International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 4, August 2018, pp. 2319~2326
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i4.pp2319-2326

A Comprehensive Survey on Exiting Solution Approaches towards Security and Privacy Requirements of IoT

Rajani Chetan[1], Ramesh Shahabadkar[2]
[1]Department of Information Science, Maharaja Institute of Technology, Mysore, India
[2]Department of Computer Science and Engineering, Vardhaman College of Engineering, Shamshabad, Kacharam, Hyderabad, India

Article Info

Article history:

Received Sep 25, 2017
Revised Jan 15, 2018
Accepted Jan 22, 2018

Keyword:

Intenet of things
Privacy preservation
Security
Sensor network

ABSTRACT

*'Internet of Things (IoT)'*emerged as an intelligent collaborative computation and communication between a set of objects capable of providing on-demand services to other objects anytime anywhere. A large-scale deployment of data-driven cloud applications as well as automated physical things such as embed electronics, software, sensors and network connectivity enables a joint ubiquitous and pervasive internet-based computing systems well capable of interacting with each other in an IoT. IoT, a well-known term and a growing trend in IT arena certainly bring a highly connected global network structure providing a lot of beneficial aspects to a user regarding business productivity, lifestyle improvement, government efficiency, etc. It also generates enormous heterogeneous and homogeneous data needed to be analyzed properly to get insight into valuable information. However, adoption of this new reality (i.e., IoT) by integrating it with the internet invites a certain challenges from security and privacy perspective. At present, a much effort has been put towards strengthening the security system in IoT still not yet found optimal solutions towards current security flaws. Therefore, the prime aim of this study is to investigate the qualitative aspects of the conventional security solution approaches in IoT. It also extracts some open research problems that could affect the future research track of IoT arena.

Corresponding Author:

Rajani Chetan,
Department of Information Science,
Maharaja Institute of Technology, Mysore, India
Email: rajanichetanvtu1@gmail.com

1. INTRODUCTION

The widespread wireless communication has broadened its scope of applicability for the extended use of internet. IoT interlinks the cyber world to the physical systems by connecting the world community of users. IoT systems provide connectivity and interactive communications over anything such as physical objects like sensors or actuators connect to the internet with unique addresses [1], [2]. The physical objects transmit their data to cloud-enabled platforms through wired/wireless channels for the further interpretation. The physical objects connected to a data-driven IoT do not require human intervention to operate on different input parameters, it is well capable of understanding the complexity of environments when needed. Their mode of operations also defined in a way where sensors or actuators will react to the environmental changes due to their in-built feature of sense and communications. The revolutionary advancement of physical objects enhanced their capability and wide adoption into IoT networks. In futuristic IoT enabled applications, the long-term vision of network engineers is to connect every possible device used in daily life, to the internet. Mobile phones will be used as an intermediate remote controller for all the objects deployed into physical world commonly termed as IoT. A study introduced by the author Gartner [3] stated that in future the number of connected devices to the internet will increase from around 25 billion to 50 billion by 2020. At that point

of time enormous data generated from different IoT enabled physical devices will become vulnerable to malicious attacks. Therefore, it is clear that pervasiveness of such big network results security threats that allows attackers to steal even more personal information about users or some reputed organization who are connected to the IoT systems. An overview of full-fledged IoT architecture is presented in Figure 1 below:

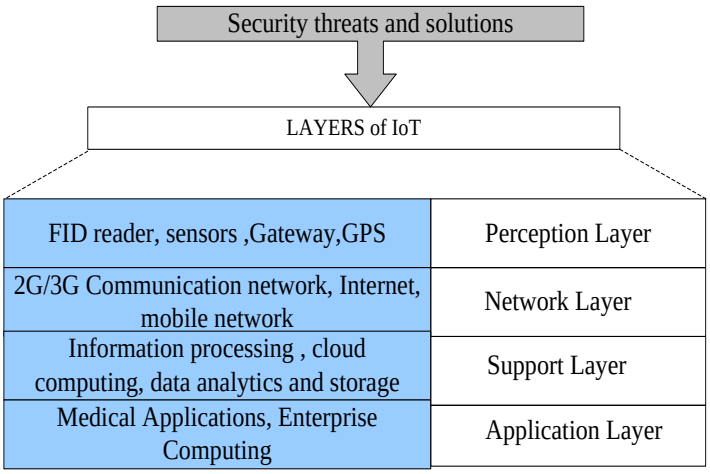

Figure 1. Overview of IoT Layers

The security concerns in IoT become a notable fact to strengthen the futuristic internet oriented systems. The prime reason to give more emphasize on security aspects regarding IoT technologies are as follows:

a. The IoT enabled data computing is an extended version of conventional internet which uses the technologies like wireless sensor network (WSN), mobile broadband and 2G/3G communications. The operational and design constraints associated with these technologies already induce various security flaws.
b. As IoT is interconnected with the existing layers of conventional internet thus naturally, it becomes unsecured environment where information sharing could easily gain the attention of an attacker. Intruders look for various system breaches and perform remote code execution to steal valuable information.
c. Objects deployed in IoT enabled networks interchange messages thus there is a possibility in which privacy and security can be threatened [4], [5].

The proposed study intends to perform an investigational survey to bring out the effectiveness of the existing security protocols towards safeguarding IoT systems. It also provides various security requirements and challenges encountered during the implementation of IoT on the top of conventional internet. The study also emphasized on presenting various security threats, and related solution approaches proposed till date using making the futuristic IoT more optimistic and secure [6]. The key solution aspects and their notable contributions also extensively discussed. The paper is organized as follows. In section 1.1 the background of the existing works is briefly discussed along with a brief insight into the current research problems identified in Section 1.2 which is followed by existing solution approaches in Section 1.3. Section 2 extensively discusses the existing security threats in IoT systems where Section 3 presents the conventional security solution approaches. Finally, section 4 briefly talks about the existing research issues and Section 5 briefs the conclusion.

1.1. Background

This section briefly introduces the conventional studies exclusively carried out to address the security flaws encountered in IoT based applications and services. As IoT is a completely new trend which revolutionizes the internet, hence there exist very few existing manuscripts available which talk about its extensibility and interoperability issues in an inherently distributed nature. Instead of discussing various manuscripts which address various security issues in IoT, the proposed survey only discusses two of the most significant studies reported security flaws of cloud-based IoT and also addressed the inappropriateness of most existing works. The study of Zhou *et al.* [7] addressed the issues about secure packet forwarding and efficient privacy preserving authentication during data aggregation in cloud-based IoT. It also analyzed the

privacy requirements for the next generation mobile technologies and finally the study extracted interesting existing open research problems and also suggested promising ideas to trigger more research efforts in the area of IoT. A closer look into the study of Leloglu *et al*. [8] listed various opportunistic aspects of data-driven IoT applications and also at the same time highlighted the fact that many existing surveys works strongly emphasized on the centralization of data in cloud and big data analysis which also follows the paradigm of high-performance parallel computing. However, there exists a possible trade-off which makes bandwidth and energy limited during the high-performance computing paradigm for transmission and processing of raw data. The privacy concern during data delivery mostly invites the communication constrained scenarios. The study also presented an extensive analysis of conventional IoT architectures where the more emphasize put towards highlighting security requirements and challenges common in IoT implementations. It also provides a discussion on the existing security threats and related solutions corresponding to each layer of IoT architecture.

1.2. Research problem

The advancement of fast-growing computing technologies making wireless communication systems operationally more challenging. In this new era of (IoT), digitally connected objects have become more superior and implicate their applicability into every aspect of our lives including our homes, office, cars and even in our bodies. The fast-growing IoT enables advent of IPv6 and wide deployment of Wi-Fi networks. According to the statistical analysis for futuristic IoTs depicts that by the period of 2020 the number of connected physical devices to the Internet will raise up to 40 billion [9], [10]. The number of connected physical devices to the IoT networks become susceptible to malicious attacks and an attractive target for cyber criminals. The number of networked devices allows attackers to plan their attack vectors which invite possibility of inevitable disaster in future. Therefore security issues in IoT should be a vital concern in the recent times. Although there exist a series of efficient security protocol stacks which emphasized mostly on cryptography based security aspects and it leads to high cost of computation in low power devices like sensors and actuators. Therefore, the security measurement matrix should be inclined towards balancing a trade-off between low cost of implementation and high-level security in IoTs.

