Security Issues in Internet of Things (IoT): A Comprehensive Review

Mohammad Reza Hosenkhan and Binod Kumar Pattanayak

Abstract Internet of things (IoT) as an extension of existing global Internet is supposed to make it possible for device-to-device communication beyond the human-to-human communication pattern of the global Internet. Billions of smart devices connected to IoT environment can communicate among themselves using sensors and actuators that lead to complex security provisioning for efficient communication across IoT globally. In this paper, we detail the major security as well as privacy issues and possible resolution strategies as extracted from the research work of various authors in this field.

Keywords IoT · Security · Smart devices · Communication

1 Introduction

Information technology (IT) as one of the biggest innovations of the twentieth century has dominated the processes involving varieties of application domains starting from business to scientific applications. It has left a significant global effect on humanity for several decades. IT has played a key role in simplification as well as amplification of outcomes in respective application domains thereby making the processes time as well as cost-effective. Cognitive computing as an integral part of IT has added intelligent behaviour in solving various real-world problems. Moving further, the emergence of global Internet has significantly amplified the effectiveness of IT-oriented processes thereby establishing a global communication environment.

M. R. Hosenkhan (✉)
Faculty of Information and Communication Technology, Université des Mascareignes,
Rose-Hill, Mauritius
e-mail: rhosenkhan@udm.ac.mu

B. K. Pattanayak
Department of Computer Science and Engineering, Siksha 'O' Anusandhan Deemed
to be University, Bhubaneswar, India
e-mail: binodpattanayak@soa.ac.in

S. Patnaik et al. (eds.), *New Paradigm in Decision Science and Management*,
Advances in Intelligent Systems and Computing 1030,
https://doi.org/10.1007/978-981-13-9330-3_36

Operating on Internet Protocol Version 4 (IPV4) backbone, Internet has made it possible for two individuals from any corners of the globe to communicate among themselves in real time that has simplified the business processes thereby significantly improving the business outputs. A wide range of services are supported by Internet that has covered practically all fields of human life. However, Internet in present form can facilitate only human-to-human communications. Recent advancements brought into Internet that is regarded as Internet of things (IoT) are presumed to facilitate communications between anything, anywhere and anytime. The principal motivation behind the innovations of IoT is to facilitate communications between intelligent devices independent of human interventions. IoT is supposed to operate on IPV6 Internet backbone that can facilitate billions of devices around the globe to get connected. As statisticians predict, by the year 2025, as many as 70 billion of intelligent/smart devices can effectively communicate among themselves using the services provided by IoT on IPV6 backbone. A simplified architecture of IoT is depicted in Fig. 1. Devices in IoT referred to as "things" possess their identity belong embedded with sensors can be capable of collecting information from their surroundings and disseminate further to other devices effectively. These "things" can virtually be controlled and regulated remotely. An enormous amount of physical devices referred to as "things" incorporated with computer-based application software can significantly improve the efficiency, accuracy of results thereby providing economic benefits as well. Examples of such "things" can be electric clams in water, biochip transponders, automobiles with built-in sensors, heart monitoring implants and so on. IoT can also be effectively used in disaster recovery applications such as operational on-field devices that facilitate search as well as rescue operations. These devices are supposed to effectively collect relevant information from the surrounding environment through sensors and then share these information autonomously with other devices as and when needed. Alongside the provisioning of the necessary infrastructure along with necessary applications in order for communication among billions of smart intelligent devices in IoT environment, these devices are capable of collecting huge amount of data, aggregate them swiftly, store and disseminate as per requirement. Advantages from the exploration of IoT technology are immense as compared with the existing global Internet. However, for the reason that a large number of devices are supposed to communicate among themselves using the services of IoT autonomously independent of human interventions, there arises ample amount of security issues associated with this innovative method of communication. Devices in IoT environment are vulnerable to external attackers with a higher degree as compared to the current Internet. This necessitates optimal solutions to be innovated to protect the devices in IoT from such attackers and make IoT communication more reliable. In this paper, we outline the security issues related to IoT communication and perform an extensive survey of literature available in the context of IoT security as of today contributed by various authors. The rest of the paper is organized as follows. In Sect. 2, we detail the IoT security architecture and layerwise security issues as well as vulnerabilities. In Sect. 3, we discuss a set of security issues and challenges as reported in the literature. Section 4 outlines the related work in the

