International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 11|| November 2017 || PP. 45-52

Internet of Things: Security Issues

A Haritha[1], A Lavanya[2]
[1](Assistant Professor, ECE Department, TKRCET, Hyderabad)
[2](Assistant Professor, ECE Department, TKRCET, Hyderabad)

Abstract: *The Internet of Things (IoT) is becoming a key infrastructure for the development of smart ecosystems. However, the increased deployment of IoT devices with poor security has already rendered them increasingly vulnerable to cyber attacks. In some cases, they can be used as a tool for committing serious crimes. Although some researchers have already explored such issues in the IoT domain and provided solutions for them, there remains the need for a thorough analysis of the challenges, solutions, and open problems in this domain. In this paper, we consider this research gap and provide a systematic analysis of security issues of IoT-based systems. Then, we discuss certain existing research projects to resolve the security issues. Finally, we highlight a set of open problems and provide a detailed description for each. We posit that our systematic approach for understanding the nature and challenges in IoT security will motivate researchers to addressing and solving these problems.*

Keywords: *Internet of Things; Security Issue; Attack Surface; Attack Taxonomy; IoT Forensics.*

I. Introduction

The Internet of Things (IoT) [1] represents a global infor- mation network of our everyday devices, such as appliances and automotive, and provides an intelligent framework with the properties of sensing capabilities, contextual awareness, and device autonomy. The connectivity among these devices enables them to communicate smartly to each other or to us. Every year, about one million new IoT devices are expected to be deployed to different application domains around the globe [2]. However, the more devices that get connected through the IoT, the greater becomes the possibility of digital mischief or mayhem.

Why is IoT security different? IoT devices and networks are inherently resource constraints. The major constraints for applying conventional security solutions to IoT-based systems are as follows [3, 4]:

a) IoT devices often use low speed CPUs and, often, devices are battery driven. Contemporary cryptographic algorithms require fast computation, so cannot be ported directly to these devices.

b) IoT devices usually are memory-constrained compared to phones and laptops. Conventional security schemes are not designed for memory-constrained devices.

c) IoT devices often use low data-rate radio interfaces for communications. Traditional security schemes cannot be applied to IoT-based systems directly because of low bandwidth communication media.

d) The installation of security patches on IoT devices might be infeasible, since lightweight IoT operating systems might lack modules to receive and integrate new codes or libraries (safely or at all).

e) Mobile IoT devices might join a network without prior configuration or might leave the network abruptly. These types of sudden change in network topologies affect the performance of existing security schemes. As a result, these schemes cannot be applied to the IoT environment as is.

f) An IoT milieu comprises different types of devices ranging from PCs to RFID tags and a wide range of wireless protocols, such as WiFi, Zigbee, and Z-Wave. Among the current security solutions, it is hard to find a solution that accommodates a heterogeneous mix of diverse devices.

In light of the above issues, particularly the resource- constrained properties of IoT devices, we argue that insecure deployments of IoT-based systems present a significant threat to the success of this emerging paradigm. Therefore, we must examine and understand key security issues in the IoT domain carefully, and include such considerations into the design of IoT devices, systems, and protocols. In this paper, we take the first step towards motivating and educating researchers about the security implications of the Internet of Things. Organization: The rest of the paper is organized as follows: We present a detailed discussion of attacks on IoT-based systems in Section II. We present the requirements for security schemes in Section III. An analysis of current security solutions is presented in Section IV. Section V enumerates open research problems in the IoT. Finally, we conclude in Section VI.

II. Attack Taxonomy

The attack surface increases manifold in the IoT environment because of the heterogeneity of devices, communication media, application, and services. We present different types of attacks that can occur in the IoT environment (Figure 1). Each attack is assigned a severity: high, medium, or low.

A. Classification of Attack Severities

High severity attacks: These types of attacks can compromise an entire IoT-based system. An attacker can access the entire IoT network and system without authentication. Such attacks could result in a complete loss of confidentiality and integrity of data, and availability of IoT services.