2. EXISTING SECURITY THREATS IN IoT SYSTEMS

This section mostly focused on the existing security threats being encountered during the implementation of cloud-based IoT. Various security threats encountered during packet forwarding with outsourced aggregated transmission evidence generation. The security requirements for existing IoT considers traditional data confidentiality and unforgeability a backbone of countermeasure, apart from these other unique security and privacy requirements are as follows:

a. Identity Privacy: It refers to a conditional privacy requirement where a matter of fact should be approved which states that the mobile users who are connected to the IoT systems must be well protected from revealing their identity to the public. However, an uncertain occurrence of dispute in an emergency case must notify the authority about it so that they can trace it properly [11].
b. Location Privacy: Location privacy seems to be a critical concern for IoT systems as frequently visited location and coordinates can reveal about living pattern associated with an IoT user. The current investigational study mostly found pseudonyms as a widely adopted technique for location hiding. But the periodically updating of pseudonyms and certificates results in a computationally challenging situation which affects the throughput of the IoT networks. As the location information is not meant for direct protection thus, it becomes an attractive target for physically dynamic tracing attack. If an attacker track down a mobile object that having pseudonym P_{ID} frequently visits n number of location loc_1 loc_2 loc_3 ….. *loc*ation it can reveal the real identity of the object considering attacking vectors. The prime target is to track down the identity of an object and its private activities over different regions [12].
c. Node Compromise Attack: It refers to the point of the situation when adversary formulates a programmatic pipeline to extract meaningful information form a resource constrained IoT device. During this attack, the attacker mostly captures all the private information along with the secret key used for encrypting a packet and the private key to generate signatures. Further, the attacker reprograms the IoT node and makes it a malicious one which works under the control of adversary [13], [14].
d. Layer Removing/Adding Attack: It occurs when a group of selfish IoT nodes removes their intermediate forwarding layers just to maximize their rewarded credits. The attackers' policy is to minimize the intermediate transmitters which share the rewards.
e. Forward and Backward Security: The forward-backward security is also an essential requirement to streng then up the IoT communication paradigm during the mobility and dynamic group formulation [15].

f. Malicious Cloud Security: The integrated convergence of cloud with IoT especially conforms the privacy and security requirements. The cloud security model intended for semi-trusted data-driven communication conveys that the cloud model should faithfully comply with the deployed protocol specifications. It tries to extract information during the interaction between IoT users. The following Table 1 represents a brief overview of existing security challenges in IoT layers [16].

Table 1. Security Aspects of IoT

Security Challenges in IoT	
Interoperability	The convenient security solutions while integrated to the IoT systems should not affect the performance of the interconnected heterogeneous devices and their operational strategies.
Resource Constraints	Set up of security protocols which implements cryptographic operations on IoT node generated data mostly undergo through different difficult circumstances and constraints such as lack of storage capacity, power, and processing capabilities. Apart from these also the security system operates on low bandwidth channels which are quite challenging.
Data Volumes	Sensor-based IoT systems generate an enormous amount of data which are heterogeneous; the system should have potential to entail huge volume of data in a centralized server.
Privacy Protection	As IoT based sensor network performs communication based on RFID tags which makes the wireless channels vulnerable where any intruder can track down the tags and identify the objects. During attack, an intruder not only read the data it modifies the content and takes over control of the particular segment of the network.
Scalability	As IoT network consists of heterogeneous nodes with different computational capabilities thus, the network protocols should work effectively irrespective of some nodes.
Automatic Control	The traditional computers of the internet are needed to re-configure them to adapt into new applications domain whereas the objects deployed over an IoT network should spontaneously connecting to each other and should have the adaptability to new application systems without bothering about where it is currently operating in.

There exist different security threats present in different layers of IoT such as spoofing, signal radio jamming, device tampered node capturing, etc. The following Figure 2 exhibits an overview of different threats specific to different layers of IoT [17].

The conventional research direction towards security solutions for IoT recommended three different aspects such as 1) security of perception layer, 2) security of network layer and 3) security of support and application layer. The following section discusses few of the significant existing security solution approaches to defending the cyber-attacks in IoT networks.

