Internet of Things (IoT), Three-Layer Architecture, Security Issues and Counter Measures

Bonani Paul

Abstract Internet of Things (IoT) a tired framework necessitates the use of diverse technologies, for capturing, processing, analyzing, and storing large unprocessed data in cloud-based data centers for the IoTs to function as desired. The security and privacy are some of the critical concerns with increased communication among billons of IoT-connected devices. In this article, an overview of three-layered IoT architecture is provided, and the vulnerabilities and threats in all the three layers have been discussed. It also discusses the security practices that can be enforced in each layer due to limiting functionalities of current hardware technology. The article also explores some of the countermeasures and protection methods such as authentication, authorization, lightweight symmetric, and asymmetric algorithms that can be implemented against various attacks on all the three layers.

Keywords IoT architecture · Security issues and challenges · RFID · Blockchain

1 Introduction

The Internet of Things (IoT) can be defined as an integration of interconnected smart objects with embedded sensors, actuators, and processors for the purpose of exchanging data over the internet to accomplish intended objective. IoT is a seamless integration of virtual and real-world technologies working together in tandem. With more consumers and business enterprises embracing IoT technologies and solutions in real-time, more are the security concerns.

Secure communication, secure storage, and effective access control mechanism, are becoming the most pressing concerns associated with widespread application of IoT [1]. Since sensor networks are extremely vulnerable to attacks [2], it is critical to have a mechanism in place to safeguard the network, smart things, and users from all types of malicious attack, thereby creating a more robust environment. The

B. Paul (✉)
Department of Computer Science, St. Mary's College, Shillong, India
e-mail: b.paul@smcs.ac.in

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_3

challenging part is the execution of light and quick cryptography algorithm because of limited processing power, limited battery, and memory capacity of these devices.

Cryptographic algorithms, like, advance encryption standard (AES), Diffi-Hellman (DH), secure hash algorithm (SHA), and Rivest Shamir Adelman (RSA), among others, can be used to address IoT security issues such as IoT data confidentiality, authenticity, and credibility [3].

The remainder of the article is structured as follows: Sect. 2 delves into the three-layer IoT architecture. Section 3 highlights some of the threats and vulnerabilities in each layer followed by potential counter measures in Sect. 4. The articles concludes in Sect. 5.

2 The IoT Architecture

The IoT architecture is a framework that defines the connectivity, communicating protocols, configuration, and organizational structure of the network to be used by the Web-enabled smart devices. Sensors, protocols, actuators, cloud services, and layers all play a significant role in IoT architecture.

There is no single IoT architecture that is widely agreed upon. Researchers have suggested a variety of architecture. In the following subsections, the three-layer architecture on IoT is discussed.

2.1 Three-Layer Architectures

The IoT architecture [4] with three layers, namely the perception layer, network layer, and application layers as shown in Fig. 1 is the most basic architecture which was initially introduced by researchers for the purpose of study.

2.1.1 Perception Layer

The perception layer is the lowest layer of the traditional three-layer IoT architecture that is responsible for hosting smart things [5]. The sensors in physical layer, senses certain physical parameters or detect other smart devices in the vicinity (such as the actuators, edge devices, and wireless sensors) to gather information from the surroundings (such as humidity, and temperature, and so on) and convert them in a digital streams. The primary function of this layer is to provide unique address identification and enable communication between low-range technologies such as RFID, near-field communication (NFC), Bluetooth, 6LoWPAN (low power personal area network) [6].