Medium severity attacks: These types of attacks result in a partial compromise of an affected IoT-based system. Such attacks have a high impact on the system but accessibility to attackers is limited (*i.e.,* an attacker might elevated privileges but does not gain complete control of the entire system).

Low severity attacks: These types of attacks constitute minor threats. In almost all cases, a successful attack does not affect the availability of IoT services broadly.

B. Attacks Based on Device Property

Low-end device class attack: The attacker and the victim both are IoT devices and have similar configurations and capabilities, such as similar memory size and CPU speed. For instance, a smart watch containing malware gets unauthorized access to a smart TV and then sends spam emails from the smart TV. High-end device class attack: The attacking device is more powerful than the victim device. An attacker uses full-fledged devices, such as a PC or laptop, or virtual machine instance to gain access to the IoT network and smart devices, and then undertakes malicious activities.

C. Attacks Based on Adversary Location

Internal attack: The adversary and the victim device are located within the same network. The adversary is authorized to access IoT resources. However, the adversary compromises a legitimate device to launch attacks. For example, this might be a malicious guest user after joining the home network who compromises the thermostat to turn off the home security system by exploiting one smart device after another through their trust relationship.

External attack: The adversary and the victim device reside in different networks. The adversary can be deployed anywhere. For example, an adversary exploits the vulnerabilities of the authorization system, gains access to home networks remotely then launches attacks on smart devices.

D. Attacks Based on Attack Strategy

Physical attacks: Such attacks cause physical damage: changes in device properties and configurations. For example, adver- saries tamper with a device by injecting malicious code. Logical attacks: These attacks do not cause any physical damage to an IoT device, but push devices into a state where devices start malfunctioning (*i.e.,* a victim device stops sending realtime data). Active and passive attacks can be combined to form logical attacks.

E. Attacks Based on Access Level

Active attacks: An adversary disrupts the normal functionality of IoT devices and networks. Different types of DoS attacks, such as resource exhaustion and jamming, are considered to be active attacks.

Passive attacks: The adversary is an authorized IoT device, but performs illegal activities to gather information from the trusted entities through monitoring and traffic analysis of the communication channel; however the communication is not disrupted. This type of attacks threaten privacy of the IoT.

F. Attacks Based on Information Damage Level

Interruption: Interruption attacks work against the availability of IoT services. This type of attack degrades service quality or makes services unavailable for legitimate consumers. Eavesdropping: The attacker gains unauthorized access to a communication channel and listens to the messages carried through the private connection. This type of attack is an attack against the confidentiality of the information.

Modification: This is an attempt to alter information (change/insert/delete) that an adversary is not authorized to do. This type of attack creates confusion and misleads communicating peers in a network. Modification attacks threaten the integrity of the information.

Fabrication: An adversary inserts counterfeit information or activities, into the message which creates confusion among the peers involved in a communication. This type of attacks threaten the originality of the message.

Message replay: An adversary stores messages without authorization. Later, he/she retransmits the stored message to trick communicating peer into unauthorized operations such as false identification or authorization, or a duplicate transaction. Protocols that are not time-ware are susceptible to message- replay attacks. This type of attack threatens message freshness.

G. Host Based Attacks

User compromise: Users are tricked into revealing their personal information (*e.g.*, their name or date of the birth) or security credentials (*e.g.*, keys, passwords) through unsporting maneuver. Insecure transfer of credentials, such as unencrypted message transfer and weak cryptographic scheme, leads to user-compromise attack.

Software compromise: An adversary exploits the vulnerabilities of the software running on the IoT devices. For example, a malicious device put a victim device in exhaustion state by sending continuous connection requests. This could happen if the victim device is not configured to block a device after receiving a certain number of requests from that device within a short time span.

Hardware compromise: Sensitive information, such as data,keys, and program codes are stored within an IoT device. An adversary extracts these embedded credentials by tampering with the hardware, which requires physical device access. The adversary performs malicious activities including micro-probing and reverse engineering of a particular device.

III. Security Requirements

There are several properties that need to be considered while devising security solutions for IoT-based systems. The requirements are described below.

