entities, communication networks transfer data captured by IoT end-point devices to appli cations and other devices, as well as instructions from applications to IoT devices [1].

3.1. Communication related security

In general, there are three types of communication for IoT devices to communicate with others: communicating through the Internet via a gateway, communicating through the Internet without a gateway, communicating through a local network (i.e., a network providing local connectivity between devices and between devices and a gateway, such as an ad-hoc network) [1], as shown in Fig. 1 . Secure communication capabilities of IoT entities need to ensure the security of data transmission in IoT networks. The main research on the security issues related to communication falls into three categories: (1) designing secure communi cation protocols for IoT devices; (2) designing efficient malicious node identification systems; (3) designing lightweight trust man- agement schemes to evaluate the trust level of nodes in an IoT local network.

3.2. Authentication and access control

IoT integrates a large number of physical objects that are uniquely identified, ubiquitously interconnected and accessible through the Internet [16]. Authentication and access control are the main security mechanisms to ensure the security of interactions among different entities (devices or users). Access control and authentication are the process of determining whether an entity can access resources and authentication, a process of identifying an entity, is a prerequisite for authorization [17] . With the limitation in computing, energy, storage of devices, the need for schemes of authentication and access control applicable to IoT is pressing.

In various IoT application scenarios, such as smart healthcare, intelligent transportation and smart home, heterogeneous devices and network architecture lead to different demands of authentication and access control to ensure the security of interactions among entities.

3.3. Open issues

Firstly, because IoT networks are usually self-organizing and wireless communication technologies are widely used, it is possible for malicious nodes to be introduced into a local network easily. However, there is still not any effective and lightweight approach to malicious nodes detection in IoT. Blockchain technology can build mutual trust at low cost in a decentralized environment without a central manager. It may be a future research direction for the security of data exchange and multi-party collaboration in IoT.

4. IOT SECURITY FROM THE END-APPLICATION DIMENSION

In this section , scrutinizing IoT security by analyzing data used in IoT applications. A huge amount of data is collected by IoT devices, transferred over networks and used by various IoT applications. Keeping IoT data life cycles in mind, from the view of data usage in IoT applications, will investigate privacy, forensics, and social or legal challenges of the whole IoT system.

4.1. Privacy concern

In real IoT scenarios, different IoT applications leverage data col lected from IoT devices to provide convenient and smart services for users while introducing potential privacy concerns. Private information may be leaked at any phase of a data life cycle in IoT environments. Therefore, privacy concerns must be considered from system perspectives. Besides individual data like fingerprints and heartbeats, which are directly related to a user's privacy, some environmental information sensed by IoT devices can be utilized to infer extra information about user's preference and trajectory. The aggregated data from various IoT devices can add up to a total surveillance of our lives [18]. A user can be both a recipient of data or services and a subject to data collection by smart things at the same time . Compared to the Internet where users have to take an active role to put their privacy at stake (i.e., query for ser- vices), much data about users are collected and transferred in IoT without their awareness [19] . A large volume of data is being generated by IoT automatically with higher velocity than before, and any breaches in security will have a knock-on effect on personal security and privacy.

4.2. Forensics challenges

With IoT gradually permeating our lives, accidents and attacks involving IoT services or devices will happen unavoidably. Forensic investigations need to be conducted in the IoT infrastructure, when IoT is the target of attacks or used to launch an attack. Data collected and shared by IoT applications introduces both opportunities and challenges into forensics. In the context of IoT, there are a diverse range of potential evidence sources, so that the forensics may need to combine multiple digital forensic methods and techniques, increasing the difficulty of forensics. Specialized tools and techniques, as well as standardized procedures are required for col- lecting, preserving and analyzing residual evidence in the IoT en- vironment. Traditional digital forensics cannot be directly applied in IoT due to highly heterogeneous and frequently changing envi ronments. With limited memory of most IoT devices, they need to transfer data to a cloud or a local hub before evidence is overwrit- ten. IoT forensics can be identified as a combination of three digital forensics schemes, including cloud forensics, network forensics and device level forensics [20] . However, as evidence can be modified at any step of data life cycles, it presents challenges to make the chain of evidence secure.

4.3. Social or legal challenges

The use of IoT is dramatically changing people's everyday life, introducing not only technical challenges but also social or legal challenges to IoT security.

Liability Dispute. Intelligent services provided by IoT may bring new responsibility disputes. For example, automated vehicles are being gradually put into use. When an accident with automated vehicles occurs, the judgment of accidental responsibility calls for a better legislation for the use of automated vehicles. The Australian National Transport Commission has drafted new Australian driving laws to support automated vehicles [21] .

Data Commodification. In IoT, the wide collection and usage of a large amount of data make data a commodity and develop as- set virtualization, bringing the problems of data ownership. How to standardize the management of data as a product? Who is the owner of the data? Can data be traded? All these questions bring corresponding responsibility issues. Data holders have the right to authorize and revoke authorization to the collection of their personal data. By fine-grained authorization based on context, data holders can just share the subset of data with the applications that they are willing to share with in the IoT environment.

Vulnerabilities of Social Engineering. IoT plays a vital role in human interactions, influencing social contact and people's everyday life. Fine-grained and ubiquitous data collection in IoT makes users vulnerable to social engineering attacks [22] . The best way to deceive a person is to gather as much information about him as possible. The emergence of IoT makes data collection easier by hijacking smart devices such as smart TVs, Fitbits, and Google Glass to monitor and learn voices, habits, and preferences of the target person.