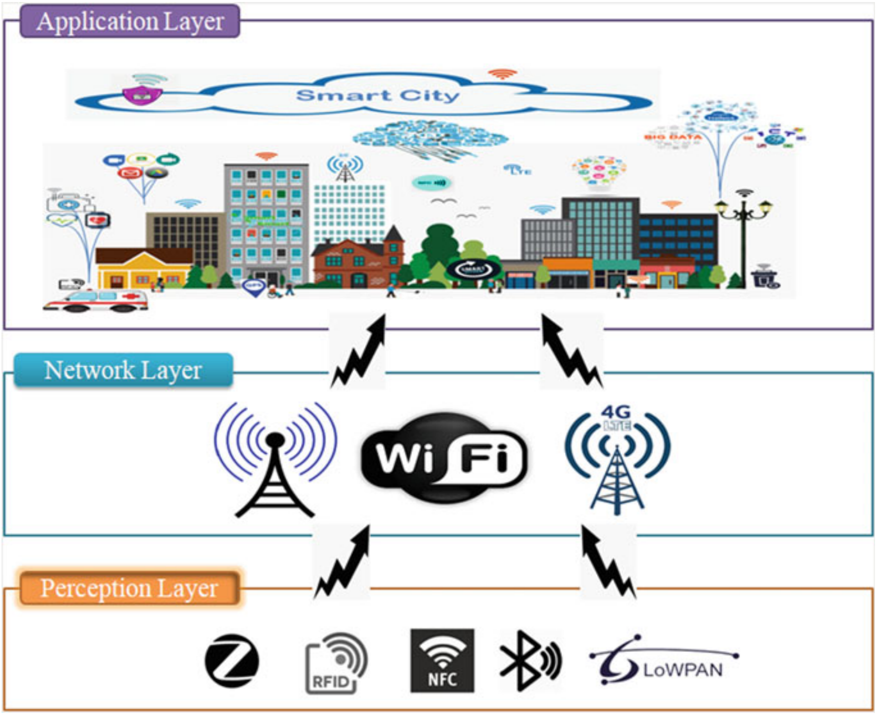

Fig. 1 The three-layer IoT architecture

2.1.2 Network Layer

The network layer is the core layer of the conventional three-layer IoT architecture that is capable of forwarding data for specific services. It enables secure communication across smart things and with the cloud via IoT gateway video networking technologies such as wired, Wi-Fi and cellular technologies. This layer also ensures that each system has its unique addressing and routing capabilities for seamless integration of infinite number of devices into a single unified network. The IETF implementation of 6LoWPAN protocol for IPV6 for unique addressing of devices is one such work involved [7].

2.1.3 Application Layer

The application layer is the topmost layer of traditional IoT architecture responsible for providing its users, customized, application specific services such as, smart education, smart health, smart energy grid, smart transportation, and many more.

3 Security Issues of Three Layer Architecture

As more and more internet-enabled smart gadgets joins the IoT community, greater the security breaches and so the attacks at the aforementioned layers. Security requirements are different at different layers of the IoT architecture. Some of them are highlighted in the following subsections.

3.1 Threats and the Vulnerabilities of Perception Layer

Lightweight encryption algorithm, data protection of sensors, and management of keys are the security requirements for the perception layer. Some of the major security threats encountered in this layer include cyber-attack, malicious code injection, fake node, sensor data security, data access, and authentication issues, malware attacks [8]. If proper security procedures, algorithms, and technologies are not applied in real time, these attacks can disrupt any form of application in IoT architecture. Technology-related attack for this layer is summarized in Table 1.

3.2 Threats and the Vulnerabilities of Network Layer

Identity authentication, encryption mechanism, and communication protection are core requirements for network layer specifications. Denial of services (DoS), man in the middle attack, eavesdropping, RFID interference, node jamming in the WSN, and network congestion attack are other security challenges faced in this layer. Some of the attacks in network layer of three-layer IoT architecture with some possible solutions are listed in Table 2.

3.3 Threats and the Vulnerabilities of Application Layer

Data exchange that protect user privacy and access controls are key security issues in application layer today. Some application layer threats include phishing, ransomware, and X scripts among others. Table 3 provides layer-wise attacks with some possible solutions.

