Trust Based Security Mechanisms for Resource-Constrained Internet of Things-A Review

K. Prathapchandran¹ P. Rutravigneshwaran²
¹² Department of Computer Applications, Karpagam Academy of Higher Education (Deemed to be University), Coimbatore-021, Tamilnadu, India

E-mail: kprathapchandran@gmail.com, rutra20190@gmail.com

Abstract. The Internet of Things (IoT) defined as the assembling of real-world objects that are connected over the Internet to make human lives become well-being. The implementation and success of an IoT depend on how it’s secured. But providing security is a critical task because of various natures of IoT devices such as shared and open environment, a wide range of communication protocols, standards, self-organized, lack of central control, heterogeneity of devices, etc. To provide security solutions and mechanisms, key management, cryptographic mechanisms such as private and public-key cryptography, Intrusion Detection System (IDS), and hash functions have been used. Though it is working well, it is not suitable for lightweight IoT devices. Because of such mechanisms always demand high computational, memory, and processing. To overcome these issues, researchers have chosen trust management for providing security. In this article, some of the trust-based solutions have presented. Besides, security issues, security loopholes/attacks in various layers of IoT, security requirements, trust management in IoT, properties of trust, trust management building blocks, the role of trust management in IoT, basic trust calculation methods have presented.

Keywords. Internet of Things (IoT), Security, Attacks and Trust

1. Introduction

The term Internet of Things first coined by Kevin Ashton in the year 1999. Initially, it is called pervasive computing. It has introduced to promote Radio Frequency Technology (RFID). The Internet of Things all about connected devices or objects. The objects categorized into two. One is called physical objects. The other one is called logical or information world or virtual objects. The physical objects are existing in the real world that are capable of sense, actuated, and connected. The logical objects, that are capable of the store, process, and access the real-world information. Therefore, The Internet of Things called IoT is well-defined by “Collection of real-world objects that may be living things or non-living things that are connected through the Internet to provide services to human beings” [1]. Things embedded with both software and hardware parts such as sensors, integrated chips, system-specific components, and applications. Besides, cloud platforms become one of the essential elements for deploying any IoT related applications. The connectivity among the objects or devices might be Person to Person (P2P), Machine to Person (M2P) and Machine to Machine(M2M). Like
ISO/OSI, IoT technology is also has a layering concept. The following figure 1 depicts the five-layering of IoT, the role of each layer and elements involved, and figure 2 the three-layering of IoT.

![Figure 1: The layering Concepts of IoT (5 Layers)](image)

Some highlighted applications are transport, military, telemedicine, agriculture, logistics, etc. [2]. The IoT is also involved with some essential core elements such as heterogeneous access, detection, processing, applications, and administrations. The essential technologies that have involved in the IoT have shown in figure 3.
Figure 2. The Layering Concept of IoT (3 Layers)

Figure 3. Essential IoT technologies

IoT has the following characteristics include open medium, shared wireless medium, self-organized, limited resources, and heterogeneous devices [3]. The characters of IoT depict the figure 4.
The unique features of IoT face numerous challenges such as computational and energy management, memory management, standardization, system architecture, integration, data storage and processing, scalability, environmental issues, privacy, and security [4]. Among the challenges, security is one of the problems because the success of any applications depends on how it can be secured but in this unique environment achieving such security is always a critical task. Based on the survey conducted, secure IoT is all about connected devices and services must have trusted Identities. Owing to, the security of IoT concern with the data, applications, architecture, and communications. All the above factors are affected by threats in terms of various security attacks.

Achieving security in IoT is a complicated task because of various reasons. The first and foremost reason is the resource-constrained nature of devices involved in the IoT. Those devices are limited in their processing, memory, computational and speed compare with other devices. For instance, an electronic IoT sensor embedded wristwatch has used to monitor the patient in the healthcare sector. Typically, those devices are small in size. To provide security, applying complex algorithms in those devices impossible. So, concerning security in those devices becomes difficult. Besides, the manufacturer of the IoT devices has been concentrating on the application part of the IoT devices. They are not in the security part of those devices. Then, the dynamic nature of the IoT environment also leads to security violations because devices are roaming here and there. They can join and leave the network at any time. In this situation, a proper security mechanism to be needed to handle the dynamic nature. Also, IoT devices have located in an open and shared environment. Therefore, there is a possibility of physical damage that leads to security violations. The information which is transferring among the devices through the wireless medium. By default, wireless mediums are susceptible to various kinds of attacks and these open and shared environment leads to more security violations.

