GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 06, June 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

INTRODUCTION OF INTERNET OF THINGS (IOT) IN BUSINESS SCIENCES—BRIEF REVIEW OF SECURITY AND CHALLENGES

Devarshi Chatterjee[1] and Dr Devapriya Chatterjee[2]

[1]Student, Indian Institute of Management Bangalore, India
Email: deva.chat123@gmail.com;
Sunder Ram Shetty Nagar, Bengaluru, India, 560076
[2]Ex-Director (MBA), Shankara Group of Institutions Jaipur, India Management Consultant and Chartered Engineer (India)
Email: chatterjee.devapriya@gmail.com
Salt Lake City, Kolkata, India, 700064

Abstract

We are aware that Internet of Things (IoT) satisfies the purpose of the free flow of information between various low-powered embedded devices, utilizing the technology of Internet for communication amongst one another. We find that Internet of Things (IoT) could be widely deployed and its applications would be in various domains of life. The technology of Internet of Things (IoT) has now appealed to various domains of life and finds the appropriateness in diverse activities. The organizations in Business Sciences are eager to implement Internet of Things (IoT), and are much inquisitive about the output that would be generated by deploying these categories of the networks. However, we also need to make an assessment of the various privacy and security issues for the end users of Internet of Things (IoT), that limit its proliferation. The paper categorizes, discusses and identifies the state-of-the-art effects, as well as various issues and challenges of security, that need to be resolved. The Internet and embedded technologies have enabled devices, that surround us to be interconnected with each other. We visualize a future, where Internet of Things (IoT) would be enclosed in a concealed manner in the environment around us, and bring the output of huge amount of data. The data is needed to be preserved and treated for making it comprehensible and functional. Any model of Internet of Things (IoT) would involve different workmen, that include access technology providers, mobile operators as well as software developers. The domains of the applications of Internet of Things (IoT) need to be broad, and that ensure that networks could be positioned in agriculture, manufacturing, healthcare and utility management. We envisage Internet of Things (IoT) as the interconnection paradigm of the next generation, that would permit connectivity amongst machines and devices of people, that would permit actions to take place, without human intervention.

Keywords : low-powered, appropriateness, privacy, security, and state-of-the-art

Introduction

The successful outcome of the world of Internet of Things (IoT) necessitates that different communication structures are well-merged, that would result in the designing of smart gateways

for the connection of the traditional Internet with the Internet-of Things (IoT) devices. The innovative efforts in the area, include the interconnection of cloud computing, that supplement the potential of Internet of Things (IoT) and the infrastructure of Internet of Things (IoT). The continuous augmentation of the complexity of the networks of Internet of Things (IoT), also augment the challenges of security, that are faced by these networks. The large number of devices, that are connected between the huge data that are generated by the devices and the Internet augment the complexity of the networks of Internet of Things (IoT). The devices in the network of Internet of Things (IoT) are susceptible to attacks, as these are easy targets for attacks. As of now, the devices of Internet of Things (IoT) do not have the software of malware protection or virus protection. As soon as the hackers gain control, the devices close to the compromised node are attacked, resulting in low power nature and low memory of the devices. The attackers also damage the forwarding operations and routing operations of the device.

Furthermore, the attackers also make access to the sensitive data, that are collected and transmitted by the devices of Internet of Things (IoT). It is thus observed that the lack of security of the data in Internet of Things (IoT) tends to make disruption in the widespread adoption of this technology. The security challenges of Internet of Things (IoT) mainly involve lightweight cryptographic framework for Internet of Things (IoT), resilience and robustness management in Internet of Things (IoT) and Denial of Service (DoS), privacy in Internet of Things (IoT), and secure forwarding and routing in Internet of Things (IoT).