A. Information security requirements

Integrity: The integrity of an IoT system can be compromised simply by modifying the in-transit or stored data. Integrity enables one to verify that any received data has not been altered.

Information protection: Privacy and confidentiality of the stored and online data should be protected. This is achieved by limiting information access and disclosure to trusted parties, as well as preventing access by or disclosure to malicious ones. For example, an IoT network should not reveal sensor readings to its neighbors (if it is configured not to do so).

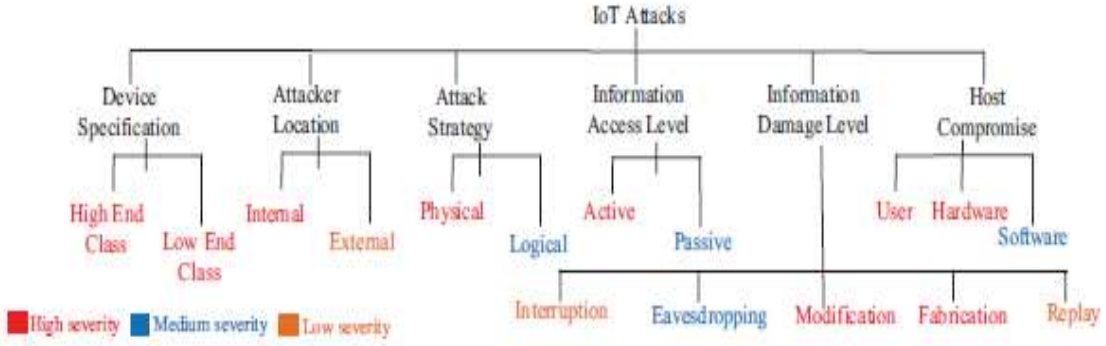

Fig 1: Taxonomy of attacks

Anonymity: This hides the source of the data and helps with data confidentiality and privacy. For example, the identity of a smart car should not be revealed while it delivers information about road conditions or traffic status to a service provider.

Non-repudiation: Non-repudiation is the assurance that some- one cannot deny something legitimate. For example, an IoT device cannot deny sending a message it has previously sent. Freshness: Message freshness is an important security property of IoT-based systems, since most those deal with real-time information. Thus, freshness guarantees that the data is recent and that no old messages have been replayed. For example, it must be ensured that a medical IoT device sends the most recent patient conditions to a physician.

B. Access level security requirements

Authentication: Authentication enables communicating peers to verify their identities. For example, a receiver executes an authentication process to verify that the received data has been originated from the correct source. Authentication also ensures that valid users gain appropriate access to IoT devices and networks. For example, users need to be authenticated to get access to IoT network and/or devices for administrative tasks such as remote reprogramming or controlling of IoT devices and networks.

Access control: This ensures secure and protected access to IoT networks, devices, services, and resources. It is possible that an authenticated user might be unauthorized to access to certain services or resources. To achieve this property, an access control mechanism (ACM) needs to be implemented. ACM ensures that authenticated users or devices access only what it is authorized to, and nothing else. For example, a guest user might be allowed to join a smart home network and to control its thermostat, but might not be authorized to control the home security system.

C. Functional security requirements

Interoperability: The deployment of security solutions should not interrupt the functional operation of heterogeneous things. Scalability: A large number of smart device are connected through IoT information network, and more devices are getting connected to the network everyday. Therefore, the proposed security scheme should provide sufficient scalability. One criteria of this property could be that the amount of information that each device requires to store in memory to establish a secure channel with its communicating parties.

Memory efficiency: IoT devices have limited memory andstorage. Security algorithms need to be optimized so that they consume minimal space in RAM during execution and do not take too much space to store cryptographic artifacts.

Minimal communication and computation overhead: Smart devices' most energy-consuming operations are communication and computation. Therefore, security schemes should be designed such that communicating peers do not require the exchange of too many messages. In addition, execution of the algorithms should not consume too many CPU cycles. Resiliency: Security systems should avoid single points of failure so that a compromised entity would not affect the whole system. For example, in case a few IoT devices of a collaborative security scheme should be compromised, the scheme should still protect against attacks. The remaining collaborating devices should be reorganized to maintain a set level of security.

