MEMS, RFIDS AND SENSORS: THE KEY ENABLERS OF INTERNET OF THINGS

Ravinder Korani[1], Dr. P. Chandra Sekhar Reddy[2]
[1]B. Tech, M. Tech, (Ph.D.), Associate Professor, ECE Department,
Shadan College of Engineering and Technology, JNTU, Hyderabad, India
[2]B. Tech, M. E, M. Tech, Ph.D. Professor & Co-ordination, ECE Department, JNTU, Hyderabad, India

Abstract

The Internet of Things includes the establishment of a network between resource-limited equipment such as sensors, MEMs, and RFIDs, however these networks often face challenges of security breach, less reliable connectivity. Some of the researchers suggested the implementation of malware defending strategies like data encryption, but the possibility of wireless intrusion from inside the 6LoWPAN continues to exist. As these within-network intrusions are highly likely to cause damage, incorporating effective malware identification strategies is mandatory. IoT technology continues to gain wide attention from both business and residential consumers globally. The flow of numerous devices with connectivity requirements and growth in internet access worldwide is encouraging companies and researchers to focus on developing new technologies. Specifically, most of the current studies are working on handling intrusion issues while boosting the speed and performance of proposed technologies. The current safety scenario depicts that no malware identification methods adhering to the needs of the IPv6-connected Internet of Things have been in-built. This is due to the fact that current approaches of malware identification in the context are designed by tailoring the WSN and traditional internet approaches. The current research work analyses the available models, implementation approaches and assessment of new defensive strategies proposed for IoT environment. The study basically explores the nomenclature of the existing framework, needs, potential intrusion and counter-defensive possibilities. Further, the current studies associated with safety and malware identification in IoT is provided. The research identified that the current approaches possess large limitations in identifying attack nodes associated with specific features like sink-hole or selected packet forwarding intrusions. Further, the research suggests that a huge scope and requirement for handling malware identification and designing defensive strategies in IoT environment. Humans interact with the environment through their senses Sensors can enrich human interaction with the surroundings Sensors create a more interactive and immersive world.

Keywords: IoT, WSN, defensive strategies, Sink-hole attacks, malware identification, IPv6 Protocols, attack nodes, and selective forwarding.

OVERVIEW

The IoT is a continuously developing network that consists of numerous sensors, MEMS, and RFID objects. These sensors, MEMS, and RFID objects include a range of computing or cellular devices and also physical devices such as watches, wearable sensors, MEMS, and RFID objects and many more smart devices, as referred in [1], [2]. In addition, IoT is often referred as an intrinsic relationship of nodes and actuators, which comprise a specific architecture to ensure reliable and effective information distribution. It is significant to note that, the IoT operates with any kind of existing contemporary approaches and improves it to achieve the maximum range [3], [4]. Thus, it is clear that, the IoT not only applicable to a particular approach. Moreover, when every

connected system is turned into a smart device, IoT automates an effective information and network administration. In addition, it also improves the system efficiency by employing Machine-to-Machine communications. By using nodes, the automation of user data and the direct interaction of specified solutions to particular things will also be carried out [5], [6]. Malicious nodes always try to absorb the sensitive data which is transferred between sensors. This exposes the IoT framework to malware intrusion. However, numerous studies have been illustrated to describe such risks in various IoT dependent smart devices such as automobiles [7], baby monitoring devices as shown in [8], therapeutic devices [9], and lights [10]. As, most of IoT's nodes utilizes cellular communication technologies to perform efficient data transmission, they face challenges from the attacks of eaves dropping and MITM. In addition, tampering is also one of the major attacks in the IoT, as IoT nodes are not addressed.

On other dimension, each MEMS accelerometer varies with others on the basis of certain bias parameter which is specific to that particular equipment. Such bias is apparent in all MEMS devices because of mild flaws unforeseen during the manufacturing stage. Because a MEMS accelerometer is not electronic equipment but a mechanical one, pressures can be felt during any stage in the manufacturing procedure. For example, the bias can occur during the assembling stage or even during the soldering stage or mounting stage as a result of pressure observed from the panel. Accordingly, the bias can be described as a function of several independent parameters, which are not always within the manufacturer's control sphere. This is because one or several factors can induce the bias and the complexity in the process is that not always such parameters are estimated in advance. The studies in [11] and [12] successfully demonstrated that an accelerometer can be employed for equipment detection [13].

The existing cryptography models like universal key cryptography are highly expensive in terms of power and frequency, to execute on IoT networks [14].

