Emerging Security Threats and Countermeasures in IoT

Zhi-Kai Zhang, Michael Cheng Yi Cho, Shiuhpyng Shieh, *IEEE Fellow*
Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan
{skyzhang.cs99g, michcho.cs98g}@g2.nctu.edu.tw, ssp@cs.nctu.edu.tw

ABSTRACT
IoT (Internet of Things) diversifies the future Internet, and has drawn much attention. As more and more gadgets (i.e. Things) connected to the Internet, the huge amount of data exchanged has reached an unprecedented level. As sensitive and private information exchanged between things, privacy becomes a major concern. Among many important issues, scalability, transparency, and reliability are considered as new challenges that differentiate IoT from the conventional Internet. In this paper, we enumerate the IoT communication scenarios and investigate the threats to the large-scale, unreliable, pervasive computing environment. To cope with these new challenges, the conventional security architecture will be revisited. In particular, various authentication schemes will be evaluated to ensure the confidentiality and integrity of the exchanged data.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Authentication.*

General Terms
Security

Keywords
IoT; Security; Privacy; Communication; Authentication

1. INTRODUCTION
Internet of Thing (IoT) is a self-configuring and adaptive complex network that interconnects uniquely identifiable "Things" to the Internet through the use of interoperable communication protocols. The "Things", sometimes referred to as devices or objects interchangeably, have sensing/actuation and potential programmability capability. Information about the "Thing" can be collected from anywhere, at anytime, by anything. IoT attracts much attention as the economic prosperity generated by the technology [1]. One of the economic opportunities is based on the data that the "Things" on the Internet shared. The shared data is processed into information as the input for other "Things" or as reports for human to read [2]. Given the data that has been shared over a network medium, namely the Internet, it is important to protect the shared data as it may contain sensitive and private information [3]. With the growth of the technology on Big Data, the threat is severer since the attacker may obtain private information through the raw data leaked by the compromised objects. Thus, privacy preservation becomes a critical issue to address.

Privacy preservation has been a critical issue for information security. Significant amount of work has been done in the research area. Authentication methods and cryptographic mechanisms were used to protect user privacy. A well-designed authentication method ensures authenticity so that only the authorized personal or object has the access to the private information. On the other hand, cryptographic mechanisms ensure that sensitive and private information is protected during transmission, storage and processing. Due to the heterogeneity, battery capacity, and resource constraints of the "Things" in IoT, not all the "Things" in IoT has the capability to engage the available authentication methods and/or cryptographic mechanisms. For this reason, privacy preservation in IoT security needs to be revisited. The recent research on IoT privacy preservation is either at high level or based on physical layer communication security [4][5]. In this paper, we will focus on IoT privacy preservation in the application layer. We will construct various application scenarios to identify privacy preservation challenges. This information can be useful for the development of IoT applications that falls into these scenarios.

IEEE IoT Initiative recently launched new standards project [6], which will define an architectural framework for the IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. Furthermore, IEEE IoT Initiative launched IoT ecosystem study to determine the connective areas and potential gaps in the concept of IoT that could be addressed through pre-standards and standards activities.

The main concern that differentiates IoT from the conventional Internet is scalability. In IoT, billions of objects are connected to the network. The conventional naming policy may not be able handle the devices on this massive scale. The naming policy may need to be improved or redesigned to provide unique naming convention. In response to the evolution of naming, identification and authentication methods also need to be redesigned accordingly. Transparency and reliability are two other key challenges that make the design of identification and authentication methods even more difficult.

Transparency is an important issue for IoT security. Most users cannot patiently finish complex configuration steps to activate their smart devices. All the configuration settings should be nearly transparent to the users. Authentication operations should be designed as simple as possible. Although X.509 PKI may be powerful enough, it is not practical to assume that a naive user has

ASIA CCS'15, April 14–17, 2015, Singapore.

http://dx.doi.org/10.1145/2714576.2737091

the ability to successfully obtain and import valid certificates to a large number of IoT devices. One of the reasonable assumptions, for example, can be that users can find a passcode printed on the label of the device or the home gateway. Then the naming, identification, and authentication settings can be automatically executed after the passcode is entered. To achieve this goal, new standards need to be established. The desired standards may not need to be totally novel. It can be a combination of existent standards in related domains, such as UPnP, DLNA, and DNSSEC.