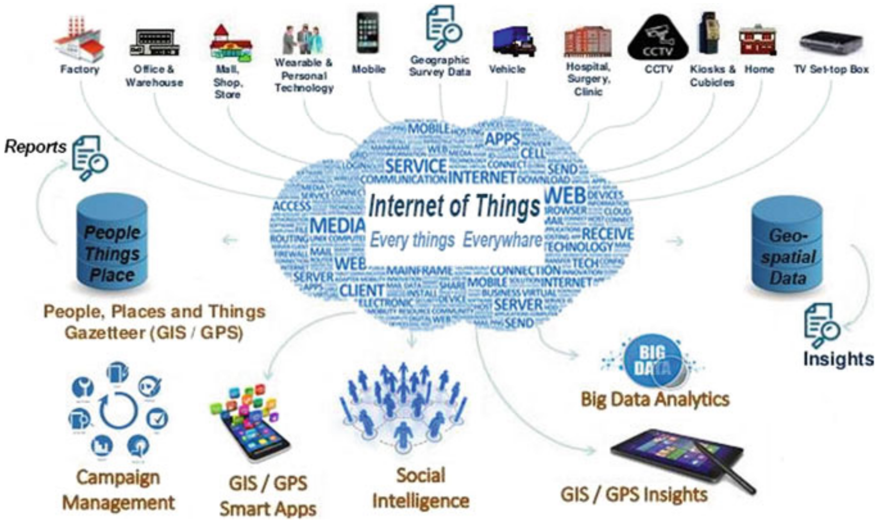

Fig. 1 IoT environment

field of IoT security. Finally, Sect. 5 concludes the paper along with probable future work in this direction.

2 IoT Security Architecture

Security issues related to IoT devices can be split into privacy, ethical and technological levels. Relating to security issues of IoT devices, various authors express their own perceptions. As claimed by authors in [1], the security requirements as required by the IoT devices are:

- Secure authentication;
- Secure bootstrapping;
- Security of IoT data;
- Secure access to data by authorized individuals.

Authors in [2] outline the security requirements for IoT devices as:

- Attack resiliency;
- Data authentication;
- Access control;
- Client privacy.

Authors in [3, 4] focus on:

- Data integrity;
- Data authentication.

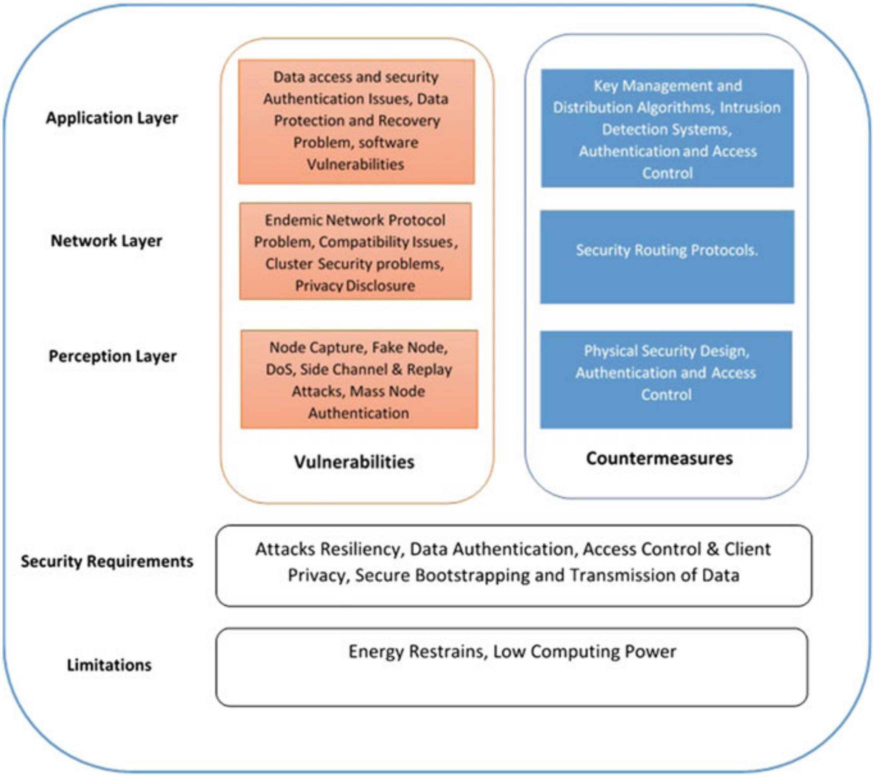
Application Layer
Data access and security Authentication Issues, Data Protection and Recovery Problem, software Vulnerabilities
Key Management and Distribution Algorithms, Intrusion Detection Systems, Authentication and Access Control
Network Layer
Endemic Network Protocol Problem, Compatibility Issues, Cluster Security problems, Privacy Disclosure
Security Routing Protocols.
Perception Layer
Node Capture, Fake Node, DoS, Side Channel & Replay Attacks, Mass Node Authentication
Physical Security Design, Authentication and Access Control
Vulnerabilities
Countermeasures
Security Requirements
Attacks Resiliency, Data Authentication, Access Control & Client Privacy, Secure Bootstrapping and Transmission of Data
Limitations
Energy Restrains, Low Computing Power

