IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

An Analysis of the Internet of Things Security From Data Perception

Raviteja Gaddam[1*], M. Nandhini[2]

[1, 2] Department of Computer Science, Pondicherry University, Puducherry, Tamil Nadu, India

[*]*Corresponding Author: raviteja.csebec@gmail.com, Tel.: +91-9010862466*

DOI: https://doi.org/10.26438/ijcse/v7i2.427433 | Available online at: www.ijcseonline.org

Accepted: 18/Feb/2019, Published: 28/Feb/2019

***Abstract*—** As the usage of the Internet of Things (IoT) is increasing, the challenges of providing security for IoT are becoming severe. Every IoT device generates and shares the data, which plays a key role in IoT applications. To understand the IoT security, one should observe many approaches like data, communications, and applications. Among these, a view from the data side may be of much help. This paper analyses various issues in IoT security from the data approach. Authors propose a Three Perspective Model consists of Exclusive, Inclusive and End-Users Perspectives to provide IoT Security by integrating IoT architecture and Data Transmission. The Exclusive Perspective focuses on individual IoT devices, the Inclusive Perspective focus on collective IoT devices and the end-users perspective focus on IoT applications. The three perspectives focus on the secure transmission of data, authentication, privacy and the challenges against IoT applications. This paper analyses the data perspective of IoT security discusses the challenges and suggests some possible solutions for IoT security.

***Keywords*—** Internet of Things, Safety, Security, Privacy

I. INTRODUCTION

Connecting the world in a pervasive manner is made possible by the Internet of Things (IoT), which can be a miracle of technology. This magnifies the communication and data transmission from any place to anything as shown in Figure 1. This extensive connectivity is also creating a lot of security problems [1]. From Smart Home to Smart Industries, IoT is providing several services by collecting, extracting and manipulating the data from IoT devices with a great impact on people's life. So it is important to consider the data perspective of IoT applications. All the IoT devices are not only data generating devices but they must be capable of communicating the data to the storage facilities over the Internet. Staring from Smart Watches to Smart Automobiles, everything can generate and use versatile data concerned to the respective applications and environments.

Data is the live part of IoT and by observing it may help to know the security of IoT. Many research works have focused on several perspectives on IoT Security without focusing on the data part. So, this paper analyses IoT security by focusing on the data generated in IoT networks.

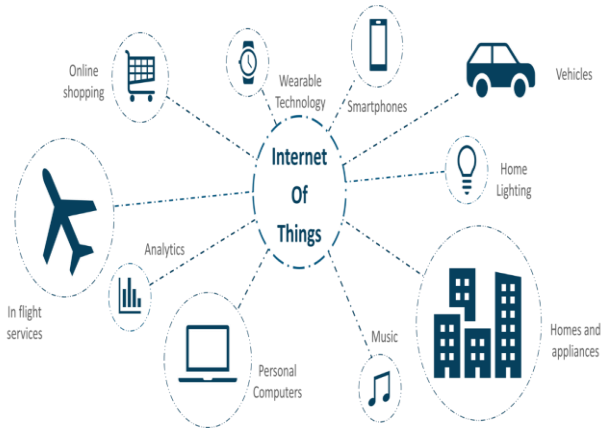

Figure 1. IoT Applications

In this paper, we propose a three perspective framework that combines the study of IoT architecture and the data cycles in the IoT networks as shown in Figure 2. These perspectives focus on individual IoT devices, a group of IoT devices and End-User Applications. IoT security can be explored by observing the data in each perspective.

The analysis of all these perspectives gives a holistic view of IoT security. As the data is present anywhere in the IoT network, including an IoT device, Internet and the Cloud Storage, it is essential to focus on this approach while considering IoT security. But, the majority of the data will be driven from IoT devices to Cloud through the Internet. Thus, this paper mainly focuses on this point and performs

a thorough analysis of issues and challenges in IoT security from the view of data.