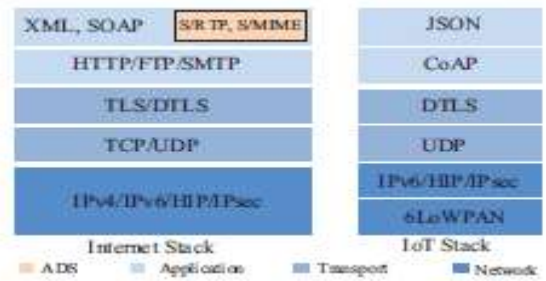

Fig 2: Comparison between Web stack and IoT stack [5]. ADS= Application data security

IV. Analysis And Comparision Of Security Schemes

Research and standardization approaches toward IoT security follow IP-based architecture and provide solutions by intro- ducing additional layers on one (or more) of the layers in the protocol stack (Figure 2). Here, we survey the state-of-the-art security schemes.

A. End to End Network Security

Host Identity Protocol (HIP)-based Schemes: HIP can be suitable for IoT devices' authentication by considering by devices' mobility properties. However, HIP Base Exchange (HIP-BEX) [6] involves intensive cryptographic computations, such as modular exponentiations of Diffie-Hellman (DH) public key generation and key exchange. HIP-DEX [7] avoids modular exponentiations and uses Elliptic Curve Diffie-Hellman (ECDH) key exchange. The authors in [8, 9] proposed to delegate cryptographic computations of the key exchange to rich resource proxies in collaborative schemes. However, both of the scheme increase communication cost and secret key setup time and are susceptible to DoS attacks. Slimfit [10] reduces communication cost by introducing a compression layer in the protocol stack below the HIP layer. Garcia-Morchon et al. [11] proposed a pre-shared-key-based HIP (HIP-PSK) for authentication; however, in general, PSK-based scheme do not provide a good degree of security. Lightweight HIP (LHIP) [12] does not implement any security mechanisms, such as authentication and encryption; it is used by HIP-BEX for simplicity, but is therefore unsuitable for IoT-based systems. Analysis and comparison: We present an analysis and comparison of HIP-based schemes in Table I. Our analysis finds that HIP collaborative schemes [8, 9] could be suitable for the IoT environment, since they are resource efficient with respect to computation and memory requirements. However, collaborative schemes increase traffic in the IoT network; hence, they lack communication efficiency. The analysis also shows that HIP-DEX [7] could be employed in

IoT devices with lower requirement for computation. HIP-PSK [11] and Slimfit [10] could be promising for the IoT environment considering their memory, computation, and communication efficiency. However, HIP-PSK and Slimfit do not provide good scalability and interoperability. In HIP-PSK, the distribution of shared secret keys is a complex task for an IoT system with a large number of smart devices. Similarly, HIP-PSK cannot guarantee that all the IoT nodes are embedded with the Simfit layer. Finally, although the LHIP [12] scheme shows resource efficiency, LHIP does not address the most important security properties, namely authentication and confidentiality.

B. End to End Transport Security

The Constrained application protocol (CoAP) [13], a new proposed standard for the IoT, runs over UDP and implements the Datagram Transport Layer Security (DTLS) to achieve end to end security. Here, we present a survey on DTLS schemes. DTLS schemes: Kothmayr et al. [14] proposed an X.509- certificate-based DTLS scheme for mutual authentication for constrained devices. Gusmeroli et al. [15] designed a two- phase authentication scheme that enables communicating peers to authenticate mutually using implicit certificates. However, both the proposed schemes do not consider scenarios in which an IoT device needs to process a certificate chain and to a check revocation list. To solve these problems, the authors in [16–18] proposed to delegate the certificate verification process to a Delegation Server (DS), a rich resource entity installed in the home network. The proposed system reduces the communication overhead of the DTLS handshake at the condition that the DS is trusted. Therefore, compromising the DS is enough to compromise an IoT-based system. Reza et al. [19] used a 6LoWPAN header-compression technique to reduce the size of the DTLS headers [20]. The proposed scheme avoids packet fragmentation; therefore, it reduces packet loss, packet processing time, retransmission rate, and energy consumption. However, the proposed solution does not provide support for backward compatibility with the standard DTLS protocol, particularly with respect to header compression.