To enhance security, various security mechanisms have been proposed. Cryptographic techniques, key management, digital signatures, hash functions, Intrusion Detection System (IDS), Zero Knowledge Proof, Artificial intelligence, and most recently the blockchain technologies have been using. The above techniques are effective but it cannot be applied to lightweight devices which are involved in the IoT environment as it demands high processing, memory, and computational capabilities. To address these issues, trust management is playing a major role at present. Researchers have witnessed the impact of trust management in the IoT environment. Trust management deals with all kinds of security such as information security, device security, and network security. Because of such popularity, in this article, we are focusing on trust-related security mechanisms for resource-
constrained IoT devices.

The remainder of the article is composed as follows: Section 2, deals with security in IoT, following that security issues, security issues at various layers and security requirements have discussed Section 3, deals with an introduction to IoT, properties of trust, trust-building blocks, trust level, and trust computational methods Section 4, deals the trust-based security mechanisms and the final section concludes.

2. Security in IoT
The following sections discuss the security issues in IoT, security requirements of IoT, security attacks at various layers of IoT, the importance of security in the IoT environment, and the architecture of IoT with respect to security concerns.

2.1 Security issues in IoT
As discussed earlier, the main security issues that arise from the IoT is a resource-constrained heterogeneous environment and the interconnection of networks through the open environment. These two factors lead the conventional security issues. The constrained nature means limited resources in memory, processing, and computational capabilities [4]. Granja et al., 2015 [5] recently surveyed that security issues also arise in terms of data, application, communication, and architecture. Granja et al.,2015 [5] also witnessed the security issues come in IoT protocols. Cloud computing is also playing a major role and it incorporated with IoT hence security issues also come in cloud platforms and it is witnessed by [6]. Unique identification objects, software that is used in IoT applications, and malware also identified as a platform for security violations [7]. The project called OWASP-Open Web Application Project elaborates on the vulnerabilities involved in the IoT environment. The vulnerabilities are devices involved insure environment, insecure of software and malware, unsuitable security configuration.

2.2 Security issues at various layers of IoT
The layers in IoT are divided into three major categories such as perception layer or sensing layer, middleware layer, and application layer. The layering concept of IoT is depicted in the following figure.1. Security issues are raised in all the above layers of IoT. The issues should be addressed at the initial stage of IoT application design or at the regular interval of time. Though the designers of IoT take care of everything in all the aspects of security, security violations till existing and all the layers of IoT are get affected.

2.2.1. Security problems at Perception/Sensing Layer
This layer interacts with the outside environment through sensors, Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), and other devices. The most common threats discuss herein.

2.2.1.1 Denial of Service Attack (DoS) [8]
This is one of the commonly faced attacks in the network environment. The aim is to network resources that become unavailable to legitimate users and exhaustion the resources of legitimate users by sending wrong network information to other legitimate devices and got the attention of them.

2.2.1.2 Replay Attack [8]
This attack executed by sending former messages again and again to the destination node by the way it tries to compromise the network and authenticated services.

2.2.1.3 Node Capture Attack [8]
An attacker will capture the node/device which is in the network environment and steal the confidential information from them. Besides, those devices may be compromised so it will disclose the confidential information of other nodes and itself.
2.2.1.4 Fake node [8]
Due to the nature of the open environment, a fake node may be injected by an attacker. Therefore, the fake node may act as a legitimate node and circulate the wrong code or information over the network. The result is the entire network becomes damaged.