Figure 2. Three Perspectives of IoT Security

The organization of the remaining paper is as follows. Section II discusses the work related to IoT security, Section III explores IoT security from the exclusive perspective, Section IV explores IoT security from an inclusive perspective, Section V explores IoT security from end user's perspective, followed by conclusion in Section VI.

II. RELATED WORK

This section discusses some of the surveys related to IoT security in various approaches.

Authors of [2] focused on the trust computation models for service management in the IoT environment. [3] focused on surveying the possibilities and challenges in using SDN and Fog Computing in IoT applications for network communications and data service respectively.

Authors of [4] focused on comparing various security solutions based on cryptographic approaches for IoT in achieving the main security requirements like Confidentiality, Integrity, and Availability. Authors in [5] focused on providing safety and security in IoT applications. Designing cyber-physical and IoT devices are harder than traditional systems.

Authors of [6] discussed the issues related to IoT security by using powerful Quantum Computers. This paper addressed various fields of IoT usage, tools and security algorithms to provide better IoT security. Authors of [7] classified the security threats of IoT using a taxonomy. This taxonomy is relating to data, architecture, communication, and application.

Authors in [8] focused on analyzing several recent works on IoT security from the last three years and gave an overview of the latest IoT security research, tools, and simulators. Authors of [9] discussed the possibilities and open issues related to the usage of Fog Computing and Edge Computing for IoT applications. Also deliberated several existing architectures in this area and gave a comprehensive view of using Fog and Edge in IoT applications.

Authors of [10] focused on providing IoT security from the application layer perspective. This paper presented and discussed some of the protocols like XMPP, MQTT, and CoAP to provide lightweight security and improving the functionality of IoT.

Authors of [11] focused on surveying the IoT Security using SDN and Blockchain technology. This paper classified and compared the existing solutions of IoT security and gave a comprehensive view of the issues and possibilities of using SDN and Blockchain for IoT Security.

Authors of [12] focused on discussing several IoT frameworks and compared the security features, security standards and secure communications of every framework along with the methodologies adopted by them. Authors of [16] provided a review on several IoT architectures and compared them against security, standards, and interoperability features.

Authors of [13] surveyed the major vulnerabilities of IoT applications and their solutions. This paper analyzed the possible threats at different levels like IoT nodes, Communications, and Edge Computing and the IoT applications in various domains like Smart Homes, Smart Cities, Transportation, Healthcare, etc. Major security and privacy challenges in these domains also deliberated along with the security needs.

Authors of [14] analyzed IoT security at various levels like data, communication and application interface. This paper also discussed various standard solutions for IoT security along with various wireless communication technologies.

Authors of [15] surveyed the crucial components in IoT security like securing devices and code integrity and authors of [16] surveyed issued related to the usage of IoT in the health care industry.

Authors of [17] surveyed the IoT security in several segments: limitations of IoT devices, a grouping of IoT attacks, architectures and security issues. Authors discussed and compared various IoT applications, architectures, limitations, and challenges. Also emphasized the usage of hardware level solutions, edge layer security, and distributed security model for providing better IoT security.

The above-mentioned research works gave a better view of IoT security in various aspects. But, none of them considered data as the primary focus in interpreting IoT security. So, this paper focuses on this data-driven perspective and finds possible issues of IoT security in a different way.

III. IoT Security from Exclusive Perspective

This section explores the IoT security by monitoring the data from an individual IoT device. Every device generates and transmit the data or may receive the data through the Internet. This data flow can be considered as input and output for the IoT device and must be focused on IoT security.

