Advanced Security Model for Internet of Things Environment

S. Mani, V. Saravanan, T. Samraj Lawrence, G. R. Sakthidharan, M. Veluchamy

Abstract: *IoT has become one of the most prominent used industry which is been intensively used in various applications across the globe. This usage has also made it more vulnerable to numerous attacks from within and outside the industry. Though this remains as one of the most predominant challenges in almost all of the industries, most of the organizations fail to allocate security budgets in order to secure their sub-networks from being misused and attacked. One of the most important aspects of this drawback is the unawareness of various upcoming IoT devices and infrastructures that are not technically sound enough to handle and meet the challenges caused by the various attacking methods. Implementation of highly secure IoT based infrastructure could basically produce various other benefits that include obtaining greater revenues from new inculcated methods and models while minimizing the operational costs by making use of the various optimized processes. This, in turn, leads to various meaningful and accurate data with a better knowledge of user experience. In order to develop such an IoT infrastructure, all the organizations have to mandatory build built-in security checks in each and every level of the applications being used by them. The paper presents a new design model that is used for securing all the devices from various malicious attacks. The paper also compares the newly designed model with the existing model and has proved the betterment of the security level that is been achieved.*

Keywords: *Security, Authentication, IoT, SIGMA Protocol, Threats*

I. INTRODUCTION

Numerous applications and organizations have been using the IoT environment across the globe. IoT is considered as a network of various physical objects dedicated to performing a certain task allocated to them in the application. It is designed in such a way that it easily communicates with all other connected physical objects and devices for transferring messages and information and senses as well as interacts with all of their external and internal states of the objects. The way in which each of these devices aspects, enables them to perfectly capture and process the data received by other devices. Through this process, the organizations can capture the entire data flowing across various levels of applications and processes it to obtain the desired value and the result. IoT forms as one of the most foundational networks for creating a digital business in today's era. Various levels of security need to be provided at each and every layer of the application to make it less vulnerable to malicious attacks.

The IoT is considered as one of the foundational capability as it is used in the creation of entirely digital business. IoT solution can also be considerably used within an outside-in approach by making use of an independent review. Some of them include the use of their infrastructure such as Threat modeling which is done across entire security layers present in the system, the use of tailored penetration testing and also the use of vulnerability assessment. Organizations that are keen on using and identifying vulnerabilities and also in improving their security from the beginning should be male use of the inside-out approach. This approach focuses on numerous elements in the systems that are embedded in their IoT solution. Some of them being: Secure booting and security controls based on hardware.

Numerous IoT devices generally make their operations present outside the organization's firewalls. Tough this is practiced, it fails to connect to the companies internal networks and all the applications. This increases the vulnerability of the devices by extending the attacks on the surfaces. All the unprotected IoT devices in the network are used for being converted into bots by various attackers. This, in turn, is used for third-party attacks in order to use the data from various communication channels. Most of the IoT devices are used as a single-purpose tool. Predominately their functions are governed and look after by various sensors and all the types of data that are being used in the enterprise and monitored by them. The functional and storage purposes of the IoT devices are strictly not intended to handle heavy-duty computing tasks in the network and the applications. Various research works have been performed and it is noticed that most of the IoT devices make use of SCADA systems.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

Mr. S. Mani*, Department of CSE, Nehru Institute of Engineering and Technology, Coimbatore, India. Email: manicovai@gmail.com

Dr. V. Saravanan*, A.P., Department of Computer Science Engg., Dambi Dollo University, Oromia Region, Ethiopia. Email: reachvsaravanan@gmail.com.

Dr. T. Samraj Lawrence, A.P., Dept. of IT., Dambi Dollo University, Oromia Region, Ethiopia. Email: drsamrajlawrence@gmail.com

Dr. G. R. Sakthidharan, Professor, Department of CSE, Gokaraju Rangaraju Institute of Engg. & Tech., Hyderabad, India, Email: grsdharan@gmail.com

Mr. M. Veluchamy, Asst. Prof., Department of Computer Science, Periyar University Constituent College of Arts and Science-Idappadi, Salem, India. Email: velu29485@gmail.com

The uses of medical devices and critical infrastructure components and also smart meters and appliances have most of the insufficient security mechanisms within themselves. The mentioned devices also don't have any kind of encryption system in order to protect or safeguard the data being transmitted within these devices.