Objectives of the Study

The main objectives of the study include :

a) Discussing the state-of-the-art lightweight cryptographic framework for Internet of Things (IoT)
b) Discussing the state-of-the-art in provisioning resilience and robustness management in Internet of Things (IoT) and Denial of Service (DoT)
c) Discussing the privacy issues in Internet of Things (IoT)
d) Discussing the state-of-the-art proposals in secure forwarding and routing in Internet of Things (IoT)

Methodology

The methodology comprises of the establishment of the motivation of the four factors related to the security issues of Internet of Things (IoT).

There are new challenges that are introduced by Internet of Things (IoT) in power and energy consumption. It was ensured that the designs for Internet of Things (IoT) of cryptographic primitives, need to be lightweight. The target result is the consumption of fewer resources by the primitives, without any compromise in the required security level. Hence the trend of focus is on lightweight cryptography. The consumption of energy and the size of the chip comprise of the most important measures for assessment of the properties of lightweight. In case of software implementation, a small code and a small size of Random Access Memory (RAM), are preferable for lightweight applications.

The networks of Internet of Things (IoT) constitute of such miscellaneous deices, that managing the network becomes a difficult task. The latest trend is to focus on service-oriented architecture (SOA), due to its ability to cater to the management and integration of heterogeneous services of Internet of Things (IoT). This paradigm enables the construction of a lightweight middleware upon the devices of Internet of Things (IoT), that delivers the necessary abstraction of manageable and integratable services of Internet of Things (IoT). The users and the developers of the devices of Internet of Things (IoT) are unaware of the methods of usage and connection of devices. System failures, that arise from the faults in the applications of Internet of Things (IoT), disrupt the activities, and may also endanger lives. The service-oriented architecture (SOA) based middleware for Internet of Things (IoT) is subjected to all types of built-in problems in distributed systems. In addition to the normal faults in the devices of Internet of Things (IoT), there could be faults due to the attacks of Denial of Service (DoS) on devices of Internet of Things (IoT), that disrupt the services of Internet of Things (IoT) to the users of applications.

The attacks of Denial of Service (DoS) make the services of Internet of Things (IoT) unavailable and hamper the normal operations. The attacks made by Denial of Service (DoS) are made in a coordinated manner, from multiple attackers simultaneously, and identification of the attacks, before the failure of the services, are difficult. The challenge of the businesses is the addressing of risks, as well as understanding themselves from insider attacks, that normally generates by the

use of unknown devices, and prove to be unmanageable and undetectable by the applications of Internet of Things (IoT), that become the integral part of applications of business.

The primary security issue that needs complete focus from the researchers is privacy in Internet of Things (IoT). It is of utmost importance that management frameworks and protocols are engaged to handle privacy in Internet of Things (IoT), that constitute the integral part in diverse applications, in the nature of energy consumption control, smart parking system, remote patient monitoring and traffic control. The users of these applications need protections of personal information, that pertain to their habits, interaction and movement.

The secure forwarding and routing in Internet of Things (IoT) involve the threats of IPv4, that are inherited by IP-based Internet of Things (IoT). These attacks are known as spoofing, black-hole attacks, eavesdropping, sybil, neighbor discovery, fragmentation, man-in-the-middle and rogue devices. These indicate that the requirement of Internet of Things (IoT) is similar measure of security, as needed in IPv4, as it is anticipated that Internet of Things (IoT) of the users of the world, would be connected with the Internet, that has several issues of security. The issues of threat not only include the maneuvering of information but also effective control of devices in the network of Internet of Things (IoT). The addition of electronic systems, result in a considerable rise in attacks, that give rise to new threats of security as miscellaneous devices, also become part of the network of Internet of Things (IoT). A route is set in a wireless mobile network, when the information from node to node is communicated, until the establishment of the new destination. Nodes are added or deleted during the period of route maintenance, and this might result in the delay of imparting control information, that is the normal function of transgressing nodes. Several attacks may take place, during the period of routing setup, in routing information. A routing table attack of overflowing, by transfer of a huge amount of incorrect routing information to neighboring nodes, would cause a neighboring routing table to overflow. Such cases resist the real routes from occupying the routing table, due to the overflow of bogus routes.

Findings

It would now be brought to light, the findings of the issues and challenges in the introduction of Internet of Things (IoT) in business sciences.