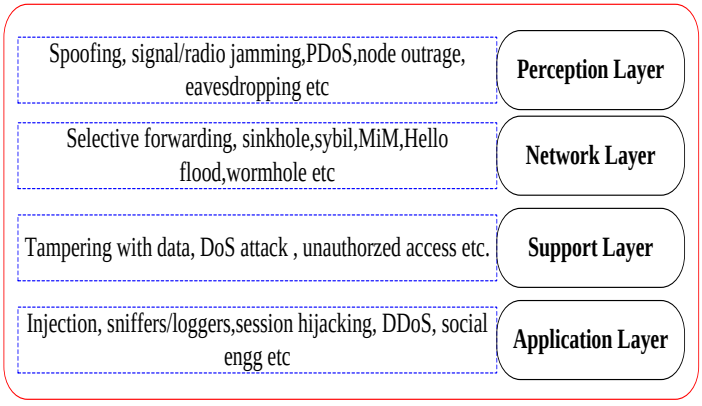

Figure 2. Threats on Layers of IoT

3. CONVENTIONAL SECURITY SOLUTION APPROACHES IN IoT

Keeping security concerns of perception layer into mind, it can be said that there is a need to execute cryptography based security protocols on equipment such as RFID readers, sensors, gateways, GPS and other devices connected to the IoT networks. OWASP [18] has encountered 10 different IoT vulnerabilities in different layers. The IoT must have its people to be authorized before permitting to access to the sensitive data produced by physical objects. It also requires implementing efficient physical identity and access management policy to satisfy the authorization and authentication policies in IoT. Data collection

also play a very significant role in this layer thereby the image, and multimedia data collection techniques are needed to be secured as much as possible. Cryptographic security mechanism also intends to perform data encryption and decryption with the purpose of securing IoT sensor-generated data. These operations are more often defined to ensure every possible privacy at the IoT objects. The following Table 2 exhibits few of the well-known cryptographic algorithms more frequently adopted into the internet security protocols for different purposes [19].

Table 2. Conventional Cryptographic Algorithms

Type	Algorithm	Purpose
1) Symmetric Encryption	Advance Encryption Standard (AES)	Confidentiality
2) Asymmetric Encryption	Rivest Shamir Adelman (RSA)/ Elliptic Curve Cryptography	Digital Signature
3) Asymmetric Key Agreement	Diffie- Hellman (DH)	Key Agreement
4) Hashing	SHA-1/SHA-256	Integrality

Most recently many authors paid attention to improve the performance of existing security protocols of IoT. In many existing review studies, design constraints of those security protocols and their lack of adaptability with new IoT based applications also have been highlighted. The following Table 3 represents few of the conventional security solutions approaches and their significant aspects.

Table 3. Review of Literatures

Authors	Problem-focused	Proposed approach	Inferencing of Performance parameters concerned
Wang *et al*. [20]	Physical layer security of IoT	Compressed sensing based security model	Mutual Information (bits) The number of arithmetic sum Sample RSSI (dBm)
Sahni *et al*. [21]	Security of physical network layer Task allocation problem	Edge Mesh	-The model discussed only from an analytical point of view no extensive simulation outcomes observed.
Chen and Zhu [22]	Security of cyber-physical layers of IoCT	Contract-based FlipCloud game	Unit defending Attacking cost Unit penalty Transfer payment
Huang *et al*. [23]	Data confidentiality in IoT	A secure and fine-grained data access control scheme	Computation time (ms) Number of attributes in access policy
Kaugianos *et al*. [24]	Secure image Communications in IoT	A modular and extensible quadrotor architecture	Size Peak signal to noise ratio (PSNR) RMSE SSIM
Xu *et al*. [25]	Defending against new-flow attack	Smart security mechanism (SSM)	Request rate of switch CDF Time New flow attack rate

Along with this the study also discusses few of the relevant literature has been recently implemented and studied. Khan *et al*. [26] present a secure cloud-based mobile healthcare framework using wireless body area networks. The line of research presented here is twofold: first, it attempts to secure the inter-sensor communication by multi-biometric based key generation scheme in WBANs; and secondly, the electronic medical records (EMRs) are securely stored in the hospital community cloud, and privacy of the patients' data is preserved. Ukil *et al*. [27] to address the issue of security for data at rest in IoT. The study of Atamli and martin [28] conceptualized a threat-model which exclusively concerned about different use cases of IoT aspects. The more focused in this regards inclined towards investing that fact that in which aspects the focus should be more to secure the IoT systems. In the study of Arias *et al*. [29] fundamental discussion on different security design practices and their impact on IoT data privacy. A study in almost similar direction has been presented in the work of Shahabadkar and Pujeri [30] where the authors mostly emphasized on ensuring better security systems over Peer-to-Peer (P2P) networks. The study also investigated and conveyed about the existing security problems associated with P2P communication layers and further introduced a security model to strengthen up the protection layer of communication channels intended for multimedia content sharing. The proposed modeling uses scalable coding with the aim of performing ciphering to encrypt the multimedia content over a P2P communication network. The simulation outcomes obtained further shows