Fig. 2 IoT security architecture

In the present scenario, with highly diversified characteristics of IoT, ensuring security and privacy imposes a lot of challenges. Highly scalable and distributive properties of IoT need more flexible as well as innovative security architecture to be devised to meet such challenges in supporting the functionality of IoT devices in the long run. Here, we discuss a security architecture as proposed by authors in [5] that is depicted in Fig. 2.

(a) **Perception Layer**:

(i) As claimed by authors in [6], the limitations of a Wireless Sensor Network (WSN) are power management, network discovery, control and routing. A WSN comprises of the modules hardware, communication stack, and middleware and secure data aggregation and, the basic components like sensor node, micro-controller, memory, radio transceiver and battery. A WSN node is associated with the security requirements like data confidentiality, integrity, freshness, availability, organization autonomy and authentication. The vulnerabilities in a WSN as suggested by authors in [7] are attacks on accuracy and authentication, silent attack on service integrity and attacks on network availability. Further, authors in [8] claim that the concerns of security in WSN can be resolved making use of authentication procedures using public key infrastructure (PKI).

(ii) Radio frequency identification (RFID): Radio frequency identification (RFID) technology can be used for unique identification by virtue of associating passive tags to the items they are attributed to. Authors in [9] propose various security standards for RFID technologies not only in order for addressing security concerns, rather the interaction issues as well.

(iii) IEEE 802.11 Wireless Protocol Standard: IEEE 802.11-based wireless networks are vulnerable to passive attacks such as eavesdropping [10]. Nevertheless, active attacks too can be viable by the virtue of exploitation of hardware vulnerabilities [11].

(iv) Long-term evolution (LTE): Long-term evolution (LTE) devices can be used to connect IoT devices to Internet in wireless mode in the absence of wired communication that guarantees efficient communication [12]. LTE devices are vulnerable to active as well as passive attacks. However, active attacks can be eliminated using cryptographic method. As claimed by authors in [13], passive attacks in such networks are almost impossible.

(v) WiMax (IEEE802.16): This technology can be extremely useful for connecting IoT devices in metropolitan areas and does not entertain the popularity in modern scenario though. It can support higher data rates with longer range of communication. Security specification in this standard basically exists in MAC layer which is also regarded as security or privacy layer [14]. That indicates that physical layer remains virtually unprotected. The security concerns related to this technology represent jamming at the level of physical layer that may very much lead to denial-of-service attack [15]. At the same time, the security/MAC layer can be susceptible to man-in-the-middle attack.

(vi) Near-field communication: Near-field communication (NFC) can be used for wide-range communication of IoT devices for operations such as payments, authentication and so on and has a short range of 20 cm though. NFC is also susceptible to security threats like denial-of-service (DOS) attacks, compromise of information and so on [16]. NFC suffers from the major security threat that sometimes it may not be encrypted that leads to the fact that the signal emerging from an IoT device may be captured by external antennas [17].