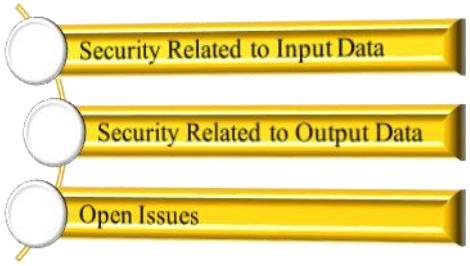

Figure 3. Views in Exclusive Perspective

A. *Security related to Input Data:*

IoT combines the physical world with the cyber world and hacking a device may bring security threats to both instances. Physical tampering of a device may affect the functionality and altering the data during transmission can affect the device state [5]. Devices perform the operations based on the input data and combining with security policies. By altering the input data and sending malicious data, attackers can compromise the devices. Unsafe operations may lead the devices to malfunction and sometimes may lead to loss of life. For example, malicious code can affect health care equipment connected to a patient and may endanger life. Most of the time all the IoT devices are connected to the Internet and if they possess vulnerabilities, then hackers can gain control over them. By using Botnets like Mirai and Reaper, hackers can get full control of the IoT devices [18]. With that, they can steal personal data and may block the applications for ransom. So [18] suggests that manufacturers must design and develop the devices to restrict the network access only when needed.

If IoT devices are used as a part of the industrial infrastructure, then one single compromised device can result in a catastrophic loss to both properties and lives. Devices must be updated on a regular basis to defend the novel attacks. Care should be taken by the vendors when pushing the updates to devices. Mere security patches may ease the hacking when hackers find the vulnerabilities. So, automatic and regular update mechanisms must be configured to get the latest firmware.

But, automatic updates may bring some more risks. If attackers use rollback attacks on the device firmware, then they can exploit the vulnerabilities and may attack the devices. So, manufacturers must send the updates in an encrypted form and digitally signed to ensure the integrity of the update.

Besides, this updating mechanism may create traffic congestion. By using Blockchain techniques, the update can be done in a distributed manner and can solve the traffic bottleneck [19]. IoT devices may request an update in a peer to peer network. Then the device can download the latest firmware by checking its integrity. However, this requesting by all the devices may generate unnecessary and useless traffic.

To reduce the risks of remote updating, [20] proposed a level-wise partial updating mechanism at runtime. This mainly consists of a dynamic system, a static system level, and a kernel level. Authors in [20] developed this approach on Contiki OS, without modifying the protocols and applications.

B. *Security related to Output Data*

All the IoT devices generate and upload the data to IoT applications through the Internet. Some data is highly sensitive and valuable. So, ensuring confidentiality while transferring the data is very much essential. Also, the legitimacy of output data can affect the reliability of services that are related to industry and social life. Hence, IoT applications must ensure confidentiality and legitimacy from all the IoT devices.

1) *Confidentiality:*

Encryption is a general approach to ensure confidentiality. IoT devices are resource constrained and cannot use general algorithms to encrypt the data [21]. Encryption algorithms in IoT devices must provide sufficient security without reducing the performance of the device. Using lightweight ciphers like SEA [13] consisting Feistel structure and mCrypton [17] consisting SP structure may simplify hardware implementation.

The simple structure in lightweight ciphers makes them vulnerable to various attacks [22]. Using a side-channel attack, hackers can extract the keys using leaked information. So, this attack can be a threat to several IoT devices like RFID networks and Smart Cards where these lightweight ciphers are applied.

2) *Legitimacy:*

Data generated by the IoT devices must be reliable and its legitimacy has a great impact on IoT security. Most of the IoT devices are in an open environment where human

intervention is not present. This openness may lead the attackers to tamper the devices, replace and hijack to compromise the device. Verifying integrity and authenticity is very much essential for the data generated by the IoT devices. General attestation methods may not be suitable to verify the device tampering because of their high resource consumption. So, lightweight methods are required for IoT devices.

Time-based software attestation methods like SWATT [23], SCUBA [24] can exploit side-channel attacks and can verify the integrity of devices without special hardware. Hybrid attestation methods like SMART [25] and TyTAN [26] use the combination of software and hardware to defend the attacks. But both these methods may not withstand physical attacks [27]. Verifying the integrity of enormous IoT devices is not a simple thing. SEDA [27], SANA [28] can be used for this purpose. It is very difficult in ad hoc networks, where the devices can join and leave the group dynamically.