Communication remains poor between the IoT teams and also priority becomes lower when securing the top-level management IoT applications remains a challenge. Most of the enterprises do have their own combination of five key architectural components; things, gateways, mobile devices, the cloud, and the enterprise.

A. Things

Things could be anything that is dumb or smart and is also used for storing most of the data within themselves. Things could also be used to refer to the ones that are also self-sufficient and can also communicate to the world of the internet for making use of centralized coordination and analysis.

B. Gateways

Gateways are referred to as the house of the application logic, which can store data and also communicate with the internet for all the things connected to it. It is not necessary that the things have to be smart, as the use of gateways can provide these necessary resources available.

C. Mobile devices

This category consists of all the smart phones or for case any of the mobile devices which consists of the application logic and is able to store the data. They are also able to communicate with all the things connected to it. Here the things need not be smart, as the mobile devices are provided with the necessary resources.

D. The Cloud

The cloud acts as a hub for providing numerous faculties for the application such as the data storage, power analytics and for also connecting various devices of the application. It is not necessary that the things connected on the cloud need to be smart, as the cloud will provide with all the necessary resources.

E. The Enterprise

The enterprise is majorly focused on making and keeping all the connected devices, analytics and application logic on-premises and keeping the enterprise firewall behind.

F. Challenges

Most of the researchers are not aware of the fact the various effects of interdependence behaviors that are present while looking upon the IoT security. most of the researchers do protect only the particular device. But, it still remains a difficulty when it comes to making a clear defensive boundary. While managing most of the entire IoT devices, which are controlled by numerous cloud platforms has already gained major popularity when it comes to smart home users in today's era. As most of the behaviors of the IoT could be changes when used with other devices and in numerous other environmental conditions, it seems to be very difficult in predefining a set of rules and policies for the devices. The problem of privilege has become one of the most common problems while taking into account the various IoT platforms and applications.

G. Opportunities

There are numerous researchers working on this particular research problem and one of the team in Carnegie Mellon University, who has been working on this particular research were well aware of the cross-device dependencies and have also suggested a new set of policies for security purposes which is able to detect the anomaly behaviour. Consideration of these policies would be more complicated and also impractical as there is an increase in the number of devices used and, also a very new context-based permission system for various IoT platforms in order to solve the over-privileged problem. The system tends to record and also compare as many context information including procedure control and also various data flow, and it's a runtime for each and every IoT device before the due course of its execution. The user is allowed or denied only after this information processing to perform various operations and actions.

While performing numerous surveys, it is planned in this paper to propose a new model in order to secure various devices in an IoT environment. An increase in the number of devices being used within the IoT environment increases the interaction being taking place between those devices. The complexity of the interaction also increases as there becomes less human interaction with the devices. Most of the IoT devices not only communicate within other devices as most of our smart phones operate. They are also intended to control numerous other devices within the environment by making use of several services. Some of them being: IFTTT (if this then that), which is predominately one of the most common scenarios in an IoT environment.

One of the examples that could be given here is: when a thermometer is placed within an indoor used to record the temperature of the environment. At the same time if it detects a rise in the temperature and also when the smart plug detects the AC in an 'off' state, then the windows present within the environment, opens automatically. Most of these examples are quite common if most of the industrial and agricultural environments. In Fig.1, it could be seen that the connection is blocked for accessing the IoT environment as the attacker tries to send a fake command rather than the original command to the IoT environment. When a fake command is sent the seems to be no response to the user as well.