(vii) Bluetooth: Bluetooth technology has been proactively used for indoor systems in the context of iBeacons [18]. It can also be used for sensor networks meant for monitoring of earthquake. Security measures in this technology can be achieved in three different ways: (1) using pseudorandom frequency hopping; (2) restricted authentication; and (3) encryption [19].

(viii) Ultra-wideband (UWB): It represents a high-precision low power technology that can be used for IoT smart applications. It is considered to be more secured as compared to other technologies due to its high processing power and high range and most importantly its security aspects [20].

(b) **Middleware**:

IoT middleware is intended for interaction with the cloud technology and peer-to-peer systems. The list of services offered by middleware [21] follows.

(i) Event-based: Authors in [21] claim that all the components of middleware communicate among themselves through events where the events operate on specific parameters that refer to changes in state. Some of the applications in the middleware do incorporate security features and some do not.

(ii) Service-based: Service-based applications in the middleware are identical to that in a service-oriented computer (SOC) system that further relies on service-oriented architecture (SOA). These applications do encompass security attributes, and at the same time, they are vulnerable to security threats too [22].

(iii) Virtual machine (VM)-oriented: As assumed by authors in [21], the applications that rely on virtual infrastructure in order for safe execution are regarded as virtual machine (VM) applications in the middleware. Each application includes specific modules which interact with the VM running on each node in the network. Mate, a middleware application, incorporates a specific component that is dedicated to security provisioning which is responsible for blocking malicious programs propagating in the network [23].

(iv) Agent-based: Agent-based middleware includes mobile agents that are responsible for the security analysis of vulnerabilities [24].

(v) Tuple spaces: Tuple space middleware comprises of components that incorporate a repository called as tuple space and those do not support any security mechanism as such.

(vi) Application-specific: This middleware focuses on the management of resources for various applications as when required by the application [25].

(c) **Application Layer**:

The application layer comprises of the following protocols.

(i) Message Queue Telemetry Transport (MQTT): The IoT devices are incapable of dealing with the higher layer traditional application layer protocols like SMTP, SNMP and so on. Mostly lightweight protocols are devised for these devices by researchers in this field. Message Queue Telemetry Transport (MQTT) belongs to the class for such lightweight protocols especially devised for IoT devices that are constrained by factors such as high latency and low bandwidth operating in unreliable network environments [26]. The biggest advantage of MQTT is that it is compatible with any identification, authorization and authentication procedures in the context of network security. Identity of MQTT server can be achieved from its IP address along with the digital certificate associated with it. Its authorization too is obtained from MQTT server. Seekit that is a model-based security tool is responsible for privacy as well as protection of data in MQTT [27].

(ii) Extensible Messaging and Presence Protocol (XMPP): Extensible Messaging and Presence Protocol (XMPP) represents an extension of Extensible Markup Language (XML) that facilitates the exchange of real-time extensible data among network nodes. It does not possess any end-to-end security feature, rather protected with TLS alone. It relies upon Salted Challenge Response Authentication Mechanism (SCRAM) for security provisioning. SCRAM and TLS together provide authentication as well as confidentiality in MQTT [5].

(iii) Blockchain: Blockchain proposed in [28] is intended for solving double spending problem in cryptocurrency systems. It can be successfully applied without relying upon any third-party authentication mechanism. Blockchain can only provide pseudo-anonymity. In order for ensuring privacy in IoT systems, additional mechanisms must be implemented.

3 IoT Security Issues and Challenges

Security provisioning in such a huge heterogeneous environment with various devices like IoT becomes extremely challenging. In this section, a list of issues and challenges pertaining to security of an IoT system is detailed below [29].

(a) Privacy Context Awareness: This feature needs that the essential portion of the context of an object must be recognized effectively.

(b) Coupling of Digital Device and Physical Ambience: It needs that the processor must be coupled with the physical environment in order for the measurement of various information.

(c) Identification in IoT: For the reason that enormous number of applications may run on IoT environment, each of them must have an identification in all layers of the IoT protocol stack.

