Authentication in the Internet of Things

Di Weng, *11621046* and Qi Song, *21521081*

Abstract—The abstract goes here.

Index Terms—internet of things, authentication.

1 Introduction

The Internet of Things (IoT) and its related technologies have been actively studied and popularized in the past few years [4]. The idea of IoT was originally formulated from the emerging advanced network infrastructures that support a large number of interconnected things or objects, such as Radio-Frequency IDentification (RFID) tags, sensors, personal accessories like smart watches and mobile phones. The objects are then given unique addresses, through which they can communicate and cooperate with each other to complete collective tasks, while the addressing scheme will also enable IoT devices to be identifiable by external services and platforms [11] [25].

However, there is a long-standing argument about the definition of Internet of Things. IoT is a generic but vague concept with several missing definitions, for example, the range of objects and addressing schemes. This leads to manifold definitions of IoT presented in prior studies. The term, *Internet of Things*, is semantically composed by two words, *Internet* and *Things*, from which two different aspects of IoT technology can be derived, namely, Internet-oriented visions and things-oriented visions, and most of the previous definitions fall into these two categories. Additionally, some other studies suggest that the third aspect, semantic-oriented visions, is also a part of the IoT framework. These three visions (Fig. 1) are discussed as follows:

Internet-oriented visions focus on the connectivity of objects inside the IoT framework. Since Internet Protocol (IP) has been widely adopted in traditional network infrastructures and is already connecting millions of devices around the world, most of the definitions in the realm of Internet-oriented vision attempt to reuse lightweight variants of the IP stack to address the connectivity issues among IoT objects. One of the definitions is canonicalized by IPSO (Internet Protocol for Smart Objects) Alliance [30], an international organization consisting of 26 companies, including several notable manufacturers of embedding processing units like ARM and Intel. IPSO Alliance proposes the usage of IP architecture on the basis of communication techniques with low power consumption like IEEE 802.15.4 and 6LoWPAN [9]. The integrated IPv6 technology provides sufficient address space for IoT objects, and low-power design enables resource-constrained IoT devices to communicate at a lower rate but consume less power. There are other similar approaches like Internet Ø, allowing "IP over anything" by reducing the complexity of the IP stack.

Manuscript received June 28, 2017; revised June 28, 2017.

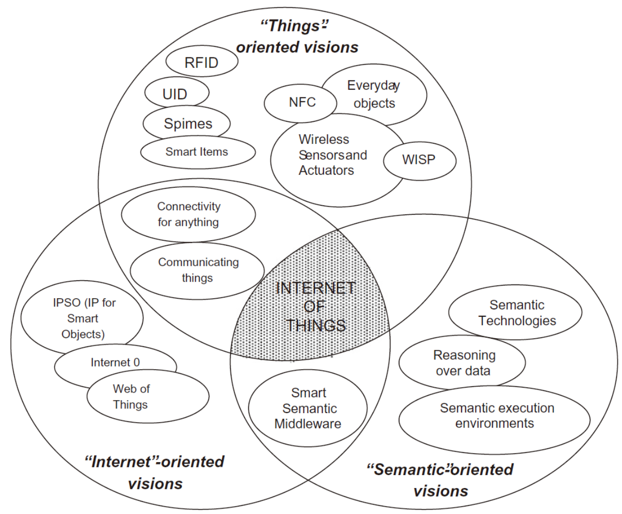

Fig. 1. Three visions of the Internet of Things paradigm by L. Atzori et al. [4], including Internet-oriented visions, Things-oriented visions, and Semantic-oriented visions. Their relations and components are described in a Venn diagram.

Things-oriented visions advocate wide-spread Radio-Frequency IDentification (RFID) tags as *things* in the IoT framework. By attaching RFID tags to everyday objects, Things-oriented visions enable users of IoT to track and identify these objects. The idea was first established by Auto-ID Labs [1], and later generalized by several studies [13] [24], which further extend identifiable tags into a Unique/Universal/Ubiquitous IDdentifier (UID) architecture. While the definition of IoT presented by these visions narrows it down to mere object identification, the maturity of RFID technologies and the popularity and enthusiasm in the business community show a promising adoption rate of such architecture. Moreover, by combining things-oriented visions with Internet-oriented visions, several unified definitions were proposed regarding both the identification and connectivity of objects, as stated by the European Commission [5]: "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts."