Reliability is another important issue for the IoT ecosystem. Due to limited resources and battery capacity, IoT objects and communication between them are error-prone. The heterogeneity of objects makes the ecosystem more complex. The implementation and evaluation of the devices and services become more difficult. Additionally, when errors occur, debugging and repairing are also more difficult in the IoT ecosystem. Therefore, not only robustness, but also easy debugging and one-step resumption should be taken into consideration during the development of identification and authentication schemes. Moreover, under a reasonable assumption, automatic self-monitoring and healing mechanisms are also desirable for the reason that debugging and repairing are difficult for naive users.

Security threats to IoT can be generally divided into two categories. In the first category, the threats, similar to the conventional network ecosystem, are against confidentiality, integrity, and availability (CIA). However, due to the large scale and heterogeneity of the objects, the complexity and severity of the security threats is much more serious. The other category of treats arises from the new property of IoT ecosystem. With IoT objects everywhere taking sensitive readings from heartbeats to room temperature at home, it can be expected that the data in the IoT ecosystem is more personal and dynamic. Because the huge number of IoT devices gather massive sensitive information about users, the data readings about its owner and the personal spaces are treated as personal assets where a leakage may reveal owner's geological location, health status, and living habits. Attackers may extract desired information and disclose personal privacy.

In response to the security threats, security requirements for privacy protection and preservation need to be defined properly in IoT. For the first aforementioned category of threats, security requirements should cover the additional concerns dealing with the large scale and heterogeneity of objects. For example, object-to-object (O2O) communication is inevitable given that IoT objects collaborate to achieve goals without human intervention. Therefore, the security requirements aiming at authentication models for IoT users/objects are important. For the second category of threats, the security requirements should cover a set of new protection models. The models should be able to handle the information gathering and leakage for the IoT objects, especially for resource-constrained devices, which only provide limited security protection. Without the protection models, private data can be misused by rouge users/objects, malicious data can cause object to misbehave, or alternation of exchanged data to deceive users/objects by a rouge party.

Software and system vulnerabilities of an IoT device are also a critical issue which can lead to backdoor problems. With software vulnerabilities, attackers exercise malicious intents, and plant a backdoor in a vulnerable IoT device to control the device. Due to the resource constraints and battery capacity of IoT devices, security mechanisms such as intrusion detection systems and antivirus which consume a fair amount of computation power are not suitable. With primitive protection mechanism, injecting backdoors into an IoT device is relatively easy. Both static and dynamic analysis techniques have been used to verify a program. Static analysis has the limitation to uncover the vulnerabilities in the real execution environment, while dynamic analysis is inadaptable to IoT for the lack of the computing power and battery capacity. More detail discussion about IoT software security can be found in articles [3]. In this paper, we will focus on object identity management and authentication in the IoT ecosystem.

This paper is organized as follows. Section 2 introduces the challenges to object identification and authentication for IoT communication, while section 3 introduces personal IoT communication scenarios, and identify authentication requirements. Section 4 lists authentication models for the personal IoT communication scenarios. Lastly, a conclusion is given in section 5.

2. Naming, Identification and Authentication

Wearable gadgets and smart home/office appliances are the main themes of Consumer Electronic Show (CES) 2015 [7]. Wearable gadgets take measurement and report it to mobile APPs. These collected data are then passed on to smart furniture and/or appliance in smart home/office to make adjustment accordingly. This is a common IoT application demonstrated in CES 2015. The communication scenario of information exchange can be broken into two categories according to the distance range, that is, domestic and foreign. Typical domestic communication is done locally without access to the public network (a.k.a. the Internet). Foreign communication, on the other hand, relies on the public network to distribute data to distant objects.

Heterogeneity of objects is expected in IoT where objects have limited resources, computing power and communication capability. With the nature of lightweight and portability, the communication capability of wearable devices is mostly in a short distance. Short-range wireless communication (i.e. domestic communication), such as Bluetooth and Zigbee [8], relies on pairing objects prior to data exchange. For wearable devices to extend the communication range (i.e. foreign communication), a delegator is required to relay the data traffic. Delegator is normally referred to as the gateway of communication [9]. For wearable devices made for mobility, the handheld device such as mobile phone is a suitable gateway to relay data. On the other hand, for home/office appliances, a hotspot such as wireless AP (Access Point) is a suitable candidate to relay data. Figure 1 illustrates the typical topology configuration for both long distance and short distance communication.