(d) Device Authentication: The smart devices in an IoT environment relying on sensors for data collection and aggregation are governed by a set of rules that provide the authentication for authorization of these sensors for sharing information.

(e) Data Combination: The heterogeneity of devices in IoT leads to different data formats supported by different devices. These data need to be combined to produce more meaningful information that further necessitates stringent security policies for its realization.

(f) IoT Scalability: With continuous innovations more and more devices can be added to IoT environment that needs the establishment of communication patterns for communication among such devices and it needs strict security measures to be incorporated in the environment.

(g) Secure Configuration and Setup: Resolving the scalability issue in IoT needs that a secure setup mechanism should also be provisioned which can be achieved on the basis of privacy.

(h) IoT and Critical Infrastructure (CI): The issues related to threats and privacy in IoT developed on critical infrastructure (CI) such as telecom, energy, etc. Need to be addressed optimally.

(i) Conflicting Market Interest: IoT becomes a more competitive environment that is capable of providing correlated data from different sources, and hence, the need arises for protection of personal correlated data.

(j) IoT with Evolution of Internet: Continuous evolution of global Internet has a direct impact on IoT, and it necessitates provisioning of data security and privacy of different elements constituting IoT environment.

(k) Trust Level Between IoT and Human: There must be guaranteed a specific level of trust between the human and IoT elements. Along with the trust level of machines belonging to IoT, human privacy must be ensured too.

(l) Data Management: Data protection on IoT can be achieved using cryptographic methods as well as respective protocols and for this purpose, exclusive policies need to be defined.

(m) IoT Devices' Durability: The fact that every entity on IoT has a limited and more specifically a short lifespan should be kept in mind during IoT security implementation.

4 Related Work

A limited spectrum of work has been reported in the literature pertaining to the security issues related to IoT. In this section, we discuss the contributions from different authors on IoT security as a whole. A general survey of various issues relating to IoT security as well as user privacy has been conducted by the authors in [30] wherein authors focus on the issues from end user's perspective with spreading of IoT technology. It should be noted that authors mostly pay attention to the security issues arising from information exchange among different entities on IoT. As a matter of fact, conventional security and privacy measures fail to provide the desirable level of security in IoT due to its decentralized topology and thus researchers now focus on blockchain (BC) technology that relies on cryptocurrency called Bitcoins. Again, BC considered to be computationally expensive is also incapable of providing desirable level of security for the reason that in incurs high bandwidth overhead. This problem is addressed by authors in [31] wherein authors propose a new secure IoT architecture using BC that is experimented on a smart home application that virtually addresses the limitation of bandwidth overhead successfully. This methodology of security provisioning in IoT using BC has been further explored by authors in [32] thereby proposing a lightweight scalable blockchain (LSB) scheme for this purpose that is again experimented on a smart home and results justified. A comprehensive analysis of security threats pertaining to IoT environment along with the probable resolution strategies is conducted by authors in [33] thereby putting emphasis on the significant role of encryption technology in security provisioning for IoT. Details of various IoT security issues along with their countermeasure with the help of some newly proposed algorithms have been addressed by authors in [34]. A matrix of security concerns has been innovated by the authors in [35] wherein focus is given on IoT middleware security provisioning with reference to the said matrix and probable measures are detailed as well. The underlying protocol architecture along with the security concerns of IoT is elaborated in a comprehensive survey work of authors in [36]. A discussion on IoT security issues related to access control to devices on IoT and their privacy concerns are addressed by authors in [37]. A layerwise security issues with respect to IoT protocol architecture along with resolution methods have been addressed by authors in their comprehensive survey work [38]. Security issues related to IoT devices specifically with low computing power and less memory capacity are addressed and measures outlined by the authors in [39]. Analysis of security as well as privacy concerns keeping in mind the heterogeneity of IoT environment is performed by authors in [40]. Taking into account the context-aware intelligent integrated services provided by IoT, the major security concerns in the context of the IoT protocol architecture are detailed in a comprehensive review work by authors in [41].