2.2.1.5 Jamming attack:[9][10]
In this attack, an attacker makes use of radiofrequency signal and emitting to other devices in the network without followed by the protocol specification. Such interferences affect the network operations means sending and receiving of information. The result is an unpredictable working nature of the IoT system.

2.2.1.6 Insecure installation [11][12]
The insecure installation also leads to improper function of IoT systems. Therefore, attention to be taken while installing and configuring security mechanisms. Insecure communication is also needed to be addressed to ensure secure communication.

2.2.1.7 Sleep deprivation attack [13]
This attack is executed by staying awake the sensor nodes while it is not functioning by the way their battery power gets drained and would not involve in the subsequent process.

2.2.1.8 Sybil attack [14]
An attacker makes use of fake identifies and gets into the network environment and will degrade the functionality of the entire system.

2.2.1.9 Insecure physical [15]
The poor security nature of the IoT environment leads to security loopholes and becomes a threat to the functionality of the IoT environment. Software access can be done through the insecure wireless environment and it may be exploited to legitimate devices’ testing and debugging tasks.

2.2.2. Security problems at Middleware Layer
Heterogeneity nature means to network and application devices involved here are having to vary in their resources. Different protocols and technologies are used here. So, maintain the coordination among is always a difficult task hence it leads to security violations. Another issue in this layer is scalability. Depends on the application nature number of devices involved in IoT may increase. In addition, a new device may join and leave at any time. Therefore, this dynamic nature leads to security violations. Most importantly, an attacker makes use of the social engineering concept to collect sensitive information from the IoT environment so the security of IoT becomes in question. Thus, middleware security issues mainly concentrate on routing, communication, and session management of IoT. The following attacks are mostly affecting the middleware layer of IoT.

2.2.2. 1.Insecure neighbor discovery [16]
In IoT, the route discovery process will execute prior to the actual data transmission happen. This is happening to find out the secure route to the destination. Here, an attacker may make use of the route discovery process and can inject false routing information and it leads to misguide to legitimate users.

2.2.2. 2.Sinkhole attack [17]
In this attack, an attacker responds quickly to the route request compare with ordinary nodes and get attention. Thereafter the nodes who want to transmit packets to other nodes make use of this sinkhole attack by the way all the incoming packets routed via this route may be dropped.
2.2.2. 3. **Work hole attack** [18]
This attack will execute by creating a tunnel between two nodes. So the packets which are transferred via this tunnel is dropped.

2.2.2. 4. **Buffer reservation attack** [19]
Usually, nodes in the network make use of buffer space to re-assemble the incoming packets. Here, an attacker will send incomplete packets to the victim node and increase the buffer size by sending unwanted packets. The result may be the denial of service to legitimate users due to the space occupied by the spoofed packets.

2.2.2. 5. **Sybil attack** [20][21]
In a Sybil attack, an attacker makes use of fake identities to communicate with other nodes. The result of these attacks may lead to various security violations such as disseminating malware, spamming, and phishing attacks.

2.2.2. 6. **Blackhole attack** [22]
In this attack, an attacker advertises itself that is having the shortest path to the destination. By advertising this, it will get attention from others. Hence, the packets transmitted via this node may be dropped.

2.2.2. 7. **DDoS attack** [8]
An attacker will send too many empty/spoofed messages to the target node. By processing those packets, the target node may drain their energy and become unavailable to legitimate users. This is called denial of service attack. If the attack can be launched by more than one attacker, it is called a distributed denial-of-service attack.

2.2.2. 8. **Privacy attack on Cloud** [23]
Cloud services are being acted as a service provider between two nodes. In this case, a malicious cloud provider may act as a genuine provider and steal confidential information to be transmitted to others.

2.2.2. 9. **Session Hijacking attack** [24][25]
An attacker may impersonate the victim node and inject it between two legitimate nodes. The conversation between these two legitimate nodes hacked by an attacker. This attack normally happens in the transport layer.

2.2.2.10. **RPL attack** [26]
The routing protocol for Low Power Lossy Network (RPL) is currently and mostly used protocol in IoT applications. Due to a lack of security mechanisms in the design of protocol itself, it may be affected by various security threats. The result will lead to denial of service attacks and eavesdropping.