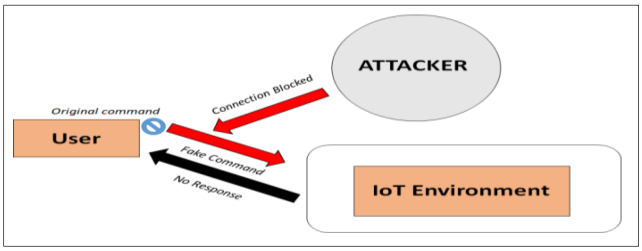

Fig. 1. Transmission of Fake commands from the Attackers

The rest of the section is as follows: Section II consists of a Literature Survey, section III consists of the proposed system used in the paper and section IV consists of various results evaluation performed with the existing and the proposed system is obtained. The paper is concluded in the last by mentioning the relevant future works that could be applied or added to the proposed work.

II. LITERATURE SURVEY

Numerous researchers have been working on this particular problem of providing security to the devices being used in an IoT environment. In this section, we would be discussing on various research works that are existing. In [1], the author discusses a recent Garter report, highlights that there would be more than the usage of 8.4 billion devices connected to each other worldwide by the end year of 2020. This is also expected to grow to almost 20.4 billion by the year 2022. The usage of devices being used in an IoT environment is being increased in almost most of the parts of the worked. Some of the top countries that have been using various aspects and applications using this IoT environment are Europe, China and North America. The year 2016 has recorded 5.6 billion Machine to Machine connections (M2M) and is expected to increase to almost 27 billion by the end of 2024.

The drastic change in these numerical itself suggests the amount of usage that the IoT environment would be witnessing in recent years to come. This would contribute to a major portion of the digital economy of any country. The revenue of the IoT industry is also expected to grow from $892 billion in the year 2018 to about $4 trillion in the year 2025[2]. Numerous applications are being covered by making using of the M2M connections as most of the devices are connected to each other and the transmission of the signals occurs between them. Some of the popular applications making use of these connections are smart cities, smart retail, smart environment, smart farming and many more[3]. The near future would see a drastic change where the devices would be communicating to other devices rather than being communicating to the internet. SIoT(Social IoT), is one of the newly emerging concepts that have the capability of enabling various users using social networks to get their devices connected to each other on a sharing basis[4]. As there are numerous other applications too which makes use of IoT devices, the need for security and privacy comes into the picture. Numerous data are being transmitted through these devices and there exists a need for them being protected from various types of attacks and attackers. users being connected to the

Numerous security and privacy attacks have already been deployed worldwide and numerous data have been attacked by various kinds of attacks. The destruction of this data has also made a heavy loss to the economy of the country too. One of the most popular one being the Mirai Attack that occurred during the last few months of the year 2016 which almost infected about 2.5 million devices that were connected to the Internet. The attack launched a DDoS (Distributed Denial of Service) to all the connected devices. There were numerous other attacks too after Mirai, such as Hajime and Reaper which launched botnet attacks a large amount of IoT devices[5]. The low cost and low powered IoT devices make the devices to pay a gateway for being attacked by numerous types of attacks and make it less secure. But still, it is widely used in numerous homes and corporate world by making it less prone to being attacked by the attackers. Numerous applications were also built to immerse the IoT devices into the human body and use it for various purposes. This was majorly used for monitoring the human body and alerting the user on various parameters[6][7]. This also paved a way for the attackers to get access to the users by locating their exact location and could also falsify the data of the individual. Tough such types of attacks have not been performed in real life but would lead to a severely dangerous situation for the individual if it gets attacked by any kind of attacker.

Yuchen et al. [10] presented a summarization of various possible security issues in her research work pertaining to IoT applications and devices. In [11], the authors have discussed the major security issues pertaining only based on location-based services in an IoT environment. The authors of the paper have also viewed the various problems relating to positioning and localization IoT devices. In [12], Anne et al. have discussed the security issues being attacked on various IoT middleware and also has discussed various protocols that could be used for overcoming these attacks. Trust remains one of the key issues in the IoT environment.