Semantic-oriented visions arise from the literature under an assumption that the number of interconnected objects exhausts the capability of direct management, where the organization of the information generated by these objects becomes challenging. Such issue can be addressed by integrating semantic technologies like data reasoning and semantic execution environment into the IoT framework [27].

As a promising technology, IoT was included in the list of six "Disruptive Civil Technologies" that will potentially generate huge impacts on US national power [8]. US National Intelligence Council, the author of the list, claimed that "popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development." Despite IoT's contribution to human's everyday life, it also brings severe security risks along the way due to its wide distribution and applicability. It is also stated in the aforementioned report that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date."

Four categories of security issues in the IoT framework are summarized by Alaba et al. [3], including application, architecture, communication, and data. With authentication and access control technologies, traditional computer networks have resolved a variety of security and privacy issues in three ways [16]: a) forbid unauthorized users to access resources; b) prohibit authorized users from accessing resources beyond their privileges; and c) grant correct resource access to authorized users. As a key issue in both categories of application and architecture, authentication technologies continues playing an important role in the security of IoT.

Two challenges arise while applying existing authentication techniques to the application and architecture of IoT devices. First, most of the IoT devices are resource-constrained, where most of the strong cryptography methods currently used cannot be computed fast enough to match the power supply of devices and the rate of information sensing. Second, the complex environment of IoT networks requires an extensible and scalable authentication scheme. The number of devices in an IoT network could scale up to millions, introducing difficulty in many aspects of traditional authentication, such as the distribution and revoking of symmetric encryption keys.

Apart from the machine authentication of IoT, which mainly consists of the authentication of application and architecture as stated above, user authentication [22] is also an essential part of IoT security paradigm. By integrating user authentication, IoT devices like mobile phones are able to identify owners with simple interactions and protect sensitive personal information from unauthorized users.

The work of this survey is divided as follows:

- **Presentation:** Qi Song presented the assigned paper [10], and Di Weng presented the survey on the authentication of the Internet of Things;
- **Writing:** Section 1, 2, and 5 were written by Di Weng, and Section 3 and 4 were written by Qi Song.

This survey is organized as follows: the machine authentication of IoT is covered in Section 2 and 3, which explain the authentication in IoT applications and architecture, respectively; then, Section 4 summarizes the user authentication in IoT framework briefly; finally, this survey is concluded in Section 5.

2 Application Authentication

Recent years have witnessed the great impacts brought by the Internet of Things technologies via a variety of applications. Applications of IoT can be categorized by: network type, scope, scale, heterogeneity, repeatability, and the involvement of users [12]. However, it remains a crucial challenge to protect the application data authentic and intact with authentication technologies while transmitting the data over IoT networks.

Studies depict that the authentication in IoT applications generally involves two validation aspects corresponding to different concerns [3]: a) peer authentication: *how does a IoT device recognize and trust its peers*; and b) data origin authentication: *how to ensure the origin of data is an authentic IoT peer*. These two validation aspects were proposed to enhance the security of machine-to-machine (M2M) communications [18] in IoT framework based on the complicated environment of IoT networks, which may comprise enormous cheap yet resource-constrained devices in contrast to traditional networks with a few hundred powerful nodes.

Several research attempts were made regarding the authentication of IoT applications. One of the earliest studies in this area was conducted by Liu et al. [16], in which they proposed an authentication and access control scheme based on Elliptic Curve Cryptography (ECC) combining both asymmetric and symmetric encryption methods. Registration Authorities (RA), a type of standalone authorization servers in IoT networks, are established to recognize the authenticity of both devices and users with predistributed certificates signed by the generated elliptic curve. Regular Elliptic Curve Diffie-Hellman (ECDH) key exchanging protocol is then performed between RA and users. This work also takes multiple domain authentication into consideration by adding a Home Registration Authority (HRA) and providing a Single Sign-On (SSO) solution for IoT users. Ndibanje et al. [20] presented a comprehensive analysis of security weaknesses in this method and proposed further improvements concerning the message exchanging performance and security assessment of the protocol.