2.2.3. **Security problems at Application Layer**
This layer deals with end-user applications. IoT is used in various applications and each application is having a variety of end-users. Each user is having different access privileges to ensure the right access privilege proper authentication mechanism is needed. Along with users, data privacy also needs to take care of. A complex and huge data processing algorithm is needed to handle the huge volume of data. Besides, application-specific vulnerabilities are also there because the security mechanism is suitable for one application may not suitable for other application. Some of the notable attacks are discussed herein.
2.2.3.1. Uncertain interface [25]
To effectively access the IoT services, the platform such as web, mobile, cloud, and other services are used. Those platforms must be protected from unauthorized access to ensure data privacy.

2.2.3.2. Insecure software [26]
The codes which are used for developing IoT platform need to be tested and executed carefully. The codes are HTML, XML, XSS, MQTT, and others. There is a possibility of malicious codes may inject into this code.

2.2.3.3. Device heterogeneous [27][28]
IoT environment is incorporated with various devices and those devices are heterogeneous in nature. So, to provide collaborative IoT service, those devices need to cooperate without compromising any security loopholes.

2.2.3.4. CoAP security violations [28][29]
CoAP called as Constrained Application Protocol especially developed for constrained devices in the IoT environment. It supports web transfer so proper encryption mechanism is needed to safeguard this protocol. The open and shared architecture of IoT leads to security violations on this protocol.

2.3 Security requirements of IoT
In IoT, data will be shared from devices to devices, devices to users, and vice versa. Shared data must be transferred securely without any loss or modification. To secure the IoT environment, various security requirements are needed and these requirements must meet by any applications. Then only we can say, the IoT environment is secured. The security requirements are [30][31]. Figure 5 shows the security requirements of IoT.

2.3.1 Authentication
Due to the heterogeneous nature of IoT, every device in the environment must trust other devices with a proper authentication mechanism. It is defined as “a device ensures the identity of other devices with which it is communicating”. It ensures the initial level of security and it can be achieved in two ways such as pre-authentication and post-authentication.

2.3.2 Authorization
Due to the open and shared environment of IoT, a proper authorization mechanism is needed to ensure the right access to the devices as well as information. Simply, only authorized users are allowed to access.
2.3.3 Accounting
To maintain consistency, accountability to be needed. It monitors the usage of available network resources as IoT poses resource-constrained devices. Besides, it also deals with auditing, reporting, and monitor the utilization of resources and devices.

2.3.4 Data Privacy
It ensures the data which has shared in the IoT environment that has used for the intended purpose. Alternatively, it ensures the right of individual users and how their information is collected and used by users.

2.3.5 Confidentiality
IoT involved with the diverse nature of services and devices. Data will travel through multiple hops hence there is a possibility of data that will disclose to unauthorized access. It should not happen since it has sensitive information.

2.3.6 Integrity
While data travel from one place to another place, the data should not alter/modify by unauthorized users. It ensures the reliability of the data which is stored.

2.3.7 Availability of Services
There is a possibility of denial of service by IoT participating devices as they drain their resources due to environmental nature. It ensures all-time availability of resources through denial of service occurs.

2.3.8 Energy efficient
IoT devices should be energy efficient at all times. The process of forged services and requests for redundant services leads to energy consumption.

2.3.9 Single point of failure
Due to heterogeneous and dynamic natures of IoT devices, failure of hardware and software may happen at any time in the network. To address such issues, alternative solutions to be needed with a tamper-proof and fault-tolerant environment.

3. Trust Management in the Internet of Things
Balze et al., 1996[32] introduced the trust management. It derived from social science. The definition is “the trustor is ready to depend on another trustee” [32]. The concept of trust has been using in various fields which shows in figure 6. According to the networks and communication field, trust defines as “a combination of relationships among devices that take part in the protocol constructed on the earlier communication of devices within the protocol [33-35]”. Trust has used as a core concept for decisions on the network and communication field included authentication, Intrusion Detection System (IDS), Key Management, Access Control, Identifying malicious behavior, and more [36].