that proposed technique ensure cost-effective security model which can operate efficiently in P2P. Shahabadkar and Pujeri [31] have presented another secure framework to establish efficient multimedia communication in P2P. They study formulated two different algorithms namely recurrence relation of degree 2 and evolutionary algorithm to ensure the security of transmitted multimedia frames over a P2P communications. Their contributory aspects approve the fact that the evolutionary algorithms can be used for strengthing the encryption process and also having a scope of implementation over futuristic IoT networks for securing complex metadata. The extensive numerical simulation carried out concerning maximized entropy of frames and Pearson product moment correlation coefficient (PPMCC) conveyed the superiority of the proposed system among adjacent pixels with key analysis. Alam *et al*. [32] proposed a layered architecture of IoT framework where a semantically enhanced overlay interlinks the other layers and facilitate secure access provision to the Internet of Things-enabled services. The study of Jing *et al*. [33] explores different security problems that associated with IoT operational constraints in different layers. It also analyzes the design aspects of security layers implemented over a large scale network. The study mostly emphasized extensively discussing the cross-layer heterogeneous issues and also summarizes the respective solution approaches. Heer *et al*. [34] discuss the applicability and limitations of existing Internet protocols and security architectures in the context of the IoTs along with an overview of the deployment model and general security needs. Babar *et al*. [35] give an overview, analysis, and taxonomy of security and privacy challenges in IoT. Chien *et al*. [36] propose and implements a new WSN-based application—an exhibit guidance and recommendation system. They focus on the study presented by Hou and Yeh [37] lay upon sensor tags oriented communication architecture. It intended to explore the extensibility of the conventional security protocols into future IoT based healthcare service systems. The work carried out by Kim *et al*. [38] proposed a method that improves the proxy enabled service connection delay by introducing a new concept that includes operational mutual authentication with session key on proxy preparation task.

In Suryani *et al*. [39] introduced a trust-based privacy mechanism for IoT and trustable objects were computed through Ant Colony algorithm. This mechanism of forms with stabilized trust values. Authors Koppula and Muthukuru [40] combinedly explained the Elliptic curve based secure signature (digital) system for IoT. The outcomes were suggested that this provides the better privacy without affecting the security level. Slimane and Ahmed [41] presented a secure key (end-to-end) management protocol for IoT and found effective with symmetric cryptography.

3.1. Existing research trends

This phase of the study also investigates the statistics of the research carried out on the security of IoT in between a timeline of 2010-2017. The data has been taken by referring IEEE Xplore digital library which approves a matter of the fact that very few effort has been given in this field of study. The following Figure 3 shows the statistics of existing research trends of security aspects of IoT.

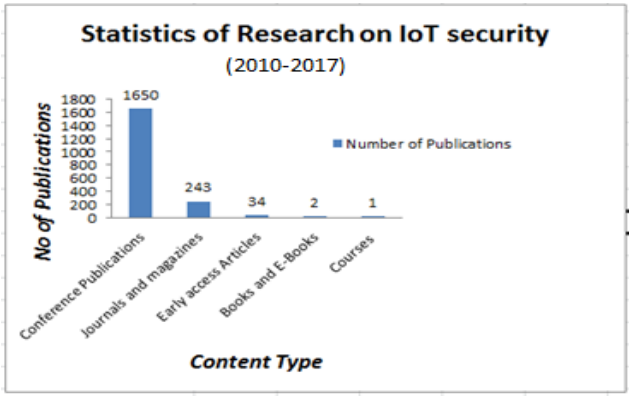

Figure 3. Statistics of research on IoT Security

4. EXISTING RESEARCH ISSUES

This section discusses the research gap after reviewing the existing techniques:

a. There is less number of standard research papers dedicated to secure communication in IoT. It is still in infancy stage.

b. Majority of the existing schemes are based on using cryptographic approach ignoring the fact that the IoT nodes have the less computational capability.
c. Studies based on heterogeneity of nodes and addressing associated security problems are quite less to find.

5. CONCLUSION

The proposed study exclusively discusses the existing research trends of IoT from security and data authentication perspectives. The study also exhibits different conventional design constraints associated different IoT protocols and also brings out the research gap. The study effectively defines how light weight usage of cryptography in IoT can result in less response time while executing less iterative steps of encryption. The study also defines the possibility of strengthening the existing routing protocols by integrating it with forwarding backward secrecy.