Analysis and comparison: Table II shows the analysis and comparison of the proposed DTLS-based schemes. The delegation-based DTLS schemes [16–18] could be suitable for the IoT environment since they have low communication, computation, and memory overhead. However, delegation-based schemes are vulnerable to single points of failure and DoS attacks, and do not scale well –with the increased deployment of smart devices the delegation server needs to handle a large number of requests. In contrast, certificate-based DTLS schemes [14] are good for interoperability, resilience, and scalability, but these schemes are not resource efficient—they suffer from considerable computation, communication, and memory overhead.

C. Access Control Mechanisms

The widespread mechanisms for restricting access to autho- rized users are as follows: Role-based Access Control (RBAC) [21] and Capability-based Access Control (CapBAC) [16, 22–28]. However, RBACs are widely used for human-to-things communication, but they are not suitable for things-to-things communication. However, CapBAC are suitable both for the human-to-things and things-to-things communications.

CapBAC maps access rights, such as read and write privilege, to a service consumer's capability token, which is cryptographi- cally protected; therefore, cannot be forged. IoT access control architecture can be divided into two categories: centralized approach and distributed approach. In the centralized approach, all the access control logics are externalized into a central entity located in Cloud. In the distributed approach, the access control logics are embedded into the IoT devices.

Analysis and comparison: Table III presents an analysis and comparison of the proposed authorization frameworks. Accord- ing to the analysis, authorization mechanisms that follow a centralized approach reduce computation overhead, show good interoperability, and enable easy management of access control policies. Centralized approaches allow constrained devices to offload expensive operations, such as policy evaluation, token status verification (signature and ticket validity checking), to external entities or proxies; thus, reduce computation overhead. Such approaches are also memory efficient, since contained devices do not store access policies, access control lists, and issuers secret credentials, such as keys or certificates. However, centralized approaches introduce communication overhead because of to the additional communications with an external entity—a smart device sends the access token to the external entity and receives authorization decision. Such communications also increase the response time of a request, which is not desired for time-sensitive scenarios.

On the other hand, distributed approaches are suitable for such real-time IoT systems and applications, since devices perform policy operations and make authorization decisions. Distributed approaches demonstrate good scalability but lack interoperability since management is complex. Distributed

approaches also do not show good performance in terms of memory efficiency because policies, secret context, and the decision algorithm are stored in device storage.

Scheme	Key Exchange	Collaborative	Interoperability	Resilience	Scalability	Communication	Memory	Computation
HIP-DEX [7]	ECDH	n	●	●	●	◐	◐	Max
Slimfit [10]	ECDH	n	○	●	○	●	◐	↑
HIP-PSK [11]	PSK-based	n	○	○	○	○	○	↑
D-HIP [8]	DH	y	◐	◐	◐	○	◐	↑
HIP-TEX [9]	PKC-based	y	◐	◐	◐	○	◐	↑
LHIP [12]	n/a	n	●	●	●	●	●	Min

Table I: Analysis and comparison of HIP-based schemes. Communication complexity is measured in terms of the number of messagesexchanged until a shared secret is negotiated. Memory refers to spaces required for keying materials. Each security property can be assigned with three different values: (good performance level), (medium performance level), and (low performance level). Thevalue indicates the level of a specific scheme to support a property. The (n/a) notation means not applicable, and 'n'= no, 'y'= yes.

Scheme	Int	Res	Scal	Comm	Comp	Mem
Certificate [14, 15]	●	●	●	○	○	○
DTLS-PSK [11]	◐	○	○	●	●	◐
Modified [19]	○	●	●	●	◐	◐
Delegation [16–18]	●	○	○	●	●	◐

Table II: Analysis and comparison of DTLS-based schemes. Int = Interoperability, Res = Resilience, Scal= Scalability, Comm= Communication, Comp = Computation, Mem = Memory.