3) Open Issues:

Ensuring confidentiality on IoT devices, developing lightweight ciphers is essential with the inclusion of latency reduction and speed optimization. For legitimacy, there is a need for more research on attestation methods to apply for enormous devices. Sometimes it is very difficult to get the correct status of an IoT device as the device can go online or offline dynamically. Also, there is not a common mechanism to update heterogeneous devices. Applying updates regularly to all the devices is another issue. There are several unsolved issues related to improving the accuracy of attestation, robustness, and efficiency

IV. IOT SECURITY FROM INCLUSIVE PERSPECTIVE

This section focus on the data flow among several IoT devices of a group. While interacting with the Internet, all IoT devices must obey the interconnectivity feature. Interaction among the devices is ensured by the communication networks while transferring the data to and from the applications. In this section, we analyze the issues related to authentication, communication and access control.

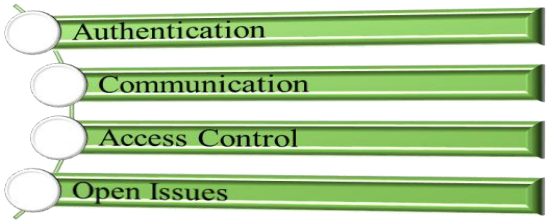

Figure 4. Views in Inclusive Perspective

A. Authentication:

Implementing a two-way authentication is essential in a decentralized network. Data holders and data collectors, data collectors and IoT devices need to authenticate before processing the data [29]. Authenticating RFID tags and the RFID reader is a security issue investigated in [30]. Approaches like key-based, biometric-based are some of the authentication efforts. For resource-constrained devices, using a challenge-response mechanism is suitable [31]. Because of privacy issues, biometric-based authentication may not be preferred by many users. But in ad-hoc network scenarios, the anonymity of the entities need to be considered because the devices can join and leave dynamically [8].

B. Communication:

For IoT devices, there are different types of communications like through the local network, through the Internet and through the Internet via gateways. For the last two types, IoT devices can use different protocols and wireless technologies like Wi-Fi, Bluetooth to communicate other devices or storage facility. Devices like sensors can communicate within a local network with their routing abilities. But most of these devices have less physical protection, so they have a great threat of hijacking [32]. Ensuring security while communicating is a critical issue. For that devices must use secure routing techniques and have to create a trustable route. Compromised nodes can bring security problems like transmitting false route information and denying legitimate routes [33].

So, ensuring secure communication in IoT network is essential to ensure the integrity of data transmission. Communication-related issues can be categorized as design: (1) Secure protocols (2) Efficient Intrusion Detection Systems (3) Lightweight trust evaluation schemes. Routing protocols like RPL, are not evading security risks [32] and intrusion detection like DEMEM [34] is working when the network overhead is minimal. Trust management model like TERP has routing issues. It is desirable for IoT communication protocols should be auto recoverable whenever network failures occur. This feature can isolate compromised IoT devices without human intervention [35].

C. Access Control:

IoT network resources must be restricted only for the authorized actors. IoT devices and users can only generate and process the data for the specified purpose. Most of the IoT devices have automatic access control mechanisms. Some of the IoT systems use the roles and attributes to control the access privileges [36]. Usage Control Models can be used for automatic and dynamic authentication that can be used to activating or revoke the access privileges [37].

D. Open Issues:

As most of the IoT devices use wireless communication, there is a possibility for compromising the nodes by the attackers. Existing intrusion detection techniques may not be suitable in an IoT environment. Using the latest technologies like Blockchain with Fog or Cloud may bring reliability in communication. Most of the IoT devices are automatic and it is essential to verify their access control mechanisms. Cross-domain authentications are required for IoT networks that are ad-hoc in nature. But designing and developing efficient authentication methods is still a big challenge for researchers.