Table 1 Attacks and possible solutions in perception layer

Technology	Attacks	Description	Possible solution
RFID	DoS [9]	Shut downs a machine or network, making it inaccessible to its users resulting in temporary or permanently incapacitated tags	Share tag with the server with a private key which can be encrypted only by authorized user [10]
	Cloning and spoofing [11]	Spoofing is the process of duplicating information from an RFID tag or smart card onto a clone tag to gain access to a protected area or object while bypassing security measures	Verify a tag's response with a OTP sent by the back-end server [12]
	MitM [13]	A hardware device captures and decodes the RFID signal between the victim's card and a card reader in an RFID enabled system	Authentication mechanism that provides evidence that message may have been tempered [14]
	Eavesdropping and replay [15]	Happens when an unauthorized reader is 'listening in' to the conversations between a tag and reader, with the intention of obtaining crucial data, replaying at a later time to steal vital information	VLFSR lightweight encryption function [16]
NFC	Eavesdropping	Happens when a third party intercepts the signal sent between two devices	Random key agreement method [17]
Bluetooth	Blue sniper rifle [18, 19]	A long-distance attacking tool with a powerful directional antenna for interception	Request for pairing before exchanging any information between paired devices [20]
	Blue jacking	Sends unsolicited messages to Bluetooth-enabled devices	
	Blue snarfing	Unwarranted access to schedules, call lists, email and SMS. It can also copy user's contents	
	Blue bugging	Technique to connect to the target device via Bluetooth connection and gain access to owners phonebook, send SMS, initiate or eavesdrop on incoming and outgoing calls	
	Blue printing	Determines the target device model and firmware version	

(continued)

Table 1 (continued)

Technology	Attacks	Description	Possible solution
Zigbee	Unauthorized traffic gathering [21]	Unauthorized access to a ZigBee sensor node causing unwarranted access to the network's shared secret key as well as the network traffic	Secure protocol which allows data flow without compromising security [23]
	Packet decoding and data manipulation [22]	The attacker captures, filters, decodes, and manipulates data packets	
	Sabotage of terminal devices	Causes the battery capacity to be depleted and the key exchange mechanism to be exploited	
6LoWPAN	Sybil attack [24]	The attacker manipulates the node to show multiple pseudo identities for the node, causing the system to be compromised resulting in false alarm. Such an attack is detrimental to distributed environment	Trusted certification, resource testing, recurring fees, privilege attenuation, economic incentives, location/position verification, received signal strength indicator (RSSI)–based scheme, and random key predistribution
	DoS [25]	Smoke screen attack causing security breach of the users' system	Intrusion detection system (IDS) solution, i.e., SVELTE
	Blackhole [26]	Happens when an intermediary captures and reprograms a group of network nodes, the packets are blocked/dropped, and false messages are generated	
	Warmhole [27]	Data packets from a source is tunneled to another location in the network	Regular monitoring of IoT sensors and the network using source routing
	Synchole [28]	This type of attack compromises data confidentiality and interrupt network service by discarding all packets	Message digest algorithm that makes use of cryptography dynamic trust elimination [29]

Table 2 Attacks and possible solutions in network layer

Technology	Attacks	Description	Possible solution
Gateways/Routers/Bluetooth/3G/4G/5G/Wi-Fi	DoS	Attacker floods network with unwanted traffic, causing resource depletion of the targeted system, resulting to inaccessible network	Traffic control, link authentication, active firewalls, and passive monitoring (probing)
	Storage attack [30]	Tempering of users vital data stored in the sensors or on the cloud leading to adversary effect	Backup for storage systems
	Exploit attack	An unethical attack through a set of code over a remote network to exploit software vulnerabilities of all the IoT resources with the intention of taking elevated privileges	
	Malicious code injection [15]	Effects data confidentiality, control flow, and device functionality by introducing a malicious code	Authentication and tamper detection
	Spoofed routing information	An attacker can spoof, alter IP addresses	Active firewalls encryption
	Cross-site scripting	Injection of malicious script into a trusted site,	
	Malicious code attack	It is a harmful script causing security breaches, data theft, and other undesired consequences to the system	

Table 3 Attacks and possible solutions in Application layer

Technology	Attacks	Description	Possible solution
	DoS attacks	Smoke screen attack causing a security breach of the users' system	Secure MQTT solution with ABE
	Gateway attacks [31]	Disconnects the IoT things from the gateway network	Identify a DDos attack early [32]
	Hello flood attack [33]	A node receives a fake HELLO packet broadcasted by attackers, assuming that it within the radio range of the parent node	Bi-directional identity verification protocol for safe communication between the sending and receiving node
	Security patch update problem [34]	Constantly evolving software bug are not being patched	Regular update with software patches/firmwares

4 Counter Measures

In addition to possible solutions listed in the above tables, below are mentioned some of the counter measures. These interventions, however, does not fully eliminate attacks, but they do help minimizes it to a great extent.