For domestic communication authentication, e.g. Bluetooth and Zigbee, basic security is provided in the link layer during object pairing where password is required. Once the object is paired, encryption is applied when data has been exchanged wirelessly [8]. On the other hand, foreign communication authentication, section 4 will enumerate a number of applicable authentication models.

Since IoT comes at a massive scale of objects, naming of the objects becomes more complex. Due to the heterogeneity of the objects and the network, conventional Internet naming and identification will not be applicable [3]. Uniquely naming the objects is one of the main challenges in IoT to be resolved before addressing object authentication. GS1 [10] suggested that the DNS naming scheme can be the naming basis of IoT given that

IoT is to be deployed on the Internet. Object Naming Service (ONS) [10] is part of GS1 EPCglobal [11] architecture framework that leverages DNS to locate authoritative metadata and services with given Electronic Product Code (EPC). The EPC is designed for the purpose of providing universal unique identity. ONS can also be integrated into DNS as a sub-domain of DNS. Therefore, the Internet becomes the communication medium for the device-naming domains.

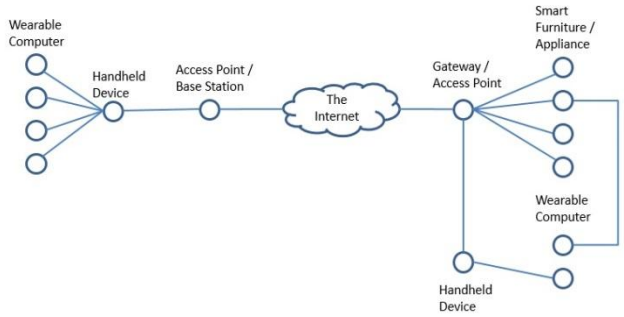

Figure 1. A typical IoT topology.

As an illustrator of the future Internet architecture, US NSF launched Future Internet Architecture Project (FIA Project) [12]. As a core sub-project of FIA Project, L. Zhang et al. proposed novel "Named Data Networking (NDN)" [13] which moves the network architecture from host-centric to data-centric. According to NDN, the identification and network routing are based on the name of the object instead of using conventional IP address. Naming in NDN is in a hierarchical structure, and is applicable to hierarchical nature of the current computer network structures. NDN has great impact, but is still in its infancy. There are still many new challenges, such as efficiency, name validation, signing key management, object authentication, and other security issues. These challenges remain unsolved and raise concerns.

3. IOT COMMUNICATION SCENARIOS

In this section, we will discuss various communication scenarios for IoT applications to exchange data. To model IoT communication scenarios, the administration domains of objects can be divided into *domestic* and *foreign domains*, based on the ownership of objects. An object of the *domestic domain* is administrated and owned by the home members while the object of a *foreign domain* is administrated and owned by outsiders. Each object is represented as a *peer*. A *domestic peer* represents an object that is registered to the domestic domain, while a *foreign peer* represents an object that is registered to a foreign domain. The communication of "things" can be formalized into three scenarios, namely, *basic scenario, extended scenario*, and *cloud scenario*. Details are given below.

3.1 Basic Communication Scenario

This basic communication scenario is regarded as domestic communication where wearable devices, smart furniture, and smart appliance exchange data within a closed network environment, such as home or organization (shown in Figure 2). For wearable devices that are incapable of making direct connection to an access point beyond the communication range, a delegator such as handheld device can play the role to relay data traffic to the access point so that the data can be transmitted to the destination. This communication scenario takes place in a closed network often referred as local area network (LAN), and the main challenges to data retrieval are as follows:

- Authentication and authorization to use the LAN
- Countermeasure for eavesdrop over wireless networks

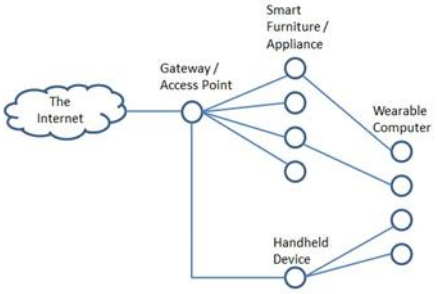

Figure 2, IoT communication in home/organization domain.