Due to the constraints in the resources of hardware, the requirement arises for the design of lightweight cryptographic framework for Internet of Things (IoT). For this purpose, it is needed to revisit cryptographic primitives, and make the necessary designs, that take into account the limitations of the devices of Internet of Things (IoT).

As far as the resilience and robustness management is concerned, the most important challenges are considered to be :

a) early detection of attacks : After the initiation of the attack, it is necessary that the protocols and the methods of the network of Internet of Things (IoT), detect the attack at the quickest possible time, before major damages are caused, that affect the entire network.

b) tolerance of attacks : It is absolutely essential that the networks of Internet of Things (IoT) are provided with novel and new network designs, that provide built-in tolerance to malicious attacks and intrusions.

c) Failure Recovery : The network of Internet of Things (IoT) needs quick recovery, before the attack becomes critical. For applications of disaster management, long duration of disruption in the services of Internet of Things (IoT), lead to life threatening situations. As such, the resource management middleware, that is designed for the network of Internet of Things (IoT) needs to make the resolution of the issue, by quick detection of failures. We have numerous possible solutions for the resolution of the failures of the devices of Internet of Things (IoT). A likely solution is the replication of the resources, and the subsequent deployment without change in the environment. This type of solution is not very cost-effective, as there is involvement of duplication of resources.

The challenges of Denial of Service (DoS) are being mentioned briefly :

a) countermeasures : It is necessary to position countermeasures to alleviate the attack as soon as Denial of Service (DoS) is detected. As the networks of Internet of Things (IoT) are extremely economic constraints, there is the priority of the design of energy efficient as well as lightweight strategies of countermeasure.

b) detection of Denial of Service (DoS) attack : Systematic Denial of Service (DoS) detection solutions are necessary, as there is considerable difficulty in detecting the attack before the launch of the attack. Due to the constraints of the devices of Internet of Things (IoT), cost-effective Distributed Denial of Service (DDoS) detection and efficient techniques of countermeasure are required. These are centralized techniques such that traffic in the network of Internet of Things (IoT) can be monitored. There are prospective techniques that assist in detecting the possible attacks of Distributed Denial of Service (DDoS). These techniques are deployed when multiple devices of Internet of Things (IoT) collectively deduce an attack of Distributed Denial of Service (DDoS) in the network of Internet of Things (IoT).

c) detection of insider attack : It is necessary that there is authorization of nodes of Internet of Things (IoT) for becoming part of the network of Internet of Things (IoT) for the prevention of insider attacks. Efficient techniques with swift reaction are necessary for the detection of insiders in the network of Internet of Things (IoT). In the absence of the same, disastrous situations would befall, as insiders could leak secret data by compromising nodes, launch attacks like Distributed Denial of Service (DDoS) attacks and disrupt the operation of the networks of Internet of Things (IoT).

As far as privacy in Internet of Things (IoT) is concerned, it is necessary for every solution or framework to address these challenges.

a) track and localize : A major threat is localization, where systems try to locate the user through space and time. The greatest challenge of security solutions is to design protocols for interactions with Internet of Things (IoT), that restrain such activities. It is common in e-commerce applications to outline information of users for deducing their interests by connecting with data of other users and data. The biggest challenge is the positioning of interests of businesses for the analyses of data and outlining with the privacy requirements of the user.

b) track and profile : When there is relation of identity with a certain user, there is a threat that leads to tracking and profiling. Here, the major challenge is to take preventive measures, to restrain such activities in Internet of Things (IoT).

c) transmission of data : It is necessary to make certain that data are transmitted in a secure path, without the hiding of any information, and preventing unlawful garnering of information about users and things.