V. IOT SECURITY FROM END-USER'S PERSPECTIVE

This section focus on exploring IoT security from end users and the data used in applications perspective. Enormous data is generated by the devices and transferred to IoT applications. By considering the data usage, this section discusses some issues related to privacy and challenges of IoT system.

Figure 5. Views in End-User's Perspective

A. Privacy:

Data used by the IoT applications may be leaked by the attackers while transferring to and from the devices. This may raise privacy issues if the data is sensitive like fingerprints, medicine and can cause a severe threat to lives [38]. Unlike on the Internet, where privacy is risked by the users, IoT devices are automatically transferring the details without the users' awareness. Data Mining and Machine Learning techniques can be efficiently designed to preserve privacy [39]. Even though the devices are not meant for monitoring privacy-related activities, some techniques need to be placed to monitor such activities. For example, Smart Home devices can be used by attackers to extract sensitive information and to gain full control over them for illegal use. But the applications like SmartApp are suffering from privilege problems [40]. In health care application, if the treatment information gets into the wrong hands, then the attackers can modify the data that may result in the loss of lives. Recent works like privacy preserving in medical data [41], pseudonym medical data management are solving the issues related to digital healthcare.

B. Challenges:

As the attacks are gradually increasing on IoT related services, there is a need for special techniques to investigate the attacks. General forensic mechanisms may not be suitable for IoT applications because of their heterogeneity. As the devices have limited memory resources and are continuously generating and transferring the data, finding the source of the attack is a complicated issue. Some of the frameworks like DFIF-IoT [42] and FaIoT [43] are easing the investigation process in IoT related applications. Preserving privacy is another important issue while investigating the attacks. PRoFIT [44] is one such privacy are IoT forensics model that collaborates with other sources to investigate the crime scene. Currently, there isn't much growth in IoT forensics and it is essential to upgrade the existing forensic tools and to develop novel IoT forensic frameworks.

As the IoT has become a part of daily life, some social challenges are introducing to people's lives. If an automated transport vehicle is a reason for an accident, then the responsibility disputes come. To support automated transportation, Australia has drafted driving laws [45]. Smart devices like fitness bands, smart TVs are becoming the primary target for attackers to perform social engineering attacks to steal personal information.

C. Open Issues:

To preserve privacy, data must be transferred according to the privacy regulations. But, there isn't a generalized framework that defines privacy regulations in IoT related services. So, privacy has to be protected at every level of IoT applications and mechanisms must be integrated into the components of IoT applications by the developers. Blockchain technology may be applied to preserve the evidence and can be useful to solve the issues related to forensics in IoT services

VI. CONCLUSION

This paper emphasized the importance of considering IoT data in providing security for IoT applications. Combination of the IoT architecture and data can outline IoT security in the three perspectives, i.e. Exclusive Perspective, Inclusive Perspective, and End-Users Perspective. Exclusive Perspective observes the data flow around individual Io devices. Inclusive Perspective observes the interconnection of a group of IoT devices. IoT applications like Smart Home, Health Care can be observed in the End-Users Perspective. To include better IoT services as a part of daily life, challenges like authentication, legitimacy, confidentiality, and privacy must be dealt in a profound way. This paper extensively focused on IoT security from

the perspective of data at various levels and mentioned several open issues that are helpful to the researchers in designing better solutions for the security of IoT related applications.

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their valuable feedback. We would like to thank our Computer Science Department for providing the necessary resources for our work. This paper reflects the views only of the authors, and others cannot be held responsible for any use which may be made of the information contained therein.

REFERENCES

[1] Trustwave and Singtel, "Internet of Things Cybersecurity Readiness," 2017.

[2] J. Guo, I. Chen, and J. J. P. Tsai, "A Survey of Trust Computation Models for Service," *Comput. Commun.*, 2016.