![Figure 6 Trust in Multiple disciplines](image)

3.1 Properties of Trust
The following section discusses the properties of trust. There are five essential properties which show in figure 7.

3.1.1 Dynamic
Because of the dynamic nature of the IoT environment, trust relationships among the participating devices will change often. Hence, it is harder to predict the trust value of one device with respect to another device. Besides, as IoT supports scalability, the new device can join or old devices can leave from the IoT environment at any time [37].
3.1.2. Subjectivity
IoT has different types of devices and it offers different services to different users. Because of this heterogeneity nature, devices in IoT might have the same level of trust with respect to other devices. Every device has different communication experiences with other devices [38].

3.1.3. Transitive
For instance, if device d1 trusts device d2, device d2 trusts device d3 simultaneously device d1 need not require to trust device d3. In this case, the transitivity between device d1 and device d3 or device d1 trusts in the device d3’s reference of the third parties [39].

3.1.4. Asymmetric
Due to the heterogenicity nature, the devices are varying in terms of their resources such as memory, bandwidth, battery, processing, and computational. Therefore, the device who is having high capacity may not trust the device who is having the lowest capacity and vice versa [39].

3.1.5. Context-dependent
A device with high computational power considered as a trusted device and the device with the low computational power is untrusted but it is not malicious [40].

3.2 The role of Trust in IoT
The main motivation of using trust in IoT is, conventional cryptographic methods always involved with computational overhead in terms of executing and processing the algorithms. Moreover, they always in need of a trusted third party, and based on key management this leads to an increase in computational overhead again and will decrease the performance of the IoT environment. The result is achieving performance metrics such as throughput, robustness and availability are in question [Wei Gong et al., 2009]. Most importantly, IoT environment compromises of various smart devices, and these devices are human-related devices or human carried devices hence social relationship among the human also considered in terms of their ownership, friendship, and community. Ownership denotes the human own devices. Friendship denotes the cooperation or friends among themselves and community denotes the devices involved in IoT are belong to some communities. To handle these types of social
relationships between the communicating devices conventional cryptographic methods are not suitable. To solve these problems, trust management has introduced.

3.3 Trust Management building blocks
The following section discusses the trust management building blocks. It consists of various entities such as trust computation, trust propagation, trust aggregation, trust prediction, and trust applications [41]. The following figure 8 depicts the trust management building blocks.

![Figure 8 Trust management building blocks](image)

### 3.4 Trust level
Trust level has defined by the trust possibility of trustor regarding trustee i.e whether the trustee performs by way of predictable or not in the opinion of the trustor. The trust level is varying from 0 (complete distrust) and 1 (complete trust). Figure 9 depicts the trust level.

### 3.5 Basic methods of Trust Computations
There two basic methods are used to compute the trust first one is, direct trust and another one is indirect trust. Both the trusts will be calculated either in a centralized manner or a decentralized manner. Sometimes a hybrid approach that means the combination of both direct and indirect trusts will be used [41]. If the trust metrics have calculated from the immediate devices, that trust will be named as direct trust. If the trust metrics are calculated based on the recommendation from others means not direct evaluation, that trust is called indirect trust. If combine both direct and indirect, that metric is called hybrid trust. Anyone of these trust metrics will be followed during the trust computation. The following figure depicts the trust evaluation.
4. Trust Based Security Schemes
The following section discusses the trust-based security schemes for the IoT environment.