The most important challenges in forwarding and secure routing, are given below, and need to be resolved on priority.

a) malicious nodes isolation : The expeditious detection of malicious nodes, along with the robust techniques of design, for making isolation, from the networks of Internet of Things (IoT) is of prime importance. The isolation of malicious nodes in the network is made by the protocol, such that disruption in the process of secure routing is completely eliminated or minimized. Most of the networks of Internet of Things (IoT) are self-organizing, and operate automatically (without human intervention) making the protocols of routing insecure. The networks of Internet of Things (IoT) are vulnerable and susceptible to malicious node, so designs of protocols with superior techniques for blocking malicious nodes on detection in the network and restrain the malicious nodes from making entry in the network.

b) location privacy preservation : It is necessary to maintain the privacy of location in the devices of Internet of Things (IoT), in the network. For this purpose, the feature for privacy of location, should be included in the secure routing protocol.

c) route establishment security : It is needed to have a protocol, that could establish a route securely, and guarantee the security among the nodes of transmission. In order to be adequately distributed by the low-powered networks, there needs to lightweight computation for the secure routing of the data.

d) Security protocol self-stabilization : The protocol should be able to make automatic recovery from any type of problem without any human involvement and within a time limit. This is known as self-stabilization.

Discussion and Implication

a) With reference to a lightweight cryptographic framework for Internet of Things (IoT), it is proposed to have a security architecture, that would confirm the goals of security.

This solution is required to work according to the lifetime of the smart device in the network of Internet of Things (IoT). The input is needed to be controlled by Trusted Third Party (TTP) infrastructure. The framework would be utilized for manufacturing smart objects in a protected framework. It is further discussed that a distributed, fast and resource-friendly mechanism for input agreement and for authentication of parameters of identification in Wireless Sensor Network (WSN). The mechanism is based on alpha secure polynomials, for the purpose of establishment and distribution of the input, and cause the calculation of polynomials to be more lightweight. The input pre-distribution schemes of lightweight are proposed for Internet of Things (IoT), that cause efficiency of the resources and the necessary algorithms. The scheme based on identity requires a Trusted Third Party (TTP), as well as a node with an identifier. The Trusted Third Party (TTP) provides in the network a node, with secret input material, that is connected to the identifier of the device in a secure way. There are a number of security challenges in Internet of Things (IoT) communication. In order to design an optimum security architecture, it is necessary to consider the capabilities as well as the life cycle of the device of Internet of Things (IoT). There is the requirement of the inclusion of the type of applied protocols and the aspects of the Trusted Third Party (TTP), in the architectural design. It is also proposed that the architecture is scaled from small scale security domains to large scale set-ups. It is necessary to adopt large-scale protocols in an architecture. It has also been found that every layer of Internet of Things (IoT), namely, link, network or application layer has a different requirement of communication and security. The network is open to attacks if security is positioned in application layer. There are possible threats of inter-application security, if security is focused on link or network layer. A lightweight framework of security, with an architecture, containing lightweight functionality of authorization and authentication on smart objects, would provide an optimum environment of Internet of Things (IoT). It is also discussed that systems based on Near Field Communication (NFC), have security weaknesses, and for this purpose, a security middleware is necessary, that is fast in detecting malicious tags of Near Field Communication (NFC). The lightweight primitives of middleware provide the applications of Near Field Communication (NFC) with the support of integrity

and confidentiality. Another security scheme could be discussed for Internet of Things (IoT) based on the Internet on a low-power hardware platform. The existing security solution is too heavy for low power devices and is unable to prevent attacks on routing. It may be established that lightweight framework, that comprises of protocols like Datagram Transport Layer Security (DTLS) and Constrained Application Protocol (CoAP) are the best end-to-end security for Internet of Things (IoT).