5 Conclusion and Future Work

Internet of things (IoT) as an innovation of the existing global Internet is supposed to connect billions of devices to the Internet worldwide. It is fascinated by its tremendous scalability features accommodating heterogeneous smart devices thereby provisioning an efficient communication among these devices using sensors and actuators. More than collection and aggregation of data, it is more important to make the communication environment more secure. With the dimensions of IoT and heterogeneity of devices connected to it, security provisioning becomes an extremely challenging task. Before security provisioning can be facilitated, it is vital to identify all security challenges and vulnerabilities related to this amazing technology. We have attempted to identify the security concerns with reference a proposed IoT security architecture and also conducted a comprehensive review of work available in the literature up to date. This paper may be quite useful for the researchers working in the area of IoT security. Moving further, we acknowledge that the amazing scalability feature of IoT that grows exponentially in terms of number of devices attached to it may lead to new security concerns that need to be resolved. We aim at extending our research work in this direction in future.

References

1. Borgia, E.: The internet of things vision: key features, applications and open issues. Comput. Commun. **54**, 1–31 (2014)

2. Weber, R.H.: Internet of things–new security and privacy challenges. Comput. Law Secur. Rev. **26**(1), 23–30 (2010)
3. Zafari, F., Papapanagiotou, I., Christidis, K.: Micro-location for internet of things equipped smart buildings. CoRR, vol. Abs/1501.01539 (2015)
4. Zafari, F., Papapanagiotou, I., Christidis, K.: Microlocation for internet-of-things-equipped smart buildings. IEEE Internet Things J. **3**, 96–112 (2016)
5. Mendez, D., Papapanagiotou, I., Yang, B.: Internet of things: survey on security and privacy. Inf. Secur. J. A Glob. Persp., 1–16 (2018)
6. Atamli, A.W., Martin, A.: Threat-based security analysis for the internet of things. In: 2014 International Workshop on Secure Internet of Things (SIoT), pp. 35–43, IEEE (2014)
7. Borgohain, T., Kumar, U., Sanyal, S.: Survey of security and privacy issues of internet of things (2015). arXiv preprint, arXiv:1501.02211
8. Medaglia, C.M., Serbanati, A.: An overview of privacy and security issues in the internet of things. In: The Internet of Things, pp. 389–395, Springer (2010)
9. Phillips, T., Karygiannis, T., Kuhn, R.: Security standards for the rfid market. IEEE Secur. Priv. **3**(6), 85–89 (2005)
10. Djenouri, D., Khelladi, L., Badache, N.: A survey of security issues in mobile ad hoc networks. IEEE commun. Surv. **7**(4), 2–28 (2005)
11. Naeem, T., Loo, K.-K.: Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, vol. 3, no. 1 (2009)
12. Costantino, L., Buonaccorsi, N., Cicconetti, C., Mambrini, R.: Performance analysis of an LTE gateway for the IoT. In: 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–6, IEEE (2012)
13. Bilogrevic, I., Jadliwala, M., Hubaux, J.-P.: Security issues in next generation mobile networks: LTE and femtocells. In: 2nd International Femtocell Workshop, No. EPFL-POSTER-149153 (2010)
14. Papapanagiotou, I., Toumpakaris, D., Lee, J., Devetsikiotis, M.: A survey on next generation mobile wimax networks: objectives, features and technical challenges. Commun. Surv. Tutorials IEEE **11**(4), 3–18 (2009)
15. Hasan, S.S., Qadeer, M.A.: Security concerns in wimax. In: First Asian Himalayas International Conference on Internet, 2009. AH-ICI 2009, pp. 1–5, IEEE (2009)
16. Madlmayr, G., Langer, J., Kantner, C., Scharinger, J.: NFC devices: security and privacy. In: Third International Conference on Availability, Reliability and Security, 2008. ARES 08, pp. 642–647, IEEE (2008)
17. Curran, K., Millar, A., Mc Garvey, C.: Near field communication. Int. J. Electr. Comput. Eng. **2**(3), 371 (2012)
18. Estimote, Estimote Real World Context for Your Apps. http://www.estimote.com. Online; Accessed 26 Sept 2014
19. Bouhenguel, R., Mahgoub, I., Ilyas, M.: Bluetooth security in wearable computing applications. In: 2008 International Symposium on High Capacity Optical Networks and Enabling Technologies, pp. 182–186, IEEE (2008)
20. Ullah, S., Ali, M., Hussain, A., Kwak, K.S.: Applications of UWB Technology (2009). arXiv preprint, arXiv:0911.1681
21. Razzaque, M.A., Milojevic-Jevric, M., Palade, A., Clarke, S.: Middleware for internet of things: a survey. IEEE Internet Things J. **3**(1), 70–95 (2016)
22. Eisenhauer, M., Rosengren, P., Antolin, P.: Hydra: a development platform for integrating wireless devices and sensors into ambient intelligence systems. In: The Internet of Things, pp. 367–373, Springer (2010)
23. Costa, N., Pereira, A., Serodio, C.: Virtual machines applied to WSN's: the state-of-the-art and classification. In: 2007 Second International Conference on Systems and Networks Communications (ICSNC2007), pp. 50–50, IEEE (2007)
24. Nagy, M., Katasonov, A., Szydlowski, M., Khriyenko, O., Nikitin, S., Terziyan, V.: Challenges of Middleware for the Internet of Things. INTECH Open Access Publisher (2009)