M. Guizani et al. [14], has done a detailed survey on various techniques in trust management including the advantages and disadvantages of each and every technique. Some of the security mechanisms pertaining to Software Defined Networking (SDN) and also Network Function Virtualization (NFV) are discussed by the authors in [13]. Edge Computing is an emerging technology that is used in numerous other technologies. In [8] and [9], the authors have done a comparative study on traditional cloud systems in order to secure various IoT devices. In [9], Lin et al. have portrayed the relationship that exists between various IoT and Fog computing technologies. Security issues that pertain while using Fog Computing have also been discussed in this paper. The term Smart cities include Smart homes, Smart Traffic, Smart utilities and many more. For this, all the devices need to be secured enough for maximizing the overall quality of the people using the technologies [15]. Numerous ways of development are done for making the cities smarter as governments are giving full encouragement in the development of the cities through numerous incentives [16].

The introduction of Smart Grids has paved a way for electricity theft[17]. All the electrical equipment is being connected to smart meters and the information being collected from these resources a falsified or misused. Intentional intrusion in most of the communication systems that are being used by the consumer or an adversary could be modified where the information is being collected, leading to monetary loss[18]. Some of these companies include Apple, Home Depot, JP Morgan Chase and Sony [19].

Numerous cases regarding home burglaries have increased rapidly after the deployment of various home automation systems [20]. This survey has brought us to develop unique models and security terms for securing the grey area of the IoT environment.

III. PROPOSED SECURITY MODEL

There have been numerous existing systems that are proposed to reduce the level of security risks pertaining to the IoT environment. The various device is being used and each device needs to be protected in each and every layer to make it less prone from being attacked by the attackers. IoT platforms provide various standards or risk-driven features that tend to make the application being deployed more safe and secure. The proposed security model in this research paper could help numerous companies in the corporate world for securing their devices and also the information is stored and transmitted in these devices. Some of the proposed recommendations are to perform valid threat modeling assessments at each and every security layer, which includes all the devices, gateways, and even the connected cloud/ IT infrastructure. The information needs to be gathered from the threat modeling analysis and a tailor penetration needs to be performed in order to assess various vulnerabilities present in each and every layer.

The choice of choosing static or dynamic analysis to be performed could be based on the particular availability of code. A detailed review of the most common occurrence of the attack surfaces, including the communication protocol and also the authentication present between both endpoints, fail-safe devices, and the exposures associated with the hosting infrastructure, such as the gateways. Enumerate attack routes, such as physical access points, communication channels, connecting applications, interfaces, and consuming services. This assessment should be tailored to each attack point in the respective layers. Fig.2 shows the proposed system and the security models in detail, this system will be used in any platform for securing the information and the network from the attackers. The following are the features of the proposed security model:

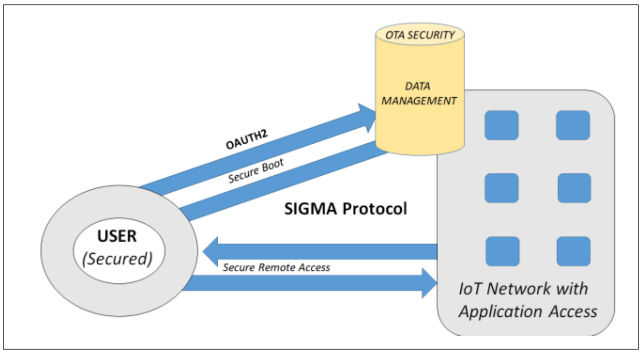

Fig. 2. Advanced Security Model

A. One way Secure boot: The choice of microcontroller; the possibility of having trusted platform modules for segregating secure operations; the use of specialized security chips/coprocessors; and the application of cryptographic modules in line with standards such as FIPS 140-215 to determine the longevity of a design and the resilience of the finished product over time.