V. Research Directions

We examined current security schemes in the IoT domain and found that most of the research work was tailored to conventional security solutions to make them compatible with IoT-based systems. Current research work mainly addresses information and access-level security properties of IoT-based systems. However, resource efficiency and functional robustness of the security schemes have been considered low priority. Additionally, few of the schemes considered the privacy issues in IoT-based systems. Furthermore, there still exist several security issues that are poorly addressed, or might have gone unnoticed since technologies, such as Machine-to-Machine, RFID, and ubiquitous computing, are yet to be integrated completely into the IoT paradigm. Here, we present some of these critical security problems and provide paths forward for each of them.

Data transparency: IoT service providers can share user data with third party providers in order to collaborate. For example, the manufacturer of a smart home device could outsource the collected data to a third party who analyzes data to understand the context of the smart home. However, security schemes are required to ensure that the privacy of a user has not been compromised or breached during the data collection, sharing, and collaboration phase. These security properties can be achieved by the level of data transparency implementation in the system.

Application data security: Security at the application level (*i.e.*, employing security within the application payload) can provide complete end-to-end security. This approach simplifies the security requirements for underlying layers since only application data have to be secured – per-packet security overhead is eliminated from the underlying layers. Application data security also reduces the cost, in terms of packet size and data processing, at underlying layers. Moreover, by encrypting data at the application level, data passing between producers and consumers could be handled and processed at the gateway without being exposed to the gateway.

Secure handling IoT big data: Billions of IoT devices will generate massive quantities of data. The types of data and formats thereof could vary from application to application and from device to device. These data will be stored in the cloud and later be analyzed to provide suggestions to users and/or to issue automated commands to IoT device(s). When the data is huge, it is challenging to achieve secure transfer, maintenance, and synchronization of data without comprising any system aspect. Providing such security for handling such data requires significant attention and effort.d constrained networks, since these protocols are designed specially for rich-resource entities, such as PCs, Laptops, etc.

Privacy-aware identity usage: A smart device should knowwhen to reveal its identity, since providing identity to an adversary could be a serious threat, such as location tracking. Therefore, a requirement is to have a system that provides a device's identity to other qualified devices that can authenticate the device without exposing its identity.

Trust management: The dynamic expansion property of theIoT network and the level of interoperability in the network can cause an IoT device to decide which other entities in the network (or outside the network) are trustworthy. Such decisions can be made only if the IoT device is able to distinguish a trustworthy node.

Group membership: Three types of group communicationstake place in an IoT network: Thing-to-Things (T2Ts), Things- to-Thing (Ts2T), and Things-to-Things (Ts2Ts). Each group is assigned with some members, and each member of a group will need specific certification. This certification can be in the form of any shared credentials. Managing and maintaining group memberships can lead to some complexity and further issues that need to be addressed. Furthermore, applying the same concepts that are applied to individual devices to these groups will be challenging.

Embedded security: Embedded security schemes (ESS)should protect on-chip storage and application debugging interfaces. Additionally, ESS should enable software installed on smart devices to be updated to the latest version. However, security updates cannot be pushed to the devices directly, since most of the devices are not connected directly to the Internet. Instead, this requires a gateway or coordinator to get access these devices. Furthermore, similar types of devices require to be updated contemporaneously to maintain interoperability. IoT network security: End-to-end communications are secured with encryption and authentication. However, communications are exposed to various network attacks (*e.g.*, wireless attacks) from inside the network and from the Internet as well. Intrusion Detection Systems (IDSs) capture network packets and analyze the packets to detect network anomalies. More safety can be ensured by applying more control and monitoring of the IoT network. Therefore, research can be done to design IDSs with an optimal level of security control, which is sufficient to detect intrusions without compromising users' privacy.

IoT forensics: Traditional tools and technologies of digital forensics are not designed to handle the IoT infrastructure fully. Billions of IoT devices will generate massive data. When the amount of possible evidence is large, it is difficult to identify the important pieces of evidence that can be used to determine the facts about a criminal incident. Furthermore, the task to maintain secure provenance of the evidence is also challenging.