[3] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, "Security and Privacy for Cloud-Based IoT : Challenges , Countermeasures , and Future Directions," no. January, pp. 26–33, 2017.

[4] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy : From sensors to the Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 75, pp. 46–57, 2017.

[5] M. Wolf and D. Serpanos, "Safety and Security of Cyber-Physical and Internet of Things Systems [Point of View]," *Proceedings of the IEEE*, vol. 105, no. 6. pp. 983–984, 2017.

[6] B. Mukherjee *et al.*, "Flexible IoT security middleware for end-to-end cloud–fog communication," *Futur. Gener. Comput. Syst.*, vol. 87, pp. 688–703, 2018.

[7] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88. pp. 10–28, 2017.

[8] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-porisini, "Security , privacy and trust in Internet of Things : The road ahead," *Comput. NETWORKS*, vol. 76, pp. 146–164, 2015.

[9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017.

[10] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, and S. Bhairav, "Security Testbed for Internet-of-Things Devices," *IEEE Trans. Reliab.*, vol. PP, pp. 1–22, 2018.

[11] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017.

[12] I. Internet, T. Policy, and C. White, "INDEX TO VOLUME THE FOURTH.," *Lancet*, vol. 2, no. 53, p. nil, 1824.

[13] S. R. Moosavi, T. N. Gia, A. Rahmani, and S. Virtanen, "SEA : A Secure and E ffi cient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways," *Procedia - Procedia Comput. Sci.*, vol. 52, no. Ant, pp. 452–459, 2015.

[14] T. H. Szymanski, "Security and Privacy for a Green Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 34–41, 2017.

[15] B. Thaker, N. Shah, and P. Bhatt, "A Survey on Developing Secure IoT Products," *Int. J. Sci. Res. Comput. Sci. Eng.*, vol. 6, no. 5, pp. 41–44, 2019.

[16] Gurpreet Kaur and Manreet Sohal, "IOT Survey: The Phase Changer in Healthcare Industry," *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 6, no. 2, pp. 34–39, 2018.

[17] C. H. Lim and T. Korkishko, "mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors," 2006, pp. 243–258.

[18] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer (Long. Beach. Calif).*, vol. 50, no. 7, pp. 80–84, 2017.

[19] B. L. J. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, 2016.

[20] P. Ruckebusch, E. De Poorter, C. Fortuna, and I. Moerman, "GITAR: Generic extension for Internet-of-Things ARchitectures enabling dynamic updates of network and application modules," *Ad Hoc Networks*, vol. 36, pp. 127–151, 2016.

[21] B. J. Mohd, T. Hayajneh, and A. V Vasilakos, "Journal of Network and Computer Applications A survey on lightweight block ciphers for low-resource devices : Comparative study and open issues," *J. Netw. Comput. Appl.*, vol. 58, pp. 73–93, 2015.

[22] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *J. Cryptogr. Eng.*, 2017.

[23] A. Perrig and C. M. U. Cylab, "SWATT : SoftWare-based ATTestation for Embedded Devices £," 2004.

[24] A. Seshadri, M. Luk, A. Perrig, L. Van Doorn, and P. Khosla, "SCUBA: Secure Code Update By Attestation in sensor networks," in *Proceedings of the 5th ACM workshop on Wireless security*, 2006, vol. 2006, pp. 85–94.

[25] K. Eldefrawy *et al.*, "SMART: Secure and Minimal Architecture for (Establishing a Dynamic Root of Trust," in *NDSS*, 2012, vol. 12, pp. 1–15.

[26] F. Brasser, B. El Mahjoub, A. Sadeghi, C. Wachsmann, and P. Koeberl, "TyTAN," in *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*, 2015, pp. 1–6.

[27] N. Asokan, F. Brasser, A. Ibrahim, … A. S.-P. of the, and U. 2015, "Seda: Scalable embedded device attestation," *dl.acm.org*, pp. 964–975, 2015.