B. Data management: The sophistication of authentication mechanisms is largely related to the choice of hardware and specifications. Authentication form factors (shared keys, user name/passwords, certificates, etc.) and current protocols are consolidating. Enterprises should develop strong device identification and authentication processes to ensure that only authenticated IoT devices are integrated with their centralized network. Extending this further, companies should ensure that devices have authorization restrictions and use encryption to secure code and data. Organizations should limit the data they collect and retain, and dispose of it once they no longer need it since unprotected data can provide attackers with ways to jeopardize IoT networks. Placing data defenses near data sources will help reduce/eliminate the risks emanating from compromised data.

C. Framework for Governance: A sound governance policy is critical for effectively managing devices, people, information, and other entities within an IoT environment. Device binaries should include signatures that identify them to a common gateway policy engine and govern the devices throughout their lifecycle from registration to key management, OTA, and data communication across the enterprise. Protocols such as OAUTH2 were used as guidelines for securely sharing information.

D. OTA Security: Performing OTA (over the air) updates is one of the most challenging elements of a robust product/solution. The process involves three distinct phases: secure production of the OTA bits, secure transport, and updating the bits on the target device. Updating binaries should take into account practical challenges, such as network bandwidth, the security of the adopted channels (open, proprietary), and the time it will take to complete an update. Secure OTA binaries can employ basic Public Key Cryptographic Standards (PKCS) for secure packaging and messaging. This is key since updated endpoint security software is necessary to keep IoT devices from being compromised.

E. Secure remote access: Malicious attackers often target the most obvious vulnerabilities – weak admin credentials, open ports, and unpatched operating systems – to gain remote access. So we focused on improving the resilience of these assets by carefully considering and strengthening their communication protocols, key management (and rotation) strategy, and their ability to render a compromised device to an uncompromised state in the event of a security breach.

F.Self-Awareness: System consider both external and extraneous factors such as weather and human actions (deliberate or inadvertent), which add dimensions to conventional threat modeling. Equipping IoT devices with contextual intelligence help in building self-awareness. Using this repeated software design principle comes in very handy in the connected world, particularly since the context imposed on these devices is far more imposing than on a typical software system.

While advanced machine learning and artificial intelligence are still not commonplace, improvements in processing power and protocol standardization enable devices to fail safely and in context.

G. SIGMA Protocol: One of the most popular protocols used for two-party key exchange widely being used id the DH protocol known as Diffie-Hellman protocol. It is well known that the protocol is not an authenticated key agreement protocol, it becomes one of the strongest bases in building numerous other protocol using it. One of the most important disadvantages of using this protocol is its vulnerability to the man-in-the-middle attack. In order to overcome this challenge numerous protocols were being proposed which included the STS protocol, SIGMA protocol and Photuris protocol. But, most of them had their own disadvantages which were recognized while making it used in real-time scenarios. But SIGMA protocol was distinguished from it as no attacks were identified while making use of it. SIGMA protocol takes its own advantage of making use of the public key infrastructure and also securing the communication inside the network.

IV. RESULT EVALUATION

We have achieved the security level to 90 % on comparing with the existing system as shown in Fig 4. NS3 simulator was used to see the weight of the system. Some models are used to reduce the attacks inside the network as well as on the application layer.