Legislation Challenges. Although legislation cannot provide guarantees for the security of data usage in IoT applications, it is a way to compensate the damage caused by the misuse of data. Perfecting legislation and policy to protect data usage in IoT applications is pressing. Countries are making effort s to provide more protection for data applications.

4.4. Open issues

For privacy protection, as privacy regulations around the world have been in operation, the transfer and usage of private data ought to be subject to privacy regulations. However, there is still not any widely accepted technical standard for privacy protection of data storage, transmission, sharing as well as application. Privacy should be ensured from the whole system perspective. Privacy protection mechanisms of each product should be implemented in accordance with general technical standards rather than being implemented arbitrarily by developers. For forensics challenges, there are many fields that have not been fully investigated, such as applying blockchain technologies to evidence preservation. Standardized forensic investigation frame- works and efficient synchronization approaches for evidence in IoT are deserved to design.

5 .CONCLUSION

Considering that IoT data may reveal a novel clue to deal with IoT security. This survey sheds light on IoT security with IoT data as a leading factor. It devises a framework for IoT security observation that takes both the typical IoT architecture and the IoT data life cycle into account, which outlines IoT security in three dimensions, i.e., the one-stop dimension, the multi-stop dimension and the end-application dimension.

REFERENCES

[1] International Telecommunication Union , Overview of the Internet of things, 2012 .

[2] S. DuBravac, C. Ratti, The internet of things: Evolution or revolution?, 2015, (https://www.onr.com/blog/health- iot-adoption- hipaa- compliance- landscape/).

[3] Cloud Security Alliance , Security guidance for early adopters of the internet of things (iot), 2015 .

[4] S. Ray , Y. Jin , A. Raychowdhury , The changing computing paradigm with in- ternet of things: a tutorial introduction, IEEE Design Test 33 (2) (2016) 76–96 .

[5] J. Guo , I. Chen , J.J.P. Tsai , A survey of trust computation models for service management in internet of things systems, Comput. Commun. 97 (2017) 1–14 .

[6] Z. Yan , P. Zhang , A.V. Vasilakos , A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134 .

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

[8] M. Wolf , D. Serpanos , Safety and security in cyber-physical systems and in- ternet-of-things systems, Proc. IEEE 106 (1) (2018) 9–20 .

[9] A. Banerjee , K.K. Venkatasubramanian , T. Mukherjee , S.K.S. Gupta , Ensuring safety, security, and sustainability of mission-critical cyberphysical systems, Proc. IEEE 100 (1) (2012) 283–299 .

[10] F.A. Alaba , M. Othman , I.A.T. Hashem , F. Alotaibi , Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28 .

[11] S. Sicari , A. Rizzardi , L.A. Grieco , A. Coen-Porisini , Security, privacy and trust in internet of things: the road ahead, Comput. Netw. 76 (2015) 146–164 .

[12] 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 applica- tions, IEEE Internet Things J. 4 (5) (2017) 1125–1142 .

[13] Q. Jing , A.V. Vasilakos , J. Wan , J. Lu , D. Qiu , Security of the internet of things: perspectives and challenges, Wireless Netw. 20 (8) (2014) 2481–2501 .

[14] Y. Yang , L. Wu , G. Yin , L. Li , H. Zhao , A survey on security and privacy issues in internet-of-things, IEEE Internet Things J. 4 (5) (2017) 1250–1258 .

[15] R. Minerva, A. Biru, D. Rotondi, Towards a definition of the inter- net of things (IoT), IEEE Internet Initative (2015) 1–86 Available on: https://iot.ieee.org/images/files/pdf/IEEE _ IoT _ Towards _ Definition _ Internet _ of _ Things _ Revision1 _ 27MAY15.pdf . Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.

[16] D. Dragomir , L. Gheorghe , S. Costea , A. Radovici ,A Survey on Secure Commu- nication Protocols for IoT Systems, in: Secure Internet of Things (SIoT), 2016 International Workshop on, IEEE, 2016, pp. 47–62 .

[17] H. Kim , E.A. Lee , Authentication and authorization for the internet of things, IT Prof. 19 (5) (2017) 27–33 .

[18] R.H. Weber , Internet of things: privacy issues revisited, Comput. Law Secur. Rev. 31 (5) (2015) 618–627 .

[19] J. López , R. Rios , F. Bao , G. Wang , Evolving privacy: from sensors to the inter- net of things, Future Gener. Comp. Syst. 75 (2017) 46–57 .

[20] S. Zawoad , R. Hasan , Faiot: Towards building a forensics aware eco system for the internet of things, in: 2015 IEEE International Conference on Services Computing (SCC), IEEE, 2015, pp. 279–284 .

[21] Changing driving laws to support automated vehicles, (http://www.ntc.gov. au/current-projects/changing- driving- laws- to- support- automated- vehicles/ ?modeId=1064&topicId=1166).

[22] I.G. Harris, Social Engineering Attacks on the Internet of Things, (https://iot.ieee.org/newsletter/september-2016/social%2Dengineering% 2Dattacks%2Don%2Dthe%2Dinternet%2Dof%2Dthings.html).singular heading even if you have many acknowledgments..