REFERENCES

[1] Z. Sheng *et al*., "A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities", *IEEE Wireless Commun*. vol. 20, no. 6, 2013, pp. 91-98.
[2] X. Li *et al*., "Smart Community: An Internet of Things Application", *IEEE Commun. Mag*., vol. 49, no. 11, 2011, pp. 68-75.
[3] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things", Computer, vol. 44, no. 9, 2011, pp. 51-58.
[4] X. Lin *et al*., "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving", *IEEE Trans. Wireless Commun*. vol. 7, no. 12, 2008, pp. 4987-4998.
[5] X. Lin and X. Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks", *IEEE Trans. Vehic. Tech*., vol. 62, no. 7, 2013, pp. 3339-48.
[6] J. Zhou *et al*., "4S: A Secure and Privacy-Preserving Key Management Scheme for Cloud-Assisted Wireless Body Area Network in m-Healthcare Social Networks", *Info. Sciences*, vol. 314, 2015, pp. 255-276.
[7] J. Sen, "Privacy Preservation Technologies in Internet of Things", *Proc. Int'l. Conf. Emerging Trends in Mathematics, Technology, and Management*, 2011.
[8] R. Roman *et al*., "Key Management Systems for Sensor Networks in the Context of the Internet of Things", *Computer & Electrical Engineering*, vol. 37, no. 2, 2011, pp. 147-59.
[9] H. Zhu *et al*., "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks", *IEEE Trans. Vehic. Tech*., vol. 58, no. 8, Oct. 2009, pp. 4628-4639.
[10] J. Zhou *et al*., "Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs", *IEEE Trans. Info. Forensics and Security*, vol. 10, no. 6, 2015, pp. 1299-314.
[11] P. Paillier, "*Public Key Cryptosystems Based on Composite Degree Residuosity Classes*", Eurocrypt '99, pp. 223-38.
[12] Y. Saleem, F. Salim, and M.H. Rehmani, "*Resource Management in Mobile Sink Based Wireless Sensor Networks through Cloud Computing*", in Resource Management in Mobile Computing Environments, Springer-Verlag, vol. 3, 2014, pp. 439-59.
[13] R. Lu *et al*., "Pi: A Practical Incentive Protocol for Delay Tolerant Networks", *IEEE Trans. Wireless Commun*, vol. 9, no. 4, Apr. 2010, pp. 1483-92.
[14] J. Zhou *et al*., "TR-MABE: White-Box Traceable and Revocable Multi-Authority Attribute-Based Encryption and Its Applications to Multi-Level Privacy-Preserving e-Heathcare Cloud Computing Systems", *IEEE INFOCOM*, 2015.
[15] J. Groth and A. Sahiai, "Efficient Noninteractive Proof Systems for Bilinear Groups", Advances in Cryptology®EUROCRYPT 2008, Springer Berlin, 2008., pp. 415-32
[16] Borgohain, T., Kumar, U. and Sanyal, S., (2015), "Survey of Security and Privacy Issues of Internet of Things", *International Journal of Advanced Networking Applic Ations*, 6, 2372-2378.
[17] Anwar, R.W., Bakhtiari, M., Zainal, A., Hanan, A.A. and Qureshi, K.N., (2014), "Security Issues and Attacks in Wireless Sensor Network", *World Applied Sciences Journal*, 30, 1224-1227.
[18] OWASP, Internet of Things Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project
[19] Deng, J., Han, R. and Mishra, S. (2005) *Defending against Path-Based DoS Attacks in Wireless Sensor Networks*. ACM Workshop / Security of Ad Hoc and Sensor Networks, Alexandria, 7 November 2005, 89-96.
[20] N. Wang, T. Jiang, W. Li and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection", in *IET Communications*, vol. 11, no. 9, pp. 1431-1437, 6 22 2017.
[21] Y. Sahni, J. Cao, S. Zhang and L. Yang, "Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things", in *IEEE Access*, vol. 5, , pp. 16441-16458, 2017.
[22] J. Chen and Q. Zhu, "Security as a Service for Cloud-Enabled Internet of Controlled Things Under Advanced Persistent Threats: A Contract Design Approach", in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2736-2750, Nov. 2017.
[23] Q. Huang, Y. Yang and L. Wang, "Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things", in *IEEE Access*, vol. 5, no. , pp. 12941-12950, 2017.