b) It is needed to discuss the robustness in the network of Internet of Things (IoT). There are problems of malicious nodes in the framework. For controlling the revocation and admission of the nodes by way of collaboration in the form of two voting procedures, another protocol, Efficient Cooperative Security (ECoSec) is brought into the picture. It is needed to depend on Trust Management, for providing resilience in Internet of Things (IoT). Artificial-Intelligence based solutions for fault tolerance in Internet of Things (IoT) could be utilized by using fault-tolerant routing protocol and hybrid cross-layer. There is optimal action when there is dynamic adaption of the algorithm to the dynamic environment. Further, there is the adoption of the fault-tolerant routing, that is energy aware, by the algorithm. There is conservation of energy by the sleep algorithm, and the entire function is coordinated by an adaptive and dynamic scheduling algorithm. For an end-to-end transmission of high efficiency, we need to use location fuzzy cognitive maps and fault detection. It is further discussed that a self-learning based sensor fault detection could be utilized for the monitoring of industrial Internet of Things (IoT). It is proposed that a cloud computing framework be used for providing fault tolerance to the Wireless Sensor Networks (WSN), and a similar effort could be made, for evaluating failures in sensor networks, by incorporating a cloud-based framework. A network management protocol is also envisaged for Wireless Sensor Network (WSN) for managing network failures. The healthcare sector was also considered and a novel architecture was established for fault tolerance and scalability.

It is now discussed about the efforts in counteracting the insider attacks in Internet of Things (IoT) and Distributed Denial of Service (DDoS). For insider attacks, a mechanism could be proposed that would manage the network by the use of a node, that makes continuous monitoring of the network. The maintenance of a dynamic threshold is the mode of working of the proposed algorithm. The view of overall loss of packets in real time make the adjustment of threshold. Due to the loss caused by the false alarm, there is a decrease in the rate of detection. The investigation of the activities of the neighborhood, based on spatial correlation mechanism without any knowledge of malicious sensor, is made by the proposed algorithm. The importance lies in the advance knowledge of sensor, that caused augmented overhead in training, and further causes sufficient strain, where behaviors of attacks are altered dynamically. It may also be proposed that a framework of Intrusion Detection System (IDS) could be allocated to Internet of Things (IoT). This allocated framework comprises of detection engine and monitoring system. There are different categories of framework of Intrusion Detection System (IDS) for Internet of Things (IoT), and also different categories for the conventional Internet. These are necessarily evaluated for Routing Protocol for Low Power and Lossy Networks (RPL).

c) It is necessary to discuss the various ways of ensuring privacy in the applications and networks of Internet of Things (IoT).

Privacy and security requirements of cloud-based Internet of Things (IoT) are privacy of location, privacy of identity, attacks of node compromise, backward and forward security, malicious security of cloud, as well as attacks of adding and removing layers. Presently, study is in progress for analyzing the solutions of privacy- preserving scenarios. After surveying the existing solutions, it may be proposed that the existing modules be translated to a common system model, with study and differentiation with the patterns of behavior of the sensor data. The analyses had revealed that all the applications garner information of time and location. The gathered data is of diverse type, that include audio and video as well. When the latest privacy countermeasures were surveyed, it was observed that potential threats in participatory sensing, result from unrestrained disclosure of personal information to

untrusted persons. The security issues of importance include man-in-the-middle, eavesdropping and other similar attacks, that threaten the integrity and confidentiality, as well as taking control of some components. The most appropriate architecture was identified to be the gateway architecture, for devices that are constrained of resources, and for high availability of systems. It implements the management algorithms on a powerful processor and operates smart home functions, that are critical in nature.

There were other architectures, that were surveyed for Internet of Things (IoT). The most suitable ones are cloud architecture and middleware architecture. The involved technologies for gateway architectures are auto-configuration that augments the security of the system; and automatic system update software and firmware for the maintenance of secure operation of ongoing system. Privacy for Internet of Things (IoT) could also be managed by efficient tagging of data through Information Flow Control (IFC). Here, the tagging of the sensed data is made with the properties of privacy, allowing the access of trusted control, that are based on sensitivity. The tagging is expensive, due to the requirement of resource of Internet of Things (IoT), and as such, necessary policy due to the constraint of resources needs to be framed for tagging. In general, the four properties of applications of Internet of Things (IoT), that are sensitive to privacy, include valuable data sensing, illumination of vulnerable sensors, physical interaction, and distributed implementation, that make the data tag of Information Flow Control (IFC) feasible for the preservation of privacy. Two other properties of this application, are skewed tag and connected operation, that make easier implementation of Information Flow Control (IFC) data tags. The various challenges to the design of security, like shared wireless medium, dynamic network topology, open peer to peer network architecture, and, stringent resource constraints. These challenges build a multi-fence solution of security, that achieves the desired network performance and broad protection. In order to achieve the comprehensive state-of-the-art solution of security, the three security components of prevention, detection, and reaction, need to be encompassed, and both layers should be spanned.

d) The secure forwarding and routing is a very important feature of Internet of Things (IoT).