| S.No | Authors | Security issues/Objectives | Attacks | Proposed Solutions |
|------|---------|-----------------------------|---------|--------------------|
| 1    | F. Bao et al., 2012 [42] | Breaks the basic functionality of Internet of Things | Bad-mouthing, self-promoting, good-mouthing | Direct trust, indirect trust, social relationship such as cooperativeness, honest, community interest |
| 2    | M. Nitti et al., 2012 [43] | Misleading other nodes by make use of services for illegal purpose | Malicious activity | Repudiation based trust mechanism, social relationship among the devices |
| 3    | L. Gu et al., 2014 [44] | Routing process is affected by compromised nodes | Malicious behavior | Semantic based, fuzzy set theory |
| 4    | Y.-B. Liu et al., 2014 [45] | Misbehaving activity by malicious nodes over the routing protocol | Malicious behavior | Recommended trust, history statistical trust and bayes algorithms |
| 5    | Yefeng Ruan et al., 2016 [46] | To analysis and reduce the error rate in IoT based food nutrition analysis | Sinkhole attack | Packet forwarding success rate, confidence, measurement theory |
| 6    | Liang Liu et al., 2019 [47] | To increase the detection ratio by avoiding collaborative attacks in routing process | tamper attack, drop attack and replay attack | Perceptron and K-means method, |
| 7    | Noshina | Malicious | Black hole and grey hole | Forwarding behavior of |

Figure 9. Trust Level
5. Conclusions and Future Direction

As IoT environment compromises of heterogeneous devices, proper security mechanisms to be needed to ensure the security of the environment. The security mechanisms which are proposed by various researchers are not suitable for all the applications. Because of each application varies in terms of their processing, computational, nature of work, utilization of memory, and other capabilities. With this idea in mind, this review article focused on trust-based security mechanisms that are suitable for lightweight applications, and devices involved in this environment are always resource-constrained. This paper discussed some of the substantial works towards trust-based security mechanisms in the IoT environment. Before this, security associated things such as security issues in various layers of IoT, attacks that are affected the layers of IoT, requirements of security, finally, the core concepts of trust management and its role in IoT environment have discussed. In the future, the research work will be focusing on the Distributed Denial of Service (DDoS) attack over the Internet of Things based military environment. Therefore, the trust-based solution will be implemented to address the DDoS attack by the way the security of Military based IoT will be ensured.

Acknowledgement

This research work is supported by Karpagam Academy of Higher Education (Deemed to be University), Coimbatore – 641 021, Tamilnadu, India, through a Seed Money Project.

References

[1] C.H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in Internet-of-Things sensory environments, Ad Hoc Netw. 18 (Suppl. C) (2014) 85–101. http://dx.doi.org/10.1016/j.adhoc.2013.02.008.

[2] D.U. Sinthan, M.-S. Balamurugan, Identity authentication and capability based access control (IACAC) for the Internet of Things, J. Cyber Secur. Mob. 1 (4) (2013) 309–348.

[3] J. Granjal, E. Monteiro, J.S. Silva, Network-layer security for the Internet of Things using TinyOS and BLIP, Int. J. Commun. Syst. 27 (10) (2014) 1938–1963. http://dx.doi.org/10.1002/dac.2444.

[4] Minhaj Ahmad Khan a, Khaled Salah b, 2018. “IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems” pp.82 -395–411.
[5] J. Granjal, E. Monteiro, J.S. Silva, 2015, “Security for the internet of things: A Survey of existing protocols and open research issues”, IEEE Commun. Surv. Tutor. 17 (3) -1294–1312. http://dx.doi.org/10.1109/COMST.2015.2388550

[6] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, 2017, “Security and privacy for cloud-based IoT: Challenges”, IEEE Commun. Mag. 55 (1) pp.26–33. http://dx.doi.org/10.1109/MCOM.2017.1600363CM.

[7] Z.K. Zhang, M.C.Y. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, S. Shieh, 2014, “IoT security: Ongoing challenges and research opportunities”, IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234. http://dx.doi.org/10.1109/SOCA.2014.58

[8] Z. Yang, et al., Study and application on the architecture and key technologies for IOT, in: Proc. ICMT, 2011, pp. 747–751

[9] W. Xu, W. Trappe, Y. Zhang, T. Wood, 2005, “The feasibility of launching an detecting Jamming attacks in wireless networks”, Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc” 05, ACM, New York, NY, USA, pp. 46–57. http://dx.doi.org/10.1145/1062689.1062697.

[10] G. Noubir, G. Lin, 2003, “Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob”. Rev. 7 (3) 29–30.