3.2 Extended Communication Scenario

Mobility is one of the features of wearable devices. Data must be exchangeable whilst a wearable device is on the move. Thus, public network (i.e. the Internet) is used to relay the exchanged data. Depending on the methods that data is exchanged and stored, network configurations can be divided into two types. Figure 3 depicts a simple network configuration for external resource access where resource and data distribution are decentralized. In this type of configuration, two gateways are employed to support communicate between the wearable devices and smart furniture/appliances. A gateway supports the local area network, while the mobile handheld device supports data relay for mobile wearable devices. As data exchanged, the two gateways handle data forwarding.

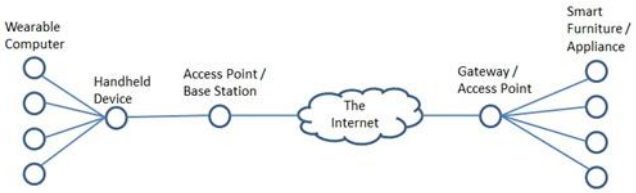

Figure 3, IoT communication over public network.

Figure 4 illustrates the network configuration where resource and data are centralized. Although the two network configurations are alike, the actual communication takes place using different approaches. In this approach, the data resource is centralized so that the objects do not communicate directly. All exchanged data is pushed and pulled from a central storage (i.e. the data pod). Regardless of centralized or decentralized network configurations, challenges to data retrieval are listed below:

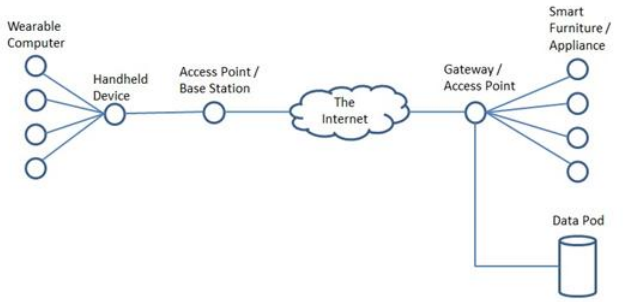

Figure 4, Centralized IoT communication over public network.

- Authentication and authorization to use the LAN
- Eavesdrop resistance over wireless networks
- Integrity assurance when using the public network
- Confidentiality assurance when using the public network

3.3 Cloud Communication Scenario

Cloud computing has been a hot topic in the recent years. Cloud computing will continue to thrive as IoT grows. The scenario involves vendors providing data storage service where data can be accessed from anywhere (shown in Figure 5). At the same time, data is replicated to prevent single point failure and ensure efficiency. The pushed data in the cloud service can also be computed for analytical purpose or for personal service recommendations. Unlike the aforementioned scenarios, the gateways of wearable devices, smart furniture, and smart appliances are only used to collect data for the cloud storage. In this context, data authentication is still needed to avoid pollution while transmitting collected data over the Internet to the cloud. The challenges to data collection is as follows:

- Authentication and authorization to use the LAN
- Eavesdrop resistance over wireless networks
- Confidentiality and integrity assurance over the Internet
- Authentication and authorization for the cloud service
- Confidentiality and integrity for the cloud storage

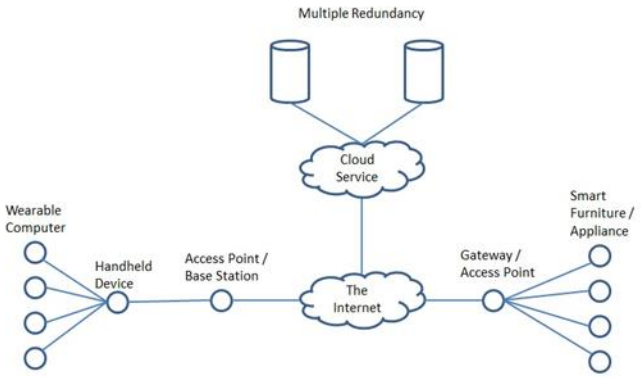

Figure 5, IoT with cloud computing.