4.1 Authentication

Authentication in IoT community allows millions of IoT things to connect for effective and secure communication over an insecure network. The authentication process grants each IoT device in the IoT ecosystem with a unique id that can be authenticated when device attempts to communicate via a gateway or cloud server [35]. However, in IoT device authentication, efficient encrypted key generation and key communication is a challenging task due to lack of guaranteed authorization mechanisms. Authentication is important at any layer of IoT. To prevent DoS attacks, sensor nodes must authenticate themselves at the perception layer. In the network layer Wi-Fi, authentication methods guarantee the security of users' data when it travels over insecure gateway [36]. Security patch update in application layer ensures reliable use of application specific devices. OpenID, a standard open, decentralized framework allows users to be authenticated by relying sites through a third-party provider.

4.2 Authorization and Access Control

Authorization involves security mechanisms to determine users/clients privilege levels to different resources while access control mechanisms guarantees access right of only authorized resources [37]. Installation and regulation of numerous authorization and access control mechanism is a challenge in a heterogeneous IoT network [38]. Authorization controls a device's access throughout the network. Using authentication and access control the relationship between IoT devices is established to exchange appropriate information. OAuth, a standard authorization framework, will grant access to resource, data and features from one application to another through the use of access tokens. However, one challenge encountered by OAuth and Connect is that they have so far only been bound to HTTP, and HTTP is believed to be insecure for communications between IoT devices. Constrained application protocol and MQ telemetry transport are new class of protocols that promises to be better suited than HTTP.

4.3 Secure Architecture

Creating a framework that addresses the aforementioned security issues in an IoT environment is a daunting task. Any IoT architecture should be able to address previously stated security concerns and also the new challenges that comes with installation of IoT devices over software defined networks (SDN) and cloud infrastructure [39], which otherwise will invariably be passed down to the underlying IoT sensors. Furthermore, the difficulties of securely connecting smart IoT objects with cloud services would slew new security risks [40]. Finally, existing intrusion detection and prevention systems face a difficult challenge in detecting malicious traffic rerouted through heterogeneous networks (i.e., SDN, Cloud, and IoT) by unauthorized users [41].

4.4 Block Chain

The Blockchain, an emerging digital technology, has recently gained much popularity in providing secure IoT solutions that can significantly aid in achieving the Internet of Things vision in various ways, such as increasing decentralization capability, promoting interactions, validate new transaction models, and enable autonomous smart objects to seamlessly coordinate through peer-to-peer (P2P) network. The authors in [42] suggests a blockchain-based framework that enables smart devices with single-board computers (SBCs) to communicate with the cloud and send/receive transactions to other internet connected devices on the blockchain network for IoT data in real time. As a proof of concept, experts have conducted simple experiments using Arduino Uno board and Ethereum smart contracts to demonstrate how the platform can be used for MTM interaction and smart prognosis.

4.5 Cryptographic Algorithm/Encryption

Encryption is used to not only protect the data from being tampered with but also to preserve data confidentiality and integrity. Encryption can be accomplished in either of the two ways: node-to-node encryption or end-to-end encryption. Node-to-node encryption performs cipher text altercation at every node, making the network layer more stable. End-to-end encryption, on the other hand, is performed at the application layer where the recipient decrypts the encrypted data sent by the sender. Mathematical algorithm like cryptographic hash functions authenticates a message by generating message authentication codes (MACs). AES, 3DES, and blowfish are other approved symmetric-key algorithms used for encryption/decryption services covering data breaches and unauthorized disclosure of personal information. Among others Hummingbird, Simon and speck, TEA are suggested light weight cryptographic algorithm providing data security [43].

5 Conclusion

IoT is reshaping the next generation Internet. Beyond laptops and smart phones, the idea of connectivity is expanding towards smart cities, smart transport, smart homes, smart farming, connected vehicles, connected wearables, and connected healthcare among others. With the revolution in the usage of Internet-enabled smart gadget and smart decisions being made in real time, the security concerns has also increased many fold. Research in the field of IoT security is still in its infancy, which needs to be explored further to develop secure solutions for its applications. This survey paper not only elicits and explains in depth, different kind of attacks that occur at all the layer of three layer IoT security protocol stack—perception, networking and application layers—but also provide possible solutions that can be applied at these layers. The article may provide researchers with insight as well as an opportunity to work on developing advanced concepts and techniques to deal with the various attacks that exists in the layered IoT architecture.