[24] E. Kougianos, S.P. Mohanty, G. Coelho, U. Albalawi and P. Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things", in *IEEE Access*, vol. 4, no. , pp. 1222-1242, 2016.
[25] T. Xu, D. Gao, P. Dong, H. Zhang, C. H. Foh and H. C. Chao, "Defending Against New-Flow Attack in SDN-Based Internet of Things", in *IEEE Access*, vol. 5, no. , pp. 3431-3443, 2017.
[26] F.A. Khana, A. Alia, H. Abbasb, N. Al Hasan Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks", *Elsevier- International Workshop on Communications and Sensor Networks*, vol.34, pp.511-517, 2014.
[27] A. Ukil, J. Sen, S. Koilakonda, "Embedded Security for Internet of Things", *IEEE National Conference on Emerging Trends and Applications in Computer Science*, 2011.
[28] A.W. Atamli, A. Martin, "Threat-based Security Analysis for the Internet of Things", *IEEE International Workshop on Secure Internet of Things*, 2014.
[29] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices", *IEEE Transactions on Multi-Scale Computing Systems*, 2015.
[30] Shahabadkar, Ramesh, and Ramchandra V. Pujeri. "Stratum based Approach for Securing Multimedia Content Transmission over Large Scale P2P", *International Journal of Computer Applications*, vol. 89, no. 5, 2014.
[31] Shahabadkar, Ramesh, and Ramchandra V. Pujeri. "Secure multimedia transmission in p2p using recurence relation and evolutionary algorithm", In *International Symposium on Security in Computing and Communication*, pp. 281-292. Springer, Berlin, Heidelberg, 2013.
[32] S. Alam, M.M.R. Chowdhury, J. Noll, "Interoperability of Security-Enabled Internet of Things", *Springer-Wireless Personal Communication*, 2011.
[33] Q. Jing, A.V. Vasilakos, J. Wan, "Security of the Internet of Things: perspectives and challenges", *Springer-Wireless Personal Communication*, 2014.
[34] T. Heer, O.G. Morchon, R. Hummen, "Security Challenges in the IP-based Internet of Things", *Springer-Wireless Personal Communication*, 2011.
[35] S. Babar, P. Mahalle, A. Stango, N. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)", *Springer*, 2010.
[36] H-Y Chien, Y.J. Li, and NW Lo, "Innovative Applications and Security of Internet of Things", *Hindawi-International Journal of Distributed Sensor Networks*, 2014.
[37] JL. Hou and KH Yeh, "Novel Authentication Schemes for IoT Based Healthcare Systems", *Hindawi-International Journal of Distributed Sensor Networks*, 2015.
[38] SK Kim, BG Kim, and BJ Min, "Reducing Security Overhead to Enhance Service Delivery in Jini IoT", *Hindawi-International Journal of Distributed Sensor Networks*, 2015.
[39] Vera Suryani, Selo Sulistyo, Widyawan, "Trust-Based Privacy for Internet of Things", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, no. 5, pp. 2396-2402, October 2016.
[40] Sumanth Koppula, Jayabhaskar Muthukuru, "Secure Digital Signature Scheme Based on Elliptic Curves for Internet of Things", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, no. 3, pp. 1002-1010, June 2016.
[41] Yamina Ben Slimane, Khelifa Ben Ahmed, "Efficient End-to-End Secure Key Management Protocol for Internet of Things", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 3622-3631, December 2017.

BIOGRAPHIES OF AUTHORS

Rajani Chetan, Assistant Professor, Department of Information Science, Maharaja Institute of Technology, Mysore, India, She has done B.E in Information Science from Vidyavardhaka College of Engineering, Mysore. She has completed M.Tech in Software Engineering from Jaya Chamarajendra College of Engineering, Mysore. She is pursuing phD from VTU.

Dr. Ramesh Shahabadkar, He is an internationally known patent researcher, academician, and academic leader. He has excellent track records of enhancing academics, teaching-learning and training. He has 26 years of highly successful professional experience, out of which 5 years in patent research and 21 years in teaching at all levels of Engineering. He is down to the earth, friendly, honest and sincere leader with a very high degree of hands on situational and motivational leadership skills. He has completed his PhD in Computer Science and Engineering. He has published total 5 papers in international journal and 4 papers in international conferences.