4. AUTHENTICATION MODEL

In this section, authentication models are introduced to cope with the challenges incurred in various communication scenarios. Each authentication model is designed in an attempt to address the challenges in a communication scenario. These challenges are further elaborated as follows. For domestic communication, O2O (Object-to-Object) communication is applied to wearable devices and handheld devices. Due to resource constraints, wearable devices rely on more powerful computational objects, such as handheld device, to relay data. To authenticate, pairing mechanism is adopted when two objects are making connection. At the pairing stage, a simple password or pre-shared key is supplied before initializing the communication. When the data exchange begins, symmetric cryptosystems are suitable for preventing eavesdropping over wireless communication. For LAN communication, the conventional Wi-Fi protecting schemes are sufficient where a passphrase is used to authenticate the object to the network and prevent eavesdropping over wireless communication. These authentication schemes cover domestic communication while the following authentication schemes cover foreign communication where exchanged data is forwarded through the Internet.

4.1 Authentication by Gateway

In the authentication-by-gateway model, the authentication process relies on the gateway between the communication parties. To communicate with a domestic peer, a foreign peer first needs to be authenticated by the domestic gateway. Being authenticated, the subsequent exchanged data from the foreign peer is directed to the destination until the session is terminated. This authentication process is repeated for each communication session whenever the communication parties exchange data via the Internet. The authentication method can be as simple as ID-password scheme or any other scheme as long as it provides the proof of authorized identity. Similar to authentication-by-gateway model, research [14] has discussed a practical IoT communication example based on CoAP (Constrained Application Protocol) [15] that the resource-constrained objects cooperate with the gateway in UCN (Unconstrained Network) to achieve data authentication. The pros and cons of authentication-by-gateway scheme are listed below:

- Pros
  - The authentication method for foreign peers is independent of the authentication method for domestic peers.
  - Peer protection is centralized in the gateway. Since the gateway should be relatively powerful in terms of computation, the protection can be designed to be more complex to strengthen the security functionalities. On the other hand, the protection for the domestic peers can be designed to be lightweight. In this way, it is more applicable to the domestic peers that may have less computation power and requires less security functionalities.
- Cons
  - Single point failure, such as compromised gateway, exposes all the peers to threats.
  - The gateway can be a bottleneck since it is in charge of authenticating network traffic from communicating peers. At the same time, the gateway is also the only ingress and egress point of public network traffic. Thus, network traffic congestion problem is inevitable.

Applying this authentication model to the IoT communication model over public network, the gateway (i.e. the access points and the handheld devices) must be capable of authenticating foreign peers. An example of IoT applications is the IoT data collection and integration for e-health. In a health caring scenario, an elder may wear a smart bracelet continuously collecting his heartbeat and GPS location information. As the mobile gateway, a smart phone may be needed to collect raw data from the bracelet and upload them to a health care cloud. In this scenario, the smart phone may communicate with the bracelet through secure Bluetooth pairing and authenticate each other with the cloud through a DTLS [16] connection. This authentication model reduces data authentication workload on the communicating objects. Therefore, it is more suitable for resource-constrained objects such as the aforementioned bracelet. It is also applicable to centralized communication over public network. However, the downside of this authentication model is that the gateway is busy with processing authenticated sessions while forwarding network traffic to the public network. For standard home gateway such as home routers and access points, the high computing workload may be minor. However, it can be problematic to a gateway powered by battery.

4.2 Authentication by Security Token

In this authentication model, the gateway is responsible for initiating the authentication session when a foreign peer begins to exchange data with a domestic peer. At initiation, the gateway will establish a security token with the communicating parties. This security token may have a time-to-live or valid-period attribute to indicate security token validity by defining the time frame or the use count. For all sessions in the valid time period, the communicating peers exchange data using the security token for authentication purpose. Before the expiration of time-to-live or valid-period attribute, the gateway is free from succeeding authentication workload. Based on the concept of this category, the research [17] constructs a delegation-based authentication and authorization scheme for DTLS. The pros and cons of the authentication methods in this category are described as follows.

- Pros
  - The load for succeeding authentication after initialization is removed from the gateway.
  - It is suitable for resource-constrained peers where token-based authentication is considered to be lightweight in computation.
- Cons
  - Single point failure, such as compromised gateway, may expose peers to threats since the initial authentication session is performed by the gateway.
  - The design of a scheme using security tokens can be difficult because both security requirements and resource restriction of the peers must be taken into consideration simultaneously.

The authentication-by-security-token model relies on the domestic gateway to distribute a security token to the communicating peers. Upon receipt of the security token, the communicating peers use it to authenticate each other. This shifted the authentication workload to the communicating peers to alleviate the workload on the gateways. The valid period of a security token can be rather short if the communicating peers are resource-constrained objects which cannot afford strong security protection. Thus, this authentication model is still resource-constrained friendly. As a comparison to the previous authentication model, this model is also applicable to centralized communication over public network. The overhead for a gateway is to set up and manage the security tokens.