Future research will be directed toward addressing the vulnerabilities of communication technologies on all the layers of three-layer IoT architecture and implementing secure authentication and authorization methods using encryption algorithm to prevent data from being tempered. This paper can also aid in doing a comparative study between different layered architecture and understand which would offer better service depending on the application need as a single architecture cannot cater to heterogeneous business requirement.

References

1. H. Suo, J. Wan, C. Zou, J. Liu, Security in the Internet of Things: a review, in *International Conference on Computer Science and Electronics Engineering (ICCSEE)* (2012), pp. 648–651
2. A.M. Sadeeq, et al., Internet of Things security: a survey, in *International Conference on Advanced Science and Engineering (ICOASE)*, Kurdistan Region, Iraq (2018)
3. B.N. Silva, M. Khan, K. Han, Internet of Things: a comprehensive review of enabling technologies, architecture, and challenges, IETE Tech. Rev. 1–16 (2017)
4. M. Farooq, M. Waseem, A. Khairi, S. Mazhar, A critical analysis on the security concerns of Internet of Things (IoT). Int. J. Comput. Appl. **111**, 1–6 (2015)
5. L. Zheng, H. Zhang, W. Han, X. Zhou, Technologies, applications, and governance in the Internet of Things. in*Internet of Things—Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT* ed. by O. Vermesan, P. Friess. (River Publishers, 2011), pp. 141–175
6. H. Eun, H. Lee, H. Oh, Conditional privacy preserving security protocol for NFC applications. IEEE Trans. Consumer Electron. **59**, 153–160 (2013)
7. H. Zhang, Y. Zhang, Architecture and core technologies of Internet of Things. J. Changchun Univ. Technol. (Natural Science Edition) 176–181 (2012)
8. U. Kumar, T. Borgohain, S. Sanyal, Survey of security and privacy issues of Internet of Things. Int. J. Adv. Netw. Appl. **6**, 2372–2378 (2015)
9. S. Ghildiyal, A.K. Mishra, A. Gupta, N. Garg, Analysis of denial of service (DoS) attacks in wireless sensor networks. IJRET Int. J. Res. Eng. Technol. 2319–1163 (2014)
10. A. Mitrokotsa, M.R. Rieback, A.S. Tanenbaum, Classifying RFID attacks and defenses. Inf. Syst. Front. **12**(5), 491–505 (2010)
11. Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (2017), pp. 193–202
12. R. Padhy, M. Patra, S. Satapathy, Cloud computing: security issues and research challenges. Int. J. Comput. Sci. Inf. Technol. Secur. (IJCSITS) **1**(2), 136–146 (2011)
13. M. Conti, N. Dragoni, V. Lesyk, A survey of man in the middle attacks, (c). IEEE Commun. Surv. Tutorials **18**, 2027–2051 (2016)
14. P. SaiKiran, E. SureshBabu, D. Padmini, V. SriLalitha, V. Krishnanand, Security issues and countermeaaures of three tier architecture of IOT—a survey. Int. J. Pure Appl. Math. **115**, 49–57 (2017)
15. J. Garcia-Alfaro, J. Herrera-Joancomartí, J. Melià-Seguí, Security and privacy concerns about the RFID layer of EPC Gen2 networks, in *Advanced Research in Data Privacy*, ed. by G. Navarro-Arribas, V. Torra. (Springer International Publishing, 2015), pp. 303–324
16. H.P.T.M. Jayawardana, R.L. Dangalia, Hybrid encryption protocol for RFID data security, in *IEEE International Conference on Decision Aid Sciences and Application (DASA)* (2020)
17. R. Jin, X. Du, Z. Deng, K. Zeng, J. Xu, Practical secret key agreement for full-duplex near field communications. IEEE Trans. Mob. Comput. **1233**, 1–16 (2015)
18. S. Sandhya, K.S. Devi, Analysis of Bluetooth threats and v4.0 security features, in *International Conference on Computing, Communication and Applications, ICCCA* (2012), pp. 1–4
19. J.P. Dunning, Taming the blue beast: a survey of Bluetooth based threats. IEEE Secur. Priv. **8**, 20–27 (2010)
20. S. Sicari, A. Rizzardi, L. Grieco, A. Coen-, Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
21. N. Vidgren, K. Haataja, J.L. Patiño-Andres, J.J. Ramírez-Sanchis, P. Toivanen, Security threats in ZigBeeenabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned, in *Proceedings of the Annual Hawaii International Conference on System Sciences* (2013), pp. 5132–5138
22. Y. Zhang, L. Bo, Q. Ma, A secure data exchange protocol for the Internet of Things (2012), pp. 224–225