The applications of Internet-of-Things (IoT) require the deployment of security services, but there are frequent encounters regarding the forwarding and routing of data. The vital requirement is the securing of a routing algorithm for Internet-of- Things (IoT). The state-of-the-art in secure routing established a schematic classification of salient issues of design in routing protocols of Wireless Sensor Network (WSN) and explained the factors of categorization of design for secure routing as optional, essential and basic. A research made on the salient attributes of design, prevention of attacks and security objectives established the latest advancements in the areas of secure routing of Wireless Sensor Network (WSN). The research established a generalized framework with an explicit representation of choices and attributes, along with open feedback. This enabled the users to adapt to the attributes of security in talk terms and run time for similar routes that are calculated on the basis of performance penalties and cost-effectiveness, against official protection in the environment. The research also established an efficient Cost Assurance Routing Protocol (CASER) for Internet of Things (IoT), where the routing is reliant on the geography. It augments the lifetime of network and balances the consumption of energy. The salient feature is that it also sends messages by double- strategy routing, comprising of deterministic routing and random walking.

The distribution of these two strategies is dependent on the requirements of security, and the selection of the two strategies is controlled by the assignment of a variable, that represents the requirements of the security, depending on the cost-effectiveness of the route. The advance security attacks in routing comprise of node capture, where a legitimate node is captured by the attacker, and the cryptographic keys are extracted. The captured node runs the malicious code. The malicious node broadcasts a fraudulent Route Request (RREQ), to the traffic, with an unreal count of hop. The research also proposes that for a secure multi-hop routing for Internet of Things (IoT), multi=layered parameters need to be embedded into the routing algorithm. The suitability of communication for Internet-of-Things (IoT) is confirmed by this algorithm. Efforts are made for the achievement of trust-aware routing algorithm,

where the framework of routing has high ability to resist various attacks, and has the lightweight attribute. The irregular behavior of traffic is detected by the usage of clustering algorithms, necessary for set-up of a model for normal traffic, that could end with irregular behavior of traffic. To boost the efforts of secure routing, proposals are being considered for the detection of dangerous attacks, in the routing of Internet of Things (IoT). It proposes the intrusion detection system for distinguishing the sinkhole attacks of the compromising nodes of the routing services of Internet-of- Things (IoT).

Conclusion

The paper has made discussion and categorization of the state-of-the-work done, for the confirmation of security in the network of Internet-of-Things (IoT).

Comprehensive discussions have been made for lightweight cryptographic framework, resilience and robustness management, provisioning of privacy, denial of service and insider attack detection, as well as secure forwarding and routing. It is concluded that the most vital aspect in the network of Internet of Things (IoT) is privacy, that differentiates it from other Internet networks. It was also discussed that, apart from privacy, there are requirements of lightweight cryptographic primitives, for greater security of the network of Internet of Things (IoT).

Limitations and Future Scope of Research

For lightweight cryptographic primitives, there needs to be limited consumption of resources in the network of Internet of Things (IoT). Lightweight protocols as well as context aware techniques are proposed for preserving privacy, and virtualization techniques need to be used for maintaining the integrity of the data. For implementation of lightweight cryptographic solutions, over Internet of Things (IoT), there could be introduction of centralized routing, offered by Software-Defined Networking (SDN) solutions. Software-Defined Networking (SDN) is virtualization Technology that could centralize the network monitoring and suggest alternative paths for compatible service, and hence this procedure needs to be researched thoroughly.