4.3 Authentication by Trust Chain

In this model, the trust relationship "peer A trusts peer B" is defined as follows. Peer A is convinced that the incoming data D is indeed from peer C, if peer B certifies that data D is from peer C. Therefore, a trust graph is constructed as a connected and directed graph in which the successor of a directed edge trusts the predecessor. The gateway is the predecessor of all the peers that are assigned to the domestic registration domain, and a public authority certifies the gateway. If two communication peers belonging to different trust graphs need to authenticate each other, one or multiple edges should be added to concatenate the two trust graphs in a proper manner. In this configuration, both peers can find particular predecessor which is trusted by itself and certifies the other peer. There are existent standards using a trust graph structure, such as X.509 PKI (IETF RFC 5280) and DNSSEC [18].

As an example, an authentication method based on X.509 PKI uses digital certificates for authentication. In the setup phase, the gateway must act as the concatenating point which requests a digital certificate from a public CA (Certificate Authority) and issues its own private, proprietary certificates to the domestic objects. For simplicity, the proprietary certificate does not need to follow the X.509 standard format; however, the communication peers must all agree on using the proprietary authentication method. After the setup phase, domestic peers can achieve mutual authentication with all the peers that trust the same proprietary CA. The pros and cons of the authentication-by-trust-chain model are listed below:

- Pros
  - After the setup phase, there will be no further authentication workload on the gateway. Thus, this authentication model reduces the workload for authentication.
  - This model is based on trust chain. In practice, authentication standards of this model are designed to provide better security functionalities compared to the basic authentication methods.
  - Instead of applying for a certificate for each domestic object, proprietary certificate authority is employed to reduce the cost of obtaining public certificates.
- Cons
  - This kind of authentication scheme is more complex, and may not be suitable for resource-constrained objects. A fair amount of computation power is required.
  - The authentication model uses similar methods for both domestic peers and foreign peers, which make it inflexible.
  - Single point of failure, such as a compromised gateway, may break the trust chain.

A prerequisite for this model is that a home/organization owner must have a certificate authority for all the objects, and this certificate authority must also obtained a digital certificate from an upper-tier to chain up the trust (i.e. trust graph concatenation). For traveling objects to phone home, no trust graph concatenation is required given that the digital certificate is issued by the domestic gateway. However, trust graph concatenation is required if an object is owned by an outsider. This will require communicating parties to acquire all the intermediate digital certificates to construct the chain of trust (i.e. trust graph concatenation). This authentication model shifts the authentication workload to the communicating objects. Therefore, it may not particularly suitable for certain resource-constrained objects.

4.4 Authentication by Global Trust Tree

Unlike the authentication-by-trust-chain model, a global trust tree is used instead. All the peers are registered in the global trust tree. As a result, all the peers can be authenticated globally. To our best knowledge, currently no global trust trees are available. DNSSEC can be a potential candidate to construct one [19]. However, some practical issues [20][21] will need to be resolved before moving forward. The pros and cons of this authentication model are as follows:

- Pros
  - Global trust graph is more reliable (in terms of management) comparing to the trust architecture using a private gateway.
  - The gateway does not intervene in authentication process, and thus can concentrate on network traffic forwarding tasks.
  - The underlying scheme is in general an international standard, which is more robust in achieving mutual authentication.
- Cons

- Global trust graph is not available in the current Internet framework.
- Constructing a global trust graph that includes all the objects in IoT is expensive and may be infeasible.
- Even if a global trust graph is available, the registration fee will be high as a whole for all the domestic objects.

In comparison with authentication-by-trust-chain, authentication-by-global-trust-tree can enforce strict rules to manage digital certificates. In this authentication model, the gateways of the communicating peers do not take part in authentication. Routing network traffic is their primary task. However, the communicating objects must be capable of performing data authentication, which may be problematic for some resource-constrained objects. Therefore, it is more appropriate in this authentication model to centralize data retrieval over the public network or cloud computing communication environment to reduce the amount of data exchanged.