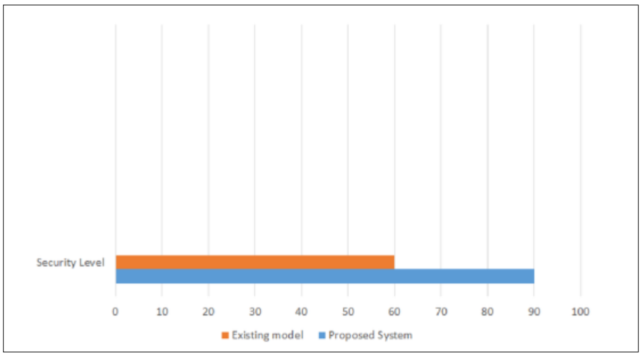

Fig. 3. Security Level

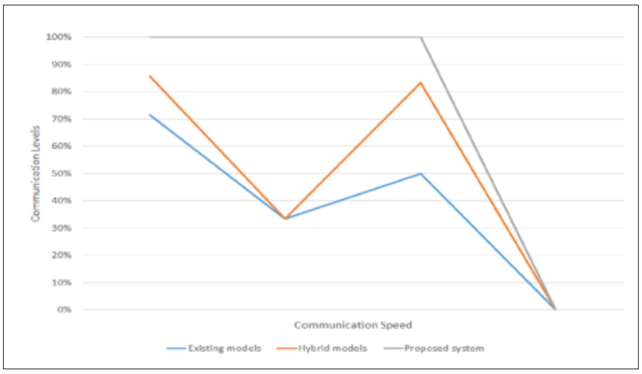

Fig. 4. Communication Speed

We have also achieved the communication speed is stable with a hybrid comparison. Some models have more weight on security without achieving the speed but this model has reached stable communication speed as shown in Fig.4. In Fig. 5, by testing our models, we have noted more attacks are reduced.

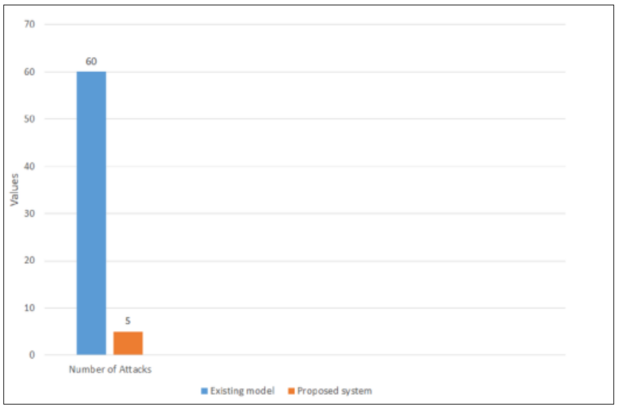

Fig. 5. Minimization of Attacks

V. CONCLUSION

In this paper, we have analyzed the various security issues in the IoT environment and implemented a new model for targeting the grey area. We have introduced various security models that could be deployed in various levels of the devices used in an IoT application. The paper discusses various security-related issues that could be attacked on various layers such as the network layer, application layer and middleware. Numerous open issues regarding the security issues in an IoT environment have been discussed and a model is suggested for making the application more secure. The designed model is compared with the existing models and the communication speed is evaluated.

It is noticed to have a higher speed and also various other factors have been evaluated such as the number of attacks and the amount of security encrypted in each and every layer. Various open issues and issues that originate from the solution itself have also been discussed. We have achieved a security level and communication speeds up to 30 % in the proposed method. In the future, the energy consumption of the devices could also be taken into account which could be minimized by decreasing the model weight and layer security.

REFERENCES

1. R. Kandaswamy and D. Furlonger. Blockchain-Based Transformation. Accessed: Jun. 5, 2018. [Online]. Available: https://www.gartner.com/en/doc/3869696-blockchain-based-transformation-a-gartner-trend-insightreport/
2. GSMA. Safety, Privacy and Security. Accessed: Jan. 29, 2019. [Online]. Available: https://www.gsma.com/publicpolicy/resources/safetyprivacysecurity-across-mobile-ecosystem/i
3. T. M. Fernández-Caramés and P. Fraga-Lamas, ‘‘A review on the use of blockchain for the Internet of Things,’’ IEEE Access, vol. 6, pp. 32979–33001, 2018.
4. M. Frustaci, P. Pace, G. Aloi, and G. Fortino, ‘‘Evaluating critical security issues of the IoT world: Present and future challenges,’’ IEEE Internet Things J., vol. 5, no. 4, pp. 2483–2495, Aug. 2018.i