[28] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A. Sadeghi, and M. Schunter, "SANA," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 2016, pp. 731–742.

[29] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Secur.*, vol. 7, 2013.

[30] C. Su, B. Santoso, Y. Li, R. H. Deng, and X. Huang, "Universally Composable RFID Mutual Authentication," *IEEE Trans. Dependable Secur. Comput.*, vol. 14, no. 1, pp. 83–94, 2017.

[31] Y. Gao *et al.*, "Obfuscated Challenge-Response : A Secure Lightweight Authentication Mechanism for PUF-Based Pervasive Devices," 2016.

[32] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *J. Netw. Comput. Appl.*, vol. 66, pp. 198–213, 2016.

[33] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision , architectural elements , and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[34] C. H. Tseng, S. H. Wang, C. Ko, and K. Levitt, "DEMEM: Distributed Evidence-driven Message Exchange intrusion detection Model for MANET," *Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, vol. 4219 LNCS. pp. 249–271, 2006.

[35] D. Airehrour and J. Gutierrez, "An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing," in *CONF-IRM 2015 Proceedings*, 2015, vol. 17, no. May.
[36] N. Ye, Y. Zhu, R. Wang, R. Malekian, and L. Qiao-min, "An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things," vol. 1624, no. 4, pp. 1617–1624, 2014.
[37] Z. Guoping and G. Wentao, "The research of access control based on UCON in the internet of things," *J. Softw.*, vol. 6, no. 4, pp. 724–731, 2011.
[38] R. H. Weber, "Internet of things : Privacy issues revisited," *Comput. Law Secur. Rev. Int. J. Technol. Law Pract.*, vol. 31, no. 5, pp. 618–627, 2015.
[39] R. Mendes and J. P. Vilela, "Privacy-Preserving Data Mining: Methods, Metrics, and Applications," *IEEE Access*, vol. 5, pp. 10562–10582, 2017.
[40] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Security Implications of Permission Models in Smart-Home Application Frameworks," in *IEEE Security and Privacy*, 2017, vol. 15, no. 2, pp. 24–30.
[41] K. Seol, Y. G. Kim, E. Lee, Y. D. Seo, and D. K. Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *IEEE Access*, vol. 6, no. XML, pp. 9114–9128, 2018.
[42] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 2016, pp. 356–362.
[43] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," in *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 2015, pp. 279–284.
[44] A. Nieto, R. Rios, and J. Lopez, "Iot-forensics meets privacy: Towards cooperative digital investigations," *Sensors (Switzerland)*, vol. 18, no. 2, 2018.
[45] National Transport Commission, "Changing driving laws to support automated vehicles," 2018.

Authors Profile

*Mr.**Raviteja Gaddam*** received B.Tech degree in CSE from Bapatla Engineering College and M.Tech degree in CSE from NIMRA College of Engineering & Technology. He is currently pursuing Ph.D. (CSE) at Pondicherry University. He received TCS Gold Medal for standing "Best Student of CSE&IT" during his B.Tech course. He qualified both SET & NET. He worked as a lecturer for three years at Bapatla Engineering College and as an Assistant Professor for six years in St. Mary's Women's Engineering College. His research interests include Network Security, Networking, Cryptanalysis, and Information Security. Currently, he is doing his research work on providing efficient intrusion detection in conventional and IoT networks.

Mrs. M. Nandhini received B.Sc. and MCA degrees from Bharathidasan University, M.Phil degree from Alagappa University and pursued Ph.D. from Bharathiar University, Tamilnadu and qualified NET with lectureship. Currently, she is working as an Assistant Professor in the Department of Computer Science, Pondicherry University. She published more than 75 papers in various national and international conferences and journals. Her area of interests includes Evolutionary Algorithms – Soft Computing, Combinatorial Problem Optimization, Artificial Intelligence, and Software Engineering.