5. CONCLUSION

In this paper, emerging security threats and countermeasures in IoT are investigated. In particular, challenges to sensitive and private information exchanged between travelling objects and objects at home/organization are evaluated. Naming, identity management, and authentication of IoT objects are the key issues for secure communication and data retrieval. Based on various communication scenarios in IoT, we enumerated a few potential authentication schemes that are applicable. Hopefully this attempt can motivate more future work to cope with security concerns in the deployment of IoT.

6. ACKNOWLEDGMENTS

This work is supported in part by Ministry of Science and Technology (MOST), Ministry of Education of Taiwan, Taiwan Information Security Center (TWISC), ITRI, III, iCAST, HTC, D-Link, Trend Micro Inc., Promise Inc., Chungshan Institute of Science and Technology, Bureau of Investigation, and Chunghwa Telecom, and Telecom Technology Center.

7. REFERENCES

[1] M. Ravindranath, (8 Jan 2014), *Cisco CEO at CES 2014: Internet of Things is a $19 trillion opportunity* [Online]. Available: http://www.washingtonpost.com/business/on-it/cisco-ceo-at-ces-2014-internet-of-things-is-a-19-trillion-opportunity/2014/01/08/8d456fba-789b-11e3-8963-b4b654bcc9b2_story.html.

[2] K. Aston, (22 Jun 2009), *That 'Internet of Things' Thing* [Online]. Available: http://www.rfidjournal.com/articles/view?4986.

[3] Z. K. Zhang, et al., "IoT Security: Ongoing Challenges and Research Opportunities," in *IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA 2014)*, Nov 2014, pp. 230-234.

[4] R. H. Weber, "Internet of Things – New Security and Privacy Challenges," in *Computer Law & Security Review*, vol. 26, issue 1, Jan 2010, pp. 23-30.

[5] C. M. Medaglia, and A. Serbanati, "An Overview of Privacy and Security Issues in the Internet of Things," in *the Internet of Things*, Jan 2010, pp. 389-395.

[6] R. Minerva, and A. Biru, "Towards a Definition of the Internet of Things," in *IEEE IoT Initiative White Paper*.

[7] R. Metz, (6 Jan 2015), *CES 2015: The Internet of Just About Everything* [Online]. Available: http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything.

[8] J. S. Lee, Y. W. Su, and C. C. Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *33rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2007)*, Nov 2007, pp. 46-51.

[9] H. Chen, X. Jiao, and H. Li, "A Brief Introduction to IoT Gateway," in *IET International Conference on Communication Technology and Application (ICCTA 2011)*, Oct 2011, pp. 610-613.

[10] GS1, "GS1 Object Name Service (ONS) Version 2.0.1," in *Ratified Standard 2*, 2013.

[11] GS1, (5 Aug 2014), *EPCglobal Standards* [Online]. Available: http://www.gs1.org/gsmp/kc/epcglobal.

[12] National Science Foundation, (21 Sep 2014), *NSF Future Internet Architectures Project* [Online]. Available: http://www.nets-fia.net.

[13] L. Zhang, et al., "Named Data Networking," in *ACM SIGCOMM Computer Communication Review*, July 2014.

[14] R. Bonetto , et al., "Secure Communication for Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples," in *IEEE Int. Symp. on World of Wireless, Mobile, and Multimedia Networks (WoWMoM 2012)*, Jun 2012, pp. 1-7.

[15] E. Rescorla, and N. Modadugu, "Datagram Transport Layer Security Version 1.2" in *IETF RFC6347*, Jan 2012.

[16] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol," in *IETF RFC7252*, Jun 2014.

[17] R. Hummen, et al., "Delegation-based authentication and authorization for the IP-based Internet of Things," in *11th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON 2014)*, Jun 2014, pp.284-292.

[18] R. Arends, et al., "DNS Security Introduction and Requirements," in *IETF RFC4033*, Mar 2005.

[19] M. C. Y. Cho, P. Chen, and S. Shieh, "Dmail: a Globally Authenticated Email Service," in *IEEE Computer*, vol. 47, issue 5, May 2014, pp. 88-91.

[20] R. H. Weber, and R. Weber, "Security and Privacy" in *Internet of Things Legal Perspectives*. Springer, 2010, pp. 41-67.

[21] S. Evdokimov, B. Fabian, and O. Günther, "Multipolarity for the Object Naming Service," in *The Internet of Things Lecture Notes in Computer Science*, Vol. 4952, 2008, pp. 1-18.