In addition to ECC, other encryption techniques have been introduced to address the authentication issue in IoT applications as well. Attribute-Based Encryption (ABE) was adapted for the authentication of resource-constrained IoT devices by Yao et al. [31]. ABE is a cryptography method based on Identity-Based Encryption (IBE) aiming to produce encrypted texts recognizable by users with certain identities only. Extended from IBE, ABE identifies users with a set of predefined attributes. Only users with the specific combinations of attributes corresponding to the defined access policy are allowed to decrypt the cipher text, enabling broadcast encryption of the application data. However, the bilinear Diffie-Hellman scheme used by ABE is slow and computationally-intensive, which is proven unsuitable for IoT devices. Yao et al. replace bilinear Diffie-Hellman scheme of general ABE with faster elliptic curve scheme, leading to better performance and improved bit security. However, the proposed method still exhibits several inherent limitations as discussed in the paper: a) poor flexibility in revoking attributes; b) poor scalability with communication and computational overhead; and c) poor generality with multiple-authority applications.

The perception layer emerges from the evolution of IoT technologies as a substantial number of sensors are being deployed in IoT networks. Despite the significant importance of perception layers, only a few studies focus on the authentication issue of these layers. Ye et al. [32] presented an efficient authentication and access control scheme between users and the perception layer in Wireless Sensor Networks (WSN) by exploiting ECC key exchanging protocol with a mutual authentication style comprising two phases, namely, authentication and key establishment. A lightweight authentication protocol specifically designed for securing RFID tags was also proposed [2] in the literature. Nonetheless, such authentication issues, for example, how to segregate and protect sensitive application data in the heterogeneous perception layer of IoT networks, remain largely unsolved.

Neisse et al. [21] proposed SecKit, a model-based security toolkit, to address security policy management issues in IoT. By analyzing the characteristics of IoT framework comprehensively, authors designed the toolkit to support various application scenarios: a) dynamic context; b) trust management; c) digital divide; d) data flow control; e) actuator action control; and f) data anonymization. Moreover, authors formalized the security management procedure by identifying several metamodels involved in the process, including data, time, identity, role, context, structure, behavior, risk, trust, and rule. These metamodels were then implemented using the Eclipse Modeling Framework (EMF). Such formalization demonstrates the feasibility of the proposed toolkit and assists the administrators of IoT networks in creating, modifying, and enforcing security policies at a fine-grained level.

3 Architecture Authentication

There is no universally acceptable IoT architecture currently. However, great efforts have been made on the IoT architecture in different scenarios and application domains in terms of authentication and authorization.

3.1 Software-Defined Networking (SDN) Architecture

Software-defined networking (SDN) is an approach to computer networking, which allows network administrators to programmatically organize and manage network behavior dynamically via open interfaces and abstraction of lower-level functionality. Nowadays, thousands of new IoT applications and online services have been developped due to the exponential growth of devices connected to the network, whereas conventional network cannot provide enough flexibility to fit the trend. In this case, Valdivieso et al. [29] adopted the SDN architecture that helps eliminate the rigidity in traditional networks. In respect of security, the Pedigree system [23] is presented as an alternative to provide security in the traffic moving in an enterprise network. It is an OpenFlow-based system which allows the controller to analyze and approve the connections and traffic flows in the network. Pedigree do increase the tolerance to kinds of attacks, such as polymorphic worms, with relatively low load in the network traffic and the host. However, the lack of sophisticated authentication and authorization mechanisms makes SDN controllers still easily get attacked by hackers.

Black SDN Architecture for Smart Cities was presented by Chakrabarty et al. [6] in 2016. This architecture consists of four basic IoT architectural blocks for secure Smart Cities: Black Network, Trusted SDN Controller, Unified Registry and Key Management System. Black Network secures all data, including the meta-data, associated with each frame or packet in an IoT protocol [7], thus providing confidentiality, integrity and privacy in IoT networks. A Trusted SDN Controller can manage and orchestrate the flow between IoT nodes and the rest of the networking infrastructure, it mainly focus on secure routing of black packets. In the case that multiple wireless technologies (e.g. WiFi, LTE), multiple protocols (such as ZigBee, Bluetooth Low Energy) and multiple addressing schemes (e.g. IPv6 128-bit addressing, E.164) may be widely used in a Smart City environment, Unified Registry is presented for identity management, node authentication and many other critical secure problems. Furthermore, an independent hierarchical key management and distribution system for each layer of the communication protocol is also mentioned in [6].