[11] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, 2014, “Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone”, Trans. Info. for. Sec. 9 (10)1617–1628. http://dx.doi.org/10.1109/TIFS.2014.2341453.

[12] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, 2013, “Enhancing physical-layer secrecy in multiantenna wireless networks: An overview of signal processing approaches”, IEEE Signal Process. Mag. 30 (5) pp.29–40

[13] T. Bhattasali, R. Chaki,2011, “A survey of recent intrusion detection systems for wireless sensor network”, Advances in Network Security and Applications: 4th International Conference, CNSA, Chennai, India, July 15–17, Springer.

[14] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, 2009, “Channel-Based detection of sybil attacks in wireless networks”, IEEE Transa. Inf. Forensics Secur. 4 (3) pp. 492–503.

[15] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index. Php/Top_IoT_Vulnerabilities.

[16] R. Riaz, K.-H. Kim, H.F. Ahmed, 2009, “Security analysis survey and framework Design for IP connected LoWPANs”, “International Symposium on Autonomous Decentralized Systems”, pp. 1–6. http://dx.doi.org/10.1109/ISADS.2009.5207373.

[17] K. Weekly, K. Pister, 2012, 6LoWPAN Fragmentation attacks and mitigation mechanisms, “Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks”, pp. 55–66. http://dx.doi.org/10.1145/2462096.2462107.

[18] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 2013, 6LoWPAN Fragmentation attacks and mitigation mechanisms, “Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks”, pp. 55–66. http://dx.doi.org/10.1145/2462096.2462107.

[19] K. Zhang, X. Liang, R. Lu, X. Shen, 2014, “Sybil attacks and their defences in the Internet of things, IEEE Internet Things J. 1 (5)–372–383.

[20] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, B.Y. Zhao, 2013, “Social turing tests: Crowdsourcing sybil detection, Symposium on Network and Distributed System Security”, pp.13-18
[22] S. Sivagurunathan and K. Prathapchandran, “A Centralized Trust Computation model for secure group formation in Military based Mobile Ad Hoc networks Using Stereotypes”, Advances in Intelligent Systems and Computing, Springer, Vol.412, pp.427-438, 2015.

[23] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos, 2017, “Security and privacy for cloud-based IoT: Challenges, IEEE Commun. Mag. 55 (1) pp.26–33.

[24] N. Park, N. Kang, 2016, “Mutual authentication scheme in secure internet of things technology for comfortable lifestyle”, Sensors 6 (1) pp.20–20.

[25] M.H. Ibrahim, 2016, “Octopus: An edge-fog mutual authentication scheme, Internat. J. Netw. Secur”. 18 (6) (2016), pp. 1089–1101.

[26] A. Dvir, T. Holczer, L. Buttyan, 2011, “VeRA - version number and rank authentication in RPL”, IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 709–714. http://dx.doi.org/10.1109/MASS.2011.76

[27] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M.A. Spirito, 2012, “The VIRTUS middleware: An XMPP based architecture for secure IoT communications”, ‘21st International Conference on Computer Communications and Networks’, ICCCN, 2012, pp. 1–6. http://dx.doi.org/10.1109/ICCCN.2012.6289309.

[28] J. Granjal, E. Monteiro, J.S. Silva, 2013, “Application-layer security for the WoT: extending CoAP to support end-to-end message security for internet-integrated Sensing applications”, “International Conference on Wired/Wireless Internet Communication”, Springer Berlin Heidelberg, pp. 140–153.

[29] M. Sethi, J. Arkko, A. Kernen, 2012, “End-to-end security for sleepy smart object Networks”, 37th Annual IEEE Conference on Local Computer Networks- Workshops, pp. 964–972. http://dx.doi.org/10.1109/LCNW.2012.6424089.

[30] S. Sicaria, A. Rizzarelli, L.A. Greco, A. Coen-Porisini, 2015. “Security, privacy and trust in Internet of Things: The road ahead”, Computer Networks . pp.76 -146–164

[31] William stalling, 1996, “Cryptography and network security”.