25. Murphy, A.L., Picco, G.P., Roman, G.-C.: Lime: a middleware for physical and logical mobility. In: 21st International Conference on Distributed Computing Systems, 2001, pp. 524–533, IEEE, 2001
26. Stanford-Clark, A.N.A.: MQTT version 3.1.1. OASIS Std., Oct 2014
27. Neisse, R., Steri, G., Baldini, G.: Enforcement of security policy rules for the internet of things. In: 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 165–172, IEEE (2014)
28. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
29. Zolanvari, M.: IoT security: a survey. (2015). http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec/index.html
30. Borgohain, T., Kumar, U., Sanyal, S.: Survey of security and privacy issues of internet of things. Int. J. Adv. Netw. Appl. **6**(4), 2372–2378 (2015)
31. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in Internet of Things: Challenges and Solutions. arXiv preprint arXiv:1608.05187 (2016)
32. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: LSB: A Lightweight Scalable Blockchain for IoT Security and Privacy, pp. 2–17 (2017) arXiv:1712.02969v1cs.CR
33. Ahmed, A.W., Ahmed, M.M., Khan, O.A., Shah, M.A.: A comprehensive analysis on the security threats and their countermeasures of IoT. Int. J. Adv. Comput. Sci. Appl. (IJCSA) **8**(7), 489–501 (2017)
34. Pandey, E., Gupta, V.: An analysis of security issues of internet of things (IoT). Int. J. Adv. Res. Comput. Sci. Softw. Eng. (IJARCSSE) **5**(11), 1768–1773 (2015)
35. Fremantle, P., Scott, P.: A survey of secure middleware for the Internet of Things. PeerJ Comput. Sci. **3**, e114 (2017)
36. Chetan, C., Tejaswini, N.P., Guruprasad, Y.K.: A survey on applications, privacy and security issues in internet of things. Int. J. Adv. Res. Comput. Sci. (IJARCS) **8**(5), 2433–2436 (2017)
37. Satish, K.J., Patel, D.R.: A survey on internet of things: security and privacy issues. Int. J. Comput. Appl. (IJCA) **90**(11), 20–26 (2014)
38. Jaychand, Behar N.: A survey on IoT security threats and solutions. Int. J. Innov. Res. Comput. Commun. Eng. (IJIRCCE) **5**(3), 5187–5193 (2017)
39. Fernandes P., Monteiro, A., Lasrado, S.A.: Evolution of internet of things (IoT): security challenges and future scope. Int. J. Latest Trends Eng. Technol. (IJLTET) (Special Issue), 164–169 (2016)
40. Suchitra, C., Vandana, C.P.: Internet of things and security issues. Int. J. Comput. Sci. Mob. Comput. (IJCSMC) **5**(1), 133–139 (2016)
41. Choudhury, A., Godara, S.: Internet of things: a survey paper on architecture and challenges. Int. J. Eng. Technol. Sci. Res. (IJETSR) **4**(6), 442–447 (2017)