VI. Conclusion

With the increasing deployment of IoT-enabled systems, there is a growing emphasis on the need for strong security for smart devices, applications, and services. Here, we examined limitations of smart devices that prevent conventional security solutions to be applied directly to such IoT-based systems. We performed a detailed analysis of current solutions and identified issues in these that deserve further research. We mentioned numerous open problems that are poorly addressed, or have gone unnoticed thus far (cf, Section V), and suggested potential solution paths for each. Solving these problems will allow further application domains to take advantages of the IoT paradigm with sufficient security.

References

[1] L. ATZORI, A. IERA, AND G. MORABITO, "THE INTERNET OF THINGS: A SURVEY,"*COMPUTER NETWORKS*, 2010.

[2] www.gartner.com, "The internet of things will transform the data center,"2014.

[3] O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen,"Security considerations in the IP-based IoT," *RFC*, 2013

[4] B. Sarikaya, Y. Ohba, R. Moskowitz, Z. Cao, and R. Cragie, "Security bootstrapping solution for resource-constrained devices," *RFC*, 2012.

[5] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet*.John Wiley & Sons, 2011.

[6] R. Moskowitz, T. Heer, P. Jokela, and T. Henderson, "Host identity protocol version 2 (HIPv2)," RFC, IETF, 2015.

[7] R. Hummen and R. Moskowitz, "HIP DEX)," RFC, IETF, 2013.

[8] Y. B. Saied and A. Olivereau, "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things," in *WoWMoM*. IEEE, 2012.

[9] Y. Ben Saied and A. Olivereau, "TEX: A distributed key exchange scheme for HIP-based Internet of Things," in *ICCN*. IEEE, 2012.

[10] R. Hummen, J. Hiller, M. Henze, and K. Wehrle, "SlimfitA HIP DEXcompression layer for the IP-based IoT," in *ICNC*. IEEE, 2013.

[11] O. Garcia-Morchon, S. L. Keoh, S. Kumar, P. Moreno-Sanchez, F. Vidal- Meca, and J. H. Ziegeldorf, "Securing the IP-based internet of things with HIP and DTLS," in *WiSec*. ACM, 2013.

[12] T. Heer, "Lightweight authentication extension for HIP," RFC, 2007. [13] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," *RFC, IETF*, 2014.

[13] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *LCN*. IEEE, 2012.

[14] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two- phase authentication protocol for wireless sensor networks in distributed iot applications," in *WCNC*, 2014.

[15] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation- based authentication and authorization for the IP-based Internet of Things," in *SECON*. IEEE, 2014.

[16] J. Park and N. Kang, "Lightweight secure communication for CoAP- enabled IoT using delegated DTLS handshake," in *ICTC*. IEEE, 2014.

[17] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the Internet of Things," in *HotWiSec*. ACM, 2013.
[18] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure coap for the iot," *Sensors Journal, IEEE*, 2013.
[19] J. Hui and P. Thubert, "Compression format for ipv6 datagrams over ieee 802.15. 4-based networks," *IETF, RFC*, 2011.
[20] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," *TISSEC*, 2001.
[21] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Mathe- matical and Computer Modelling*, 2013.
[22] J. L. Herná ndez-Ramos, A. J. Jara, L. Marın, and A. F. Skarmeta, "Distributed capability-based access control for the Internet of Things," *Journal of Internet Services and Information Security*, 2013.
[23] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the Internet of Things," *Journal of Cyber Security and Mobility*, 2013.
[24] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the Internet-of-Things," in *WoWMoM*. IEEE, 2013.
[25] P. P. Pereira, J. Eliasson, and J. Delsing, "An authentication and access control framework for CoAP-based IoT," in *IECON*. IEEE, 2014.
[26] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios," *Journal of Sensors*, 2015.
[27] S. Gerdes, O. Bergmann, and C. Bormann, "Delegated CoAP authenti- cation and authorization framework (DCAF)," ETF Internet Draft, 2014.
[28] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability- based access control delegation model on the federated IoT network," in *WPMC*. IEEE, 2012