[32] Blaze M., Feigenbaum J., Lacy J., 1996, “Decentralized trust Management, Proceedings of IEEE Symposium on security and Privacy”, pp. 164-73.

[33] Mayer R C., Davis J H., Schoorman F D., 1995, “An Integrative Model of Organizational Trust- Academy of Management Review”, Vol. 20 (3), pp. 709-734.

[34] Bamberger, Walter, 2010, Interpersonal Trust – Attempt of a Definition, Scientific report.

[35] Baras J S., Jiang T., 2005, “Managing Trust in Self-Organized Mobile Ad Hoc Networks”, Proc. 12th Annual Network and Distributed System Security Symposium Workshop.

[36] Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen, 2011, “ A Survey on Trust Management for Mobile Ad Hoc Networks”, IEEE communications surveys & tutorials, Vol. 13(4),pp.562-583.

[37] Schenauer L., Gligor V D., and Baras J., 2002, “On Trust Establishment in Mobile Ad Hoc Networks”, 10th Int‘l Security Protocols Workshop, vol. 2845, pp. 47-66.

[38] Abdul-Rahman A., Hailes S., 1997, “ Using Recommendations for Managing Trust in Distributed Systems”, Proc. IEEE Malaysia Int’l Conf.on Communication.

[39] Adams W J., Hadjiichristofi G C., Davis N J., 2005: “Calculating a Node’s Reputation in a Mobile Ad Hoc Network”, Proc. 24th IEEE Int’l Performance Computing and Communications Conference, pp. 303-307.

[40] Staab S., 2004, “The Pudding of Trust, IEEE Intelligent Systems”, vol. 19(5), pp. 74-88.

[41] Kannan Govindan, Prasant Mohapatra, 2012, “Trust Computations and Trust Dynamics in Mobile Ad hoc Networks,-A Survey”, IEEE Communications Surveys & Tutorials, Vol.14 (2), pp.279-298.
[42] F. Bao, I. Chen, Dynamic trust management for internet of things applications, in: Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, Self-IoT ’12, USA, San Jose, 2012, pp. 1–6.

[43] M. Nitti, R. Girau, L. Atzori, A. Iera, G.Morabito, A subjectivemodel for trustworthiness evaluation in the social internet of things, in: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC, Australia, Sydney, 2012, pp. 18–23.

[44] L. Gu, J. Wang, B.b. Sun, Trust management mechanism for internet of things, China Commun. 11 (2) (2014) 148–156.

[45] Y.-B. Liu, X.-H. Gong, Y.-F. Feng, Trust system based on node behavior detection in internet of things, Tongxin Xuebao/J. Commun. 35 (5) (2014) 8–15.

[46] Yefeng Ruan, Arjan Durresi, Lina Alfantoukh, Trust Management Framework for Internet of Things, 2016 IEEE 30th International Conference on Advanced Information Networking and Applications, 1550-445X/16 $31.00 © 2016 IEEE, pp. 1013-1120

[47] Liang Liu a, Zuchao Maa, Weizhi Meng b, Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks, Future Generation Computer Systems 101 (2019) 865–879

[48] Noshina Tariqa, Muhammad Asima, , Zakaria Maamarb, M. Zubair Farooqia, Noura Facic, Thar Bakerd, A Mobile Code-driven Trust Mechanism for Detecting Internal Attacks in Sensor Node-powered IoT, journal of parallel and distributed computing August 18, 2019

[49] Mohamed Tahar Hammi a, b, Badis Hammi a, *, Patrick Bellot a, b, Ahmed Serhrouchni, Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, computers & security 78 (2018) 126–142

[50] Lin, Z., Dong, L., 2018. Clarifying trust in social internet of things. Feb IEEE Trans. Knowl. Data Eng. 30 (2), 234–248, https://doi.org/10.1109/TKDE.2017.2762678 ISSN 1041-4347.

[51] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, 2017,” Internet of things security: A survey”, J. Netw. Comput. Appl. 88 (Suppl. C).pp. 10–28.