5. Flashpoint. Mirai Botnet Linked to Dyn DNS DDoS Attacks. Accessed: Dec. 18, 2018. [Online]. Available: https://www.flashpointintel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/
6. G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, ''IoT-based remote pain monitoring system: From device to cloud platform,'' IEEE J. Biomed. Health Inform., vol. 22, no. 6, pp. 1711–1719, Nov. 2018.
7. A. Mosenia and N. K. Jha, ''A comprehensive study of security of Internet-of-Things,'' IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4, pp. 586–602, Dec. 2017.
8. W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, ''A survey on the edge computing for the Internet of Things,'' IEEE Access, vol. 6, pp. 6900–6919, 2018.
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, Oct. 2017.
10. 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, Oct. 2017.
11. L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, ''Robustness, security and privacy in location-based services for future IoT: A survey,'' IEEE Access, vol. 5, pp. 8956–8977, 2017.
12. A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, ''IoT Middleware: A survey on issues and enabling technologies,'' IEEE Internet Things J., vol. 4, no. 1, pp. 1–20, Feb. 2017.i
13. I. Farris, T. Taleb, Y. Khettab, and J. Song, ''A survey on emerging SDN and NFV security mechanisms for IoT systems,'' IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 812–837, 1st Quart., 2019.i
14. I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, ''Trust management techniques for the Internet of Things: A survey,'' IEEE Access, vol. 7, pp. 29763–29787, 2019
15. A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, ''Smart cities: A survey on data management, security, and enabling technologies,'' IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.
16. D. Eckhoff and I. Wagner, ''Privacy in the smart city—Applications, technologies, challenges, and solutions,'' IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 489–516, 1st Quart., 2018.
17. X. Xia, Y. Xiao, and W. Liang, ''ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 445–458, 2019.
18. V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, ''Toward a secure wireless-based home area network for metering in smart grids,'' IEEE Syst. J., vol. 8, no. 2, pp. 509–520, Jun. 2014.
19. N. N. Dlamini and K. Johnston, ''The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review,'' in Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE), Nov. 2016, pp. 430–436.
20. A. C. Jose and R. Malekian, ''Improving smart home security: Integrating logical sensing into smart home,'' IEEE Sensors J., vol. 17, no. 13, pp. 4269–4286, Jul. 2017.

AUTHORS PROFILE

Mr. S. Mani is presently in the Department of Computer science and Engineering at Nehru Institute of Engineering and Technology, Coimbatore, Tamilnadu, India. He has got his M.E. in Computer Science and Engineering from Sri Ramakrishna Engineering College, Coimbatore. He has more than 10 years of Teaching and Research Experience. His research interest lies in the field of semantic web, Artificial Intelligence, Information retrieval and IOT.

Dr. V. Saravanan is currently working as an Assistant Professor in the department of Computer Science Engineering, Dambi Dollo University, Oromia Region, Ethiopia. He completed M.E. and Ph.D. degrees in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, India. He has more than 12 years of Teaching and Research Experience. His research interest lies in the field of Mobile Computing, Wireless networks and IOT. He is a member in C.S.I and I.S.T.E.

Dr. T. Samraj Lawrence is currently working as an Assistant Professor in the department of Information Technology, Dambi Dollo University, Oromia Region, Ethiopia. He completed M.E. and Ph.D. degrees in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, India. He has more than 12 years of Teaching and Research Experience. His research interest lies in the field of Mobile Computing, Wireless networks and IOT. He is a life member in I.S.T.E.

Dr. G. R. Sakthidharan is currently working as Professor in the department of computer science and engineering in GRIET, Hyderabad. He had completed his B.E in Periyar University, Salem and M.Tech in S.R.M University, Chennai. He was awarded Ph.D. on November, 2014 under Anna university, Chennai. He is holding 14 years of experience. He is life member in C.S.I and I.S.T.E.

Mr. M. Veluchamy is presently working as an Assistant Professor in the Department of Computer Science at Periyar University Constituent College of Arts and Science -Idappadi, Salem, Tamil Nadu, India. He completed M.C.A and M.E in Anna University, Chennai. He has completed UGC-NET in Computer Science and Applications. He has published 6+ Journals and conference papers. He is doing research in the field of Trust based security mechanism implementations in Internet of Things environment. He has 9+ years experience in teaching.