3.2 Secure and Efficient Authentication and Authorization (SEA) Architecture

CodeBlue is one of the most popular healthcare research projects that has been developped by Malan et al. [17] Several medical sensors are places on patients' body in this approach. Out of security, Elliptic Curve Cryptography (ECC) [15] and TinySec [14] are alternative ways for key generation and symmetric encryption. Mossavi et al. [19] proposed a type of distributed smart e-health gateway architecture for IoT-based health-care systems. It bases on the DTLS handshake protocol, the basic IP security solytion for the IoT. In such a system, patient health-related information is recorded by body-worn or implanted sensors. In the area of IoT-based healthcare, the role of a gateway is extented to provide services such as temporary storage of sensors' and users' information. With traditional e-health gateway, a DoS attack on delegation server can disrupt all the available constrained domains as the functionality of the IoT-based healthcare still depends on the centralized delegation server. As an important improvement, Mossavi presents that the authentication and authorization task of a centralized delegation server can be broke down to be handled by distributed smart e-health gateways to defend DoS attack. But the techniques utilized in the proposed architecture do not support the privacy assurance re-used on constrained devices because of the security level requirements.

3.3 Service-Oriented Architecture (SOA)

Currently, IoT is expected to offer to users advanced connectivity of devices, systems, and services in a way that goes beyond machine-to-machine (M2M) communications, which furthers the integration of things not only to the Internet, but also to the web. Service-based applications built upon a large number of networked physical elements are presented in [11]. SOA-based techniques provide to IoT applications with an abstraction of services. As security is always a tough problem, Ramão et al. [26] present a security taxonomy for SOA-based IoT middleware based on different kinds of attacks. According to [26], authentication must be provided for both applications and devices, it includes features such as credentials and trust management, and guaranteeing the correct identity of the application or device. The main function of authentication is to prevent unauthorized access. Most SOA-based IoT middlewares including SIRENA, COSMOS, SOCRADES and HYDRA address authentication, which is typically provided by security token. Ramão et al. also provide a definition of standard security architecture, which consists of four security services: application and device authentication (ADA); authorization and access control (AAC); data confidentiality and integrity (DCI); and communication channel protection (CCP). The ADA service could be provided in all layers of the middleware, and take responsibility for enabling the authentication in the middleware core.

4 User Authentication

User authentication is usually used for checking whether the user asking for services is the legitimate one. According to Gorman et al. [22], there are three user authentication models that are widely used nowadays. In most kinds of authentication models, the user has to submit an authenticator to the intermediary or directly submit it to a machine. Many types of authenticators are commonly used, such as password, challenge questions, credentials and biometrics.

Turkanović et al. [28] presented a user authentication scheme for heterogeneous ad hoc wireless sensor networks based on the IoT. With gateway node (GWN) and traditional password, Turkanović provided a highly secure but lightweight authentication scheme, which is resilient to a variety of attacks such as replay attacks, privileged-insider attacks, DoS attacks and etc. Although the process of authentication is quite complicated enough as a defender, the traditional password authentication is not a good idea for the IoT based systems. Because a brief password is too weak to defend brute force attack, while a complicated password is too hard to memorize.

Biometric authenticators have been more and more popular in recent years. Footprint, eye, heartbeat and many other biometrics of human beings are developped for authentication among the industry based on diverse sensors. Mario et al. [10] presented a behaviroal biometric for continuous authentication based on touchscreen input. As a matter of fact, The entry-point authentication scheme used currently is not good enough with the lack of intruder detections after the authentication step. Besides, Smudge attacks can easily break conventional password and gesture password. Mario concluded that touchscreen input of people are sufficient to authenticate a user, and the continuous authentication can help with intruder detections even after entry-point authentication. However, this method is not widely put in use among the industry. The accuracy problem is urged to be improved through combining touch analytics with other modalities.

5 Conclusion

This survey briefly summarizes the evolving authentication technologies adopted in the Internet of Things framework in three aspects: application, architecture, and user authentication. The security of complex IoT networks will surely benefit from the implementation of an increasing number of authentication techniques. However, weaknesses were also observed in the prior authentication studies. Most of the state-of-the-art authentication techniques are limited to adapting existing cryptography methods or infrastructures from tranditional networks, rather than developing new techniques in the best interest of IoT networks. We are looking forward to seeing more novel and exciting ideas arised from the evolution of authentication techniques in the Internet of Things.

REFERENCES

[1] Auto-ID labs. https://autoidlabs.org/.