Reference

1. A. D. Wood and J. A. Stankovic, “A taxonomy for Denial of Service (DoS) attacks in wireless sensor networks,” in *Handbook of Sensor Networks : Compact Wireless and Wired Sensing Systems,* CRC Press, Boca Raton, FL, USA, 2004.
2. A. Samani, H. H. Ghenniwa, and A. Wahaishi, “Privacy in Internet of Things (IoT) : a model and protection framework,” *Procedia Computer Science*, vol.52, pp.606-613, 2015.
3. C. P. Mayer, “Security and privacy challenges in the Internet of Things (IoT).” *Electronic Communication of the European Association of Software Science and Technology-ECEASST*, vol. 17, pp. 1-12, 2009.
4. D. Christin, A. Reinhardt, and M. Hollick, “On the efficiency of privacy- preserving path hiding for mobile sensing applications”, in *Proceedings of IEEE LCN*, Sydney, NSW, Australia, 2013.
5. D. Christin, M. Hollick, and M.Manulis, “Security and privacy objectives for sensing applications in wireless community networks,” in *Proceedings of ICCCN*, pp. 1-6, Zurich, Switzerland, August 2010.
6. D. Juneja and N. Arora, “An ant based framework for preventing Distributed Denial of Service (DDoS) Attack in wireless sensor networks,” *International Journal of Advancements in Technology,* vol. 1, no. 1, pp. 34-44, 2010.
7. D. Moore, C. Shannon, D. J. Brown, G. M. Voelkar, and S. Savage, “Inferring internet Denial of Service (DoS) activity,” *ACM Transactions on Computer Systems*, vol.24, no. 2, pp. 115-139, 2006.
8. F. Liu, X. Cheng, and D. Cheng, “Insider attacker detection in wireless sensor networks,” in *Proceedings of INFOCOM,* pp.1937-1945, Anchorage, AK, USA, 2007.
9. H. Lin and N. Bergmann, “IoT privacy and security challenges for smart home environments,” *Information,* vol. 7, no. 3, p. 44, 2016.
10. J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle,”Privacy in the Internet of Things (IoT) : threats and challenges,” *Security and Communication Networks*, vol. 7, no. 12, pp. 2728-2742, 2014.
11. J. L. Hou and K. H. Yeh, “Novel authentication schemes for Internet of Things (IoT) based

healthcare systems," *International Journal of Distributed Sensor networks*, vol. 11, no. 11, article 183659, 2015.

12. J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT : challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26-33, 2017.
13. K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things (IoT)," *Ad Hoc Networks,* vol. 32, pp. 17- 31, 2015.
14. O. Garcia-Morchon, D. Kuptsov, A. Gurtov, and K. Wehrle, "Cooperative security in distributed networks," *Computer Communications,* vol.36, no. 12, pp. 1284-1297, 2013.
15. P. Pongle and G. Chavan, "A survey : attacks on RPL and 6LoWPAN in IoT," in *Proceedings of International Conference on Pervasive Computing (ICPC),* 2015.
16. R. Kamal, C. S. Hong, and S. Member, "Automatic resilient Internet of Things (IoT) management," 2015, http://arxiv.org/abs/1508.03975.
17. S. Hameed and H. A. Khan, "SDN based collaborative scheme or mitigation of Distributed Denial of Service (DDoS) attacks," *Future Internet*, vol. 10, no. 3, p. 23, 2018.
18. S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things (IoT) : the road ahead," *Computer Networks*, vol. 76, pp. 606-613, 2015.
19. V. Nigam, S. Jain, and K. Burse, "Profile based scheme against DDoS attack in WSN," in *Proceedings of Communication Systems and Network Technologies (CSNT),* pp. 112-116, Bhopal, India, April 2014
20. X. Li, H. Ji, and Y. Li, "Layered fault management scheme for end-to-end transmission in Internet of Things (IoT)," *Mobile Networks and Applications,* vol. 18, no.2, pp.195-205, 2012.