23. W. Razouk, G.V. Crosby, A. Sekkaki, New security approach for ZigBee weaknesses. Procedia Comput. Sci. **37**, 376–381 (2014)
24. P. Pongle, C. Gurunath, A survey : attacks on RPL and 6LoWPAN in IoT, in *International Conference on Pervasive Computing (ICPC)* (2015), pp. 1–6
25. M.U. Farooq, W. Muhammad, A. Khairi, S. Mazhar, A critical analysis on the security concerns of Internet of Things (IoT). Int. J. Comput. Appl. **111**, 0975 8887 (2015)
26. J. Jiang, Y. Liu, B. Dezfouli, A root-based defense mechanism against RPL blackhole attacks in Internet of Things networks, in *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* (2018)
27. J. Eriksson, S.V. Krishnamurthy, M. Faloutsos, A practical countermeasure to the wormhole attack in wireless networks, in *Proceedings of the 2006 IEEE International Conference on Network Protocols* (2006)
28. I. Raju, P. Parwekar, Detection of sinkhole attack in wireless sensor network. Adv. Intell. Syst. Comput. **381**, 629–636 (2016)
29. G.W. Kibirige, C. Sanga, A survey on detection of sinkhole attack in wireless sensor network, arXiv preprint arXiv:1505.01941 (2015)
30. S.A. Kumar, T. Vealey, H. Srivastava, Security in Internet of Things: challenges, solutions and future directions, in *Proceedings of the Annual HI International Conference on System Sciences* (2016), pp. 5772–5781
31. R. Zheng, M. Zhang, Q. Wu, C. Yang, An IoT security risk autonomic assessment algorithm. Indonesian J. Electr. Eng. Comput. Sci. **11**, 819–826 (2013)
32. A. Kanuparthi, R. Karri, S. Addepalli, Hardware and embedded security in the context of Internet of Things, in *Proceedings of the 2013 ACM Workshop on Security, Privacy and Dependability for Cyber Vehicles.* (ACM, 2013), pp. 61–64
33. V.A.B.B. Gupta, Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommun. Syst. (2017)
34. L. Kvarda, P. Hnyk, L. Vojtech, M. Neruda, Software implementation of secure firmware update in IoT concept. Adv. Electr. Electron. Eng. **15**(4), 626–632 (2017)
35. F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K.R. Choo, et al., An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. J. Netw. Comput. Appl. **89**, 72–85 (2017)
36. R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, Internet of Things (IoT) security: current status, challenges and prospective measures, in *10th International Conference for Internet Technology and Secured Transactions* (2015)
37. E. Bertino, K.-K.R. Choo, D. Georgakopolous, S. Nepal, Internet of Things (IoT): smart and secure service delovery. ACM Trans. Internet Technol. **16**(4), 1–7 (2016)
38. F. Li, J. Hong, A.A. Omala, Efficient certificateless access control for industrial Internet of Things. Future Gener. Comput. Syst. (2017)
39. S. Raza, T. Helgason, P. Papadimitratos, T. Voigt, SecureSense: end-to-end secure communication architecture for the cloud-connected Internet of Things. Fut. Gener. Comput. Syst. (2017)
40. C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and cloud computing. Fut. Gener. Comput. Syst. (2016)
41. H.H. Pajouh, R. Javidan, R. Khayami, D. Ali, K.-K.R. Choo, A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Trans. Emerg. Top. Comput. (2016)
42. A. Bahga, V.K. Madisetti, Blockchain platform for industrial Internet of Things. Tech. Rep. (2016)
43. S. Surendran, A. Nassef, B.D. Beheshti, A survey of cryptographic algorithms for IoT devices, in *IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (2018)