[2] F. Al-Turjman and M. Gunay. CAR approach for the Internet of Things. *Canadian Journal of Electrical and Computer Engineering*, 39(1):11–18, 2016.

[3] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. Internet of Things security: A survey. *J. Network and Computer Applications*, 88:10–28, 2017.

[4] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.

[5] A. Bassi and G. Horn. Internet of Things in 2020: A roadmap for the future. *European Commission: Information Society and Media*, 22:97–114, 2008.

[6] S. Chakrabarty and D. W. Engels. A secure IoT architecture for smart cities. In *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*, pages 812–813. IEEE, 2016.

[7] S. Chakrabarty, D. W. Engels, and S. Thathapudi. Black SDN for the Internet of Things. In *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*, pages 190–198. IEEE, 2015.

[8] N. Council. Six technologies with potential impacts on us interests out to 2025. *Disruptive Civil Technologies*, 2008.

[9] D. Culler and S. Chakrabarti. 6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture. *IPSO Alliance White Paper*, 2009.

[10] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans. Information Forensics and Security*, 8(1):136–148, 2013.

[11] D. Giusto, A. Iera, G. Morabito, and L. Atzori. *The Internet of Things: 20th Tyrrhenian workshop on digital communications*. Springer Science & Business Media, 2010.

[12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Comp. Syst.*, 29(7):1645–1660, 2013.

[13] E. K. Chiew et al. Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz version 1.0. 9. *On False Authentications for C1G2 Passive RFID Tags*, 65, 2004.

[14] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175. ACM, 2004.

[15] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[16] J. Liu, Y. Xiao, and C. L. P. Chen. Authentication and access control in the Internet of Things. In *32nd International Conference on Distributed Computing Systems Workshops (ICDCS Workshops)*, pages 588–592, 2012.

[17] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton. Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In *International workshop on wearable and implantable body sensor networks*, volume 5. Boston, MA;, 2004.

[18] F. Martín-Fernández, P. Caballero-Gil, and C. Caballero-Gil. Authentication based on non-interactive zero-knowledge proofs for the Internet of Things. *Sensors*, 16(1):75, 2016.

[19] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, 52:452–459, 2015.

[20] B. Ndibanje, H. Lee, and S. Lee. Security analysis and improvements of authentication and access control in the Internet of Things. *Sensors*, 14(8):14786–14805, 2014.

[21] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini. Seckit: A model-based security toolkit for the Internet of Things. *Computers & Security*, 54:60–76, 2015.

[22] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[23] A. Ramachandran, Y. Mundada, M. B. Tariq, and N. Feamster. Securing enterprise networks using traffic tainting. *Georgia Inst. Technol., Atlanta, GA, USA, Tech. Rep. GTCS-09-15*, 2009.

[24] K. Sakamura. Challenges in the age of ubiquitous computing: a case study of T-Engine, an open development platform for embedded systems. In *28th International Conference on Software Engineering (ICSE)*, pages 713–720, 2006.

[25] L. Tan and N. Wang. Future internet: The Internet of Things. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, volume 5, pages V5–376. IEEE, 2010.

[26] R. T. Tiburski, L. A. Amaral, E. De Matos, and F. Hessel. The importance of a standard security architecture for SOA-based IoT middleware. *IEEE Communications Magazine*, 53(12):20–26, 2015.

[27] I. Toma, E. Simperl, and G. Hench. A joint roadmap for semantic technologies and the Internet of Things. In *Proceedings of the Third STI Roadmapping Workshop*, volume 1, 2009.

[28] M. Turkanović, B. Brumen, and M. Hölbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, 20:96–112, 2014.

[29] Á. L. Valdivieso Caraguay, A. Benito Peral, L. I. Barona López, and L. J. García Villalba. SDN: Evolution and opportunities in the development IoT applications. *International Journal of Distributed Sensor Networks*, 10(5):735142, 2014.

[30] J. Vasseur and A. Dunkels. IP for smart objects. *IPSO Alliance, White paper*, 1, 2008.

[31] X. Yao, Z. Chen, and Y. Tian. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Comp. Syst.*, 49:104–112, 2015.

[32] N. Ye, Y. Zhu, R.-c. Wang, and Q.-m. Lin. An efficient authentication and access control scheme for perception layer of Internet of Things. *Applied Mathematics & Information Sciences*, 8:1617–1624, 2014.