Enterprises of all sizes have their primary focus on minimizing operational overheads and other associated costs as much as possible. Thus, all enterprises frequently monitor for effective strategies and solutions to enhance the security of the system, error tolerance, ability to adapt system changes, as well as cost effectiveness. These solutions are likely to widen the complexity and the data transmission across the enterprise systems. Among the solutions, IoT is one of the significant solutions to tap the present requirements of diversified commercial enterprise applications. IoT includes numerous features of cloud computation. Generally, IoT refers to a distributed network which includes nodes, servers, as well as software. This allows quick sensing of data spontaneously, leading to a straight communication infrastructure among cyber-physical applications.

This kind of technique is significant to achieve enhanced efficiency in both data creation and data utilization, resulting into numerous economic advantages, as depicted in [15]. Continuously emerging developments of IoT lead to have various types of IoT applications that contribute to the daily lives of individuals. They range from conventional devices to typical residential devices that assist in making lives of human beings to become extreme better. Hence, it caters a massive prospective, as depicted in [16].

The Internet of Things technology empowers the real-world equipment to communicate among themselves and finally, with the internet. Communications between the internet and real-world devices [17] involves some serious threats, mostly in terms of security breaches and unauthentic information access. Because the interactions occur over numerous equipment and networking environments, the probability of security breaches is alarmingly high. Limited awareness of security coupled with market forces restricts manufacturers from producing highly secure and tamper-proof equipment. Most of these real-world devices are produced without necessary features including privacy, integrity and authentication [18], [19].

Adhering to strict security norms is regarded often as an additional feature and not as a mandatory feature, which should be integrated into the device [20].

In the Internet of thing environment, security remains the most important technology due to the fact that the transmission traffic is managed by security defence mechanisms. However, due to the low volume of traffic in the embedded computer system context, the traffic remains unprotected and therefore, requires strong security defensive features. The environment confronts different and novel issues, limitations and risks which can be managed only through an efficiency security mechanism, which is compatible to traditional intrusions on ubiquitous systems.

Though, distinct studies are proposed by various researchers for the implementation of low weight cryptography mechanisms [21], they failed to secure the network environment, predominantly from the intrinsic intruders.

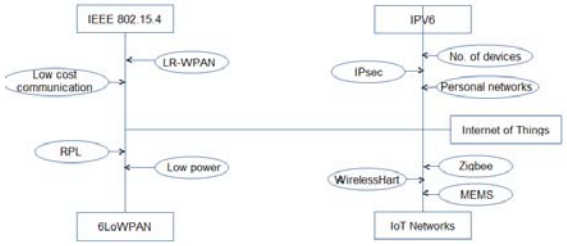

Figure 1: Functional flow of Internet of Things (IoTs)

IoT networks together with low-power devices and resource limited internet devices are increasing the number of device types, which can be linked to internet via IoT. In particular, Internet Protocol Version 6 [22] and a standard IEEE 802.15.4 specification [23] are vital in providing new addresses and places additional elements and networks across the IoT environment. As depicted in Figure 1, the existing technologies are essential in the conversion of internet into IoT. A noteworthy point is that, various protection threats in a completely developed Internet of Things environment enables scholars to focus on developing most efficient IoT embedded smart devices with more protection. Such secure device introductions will obviously fulfil the emerging demand of IoT smart systems. Distinct protection challenges are present in the proposed structural designs and its related technologies, which supports the IoT [24]. Further, a tolerable delay might be unacceptable in IoT case, as a late acknowledgment could be considered as severe as like a DoS attack in real-time systems. Few of such systems include traffic monitoring systems and emergency systems. Thus, efficient information exchange through selecting a suitable path is also significant in IoT networks.

In [25], IPv6 routing protocol referred as RPL is proposed. This protocol is primarily designed for the systems, where the utilization of power is low. RPL plays a significant role in IoT networks and includes traditional security methods only. RPL is lack of unique information security measures. Though, numerous studies have been carried out to overcome the risks associated with RPL, the protocol still includes severe security challenges. The attacks which are present inside the protocol are hardly determined in comparison with the extrinsic attacks of the protocol. The possibilities of executing a DoS attack using the flaws of RPL remains a major challenge. The utilization of RPL protocol and 6LoWPAN as depicted in [26] resulting into distinct security challenges. In addition, defects which are exist in the network technologies are likely to compromise and finally, generate a Botnet attack outside the Internet of Things systems. The methods of IDS and firewalls protection have to be enough strong and must have capability to analyze the diversified security threats in the protocol.

Internet of Things

The IoT is used to inter-connect the various networks of physical systems, buildings, and distinct sensors, MEMS, and RFID objects equipped with electronics, sensing nodes, and machine components for movement. In addition, it acts as a network connectivity to permit the sensors, MEMS, and RFID objects for collecting information and also allows efficient information transmission as described, During 2013, the IoT-GSI explained IoT as “a globally recognized architecture employed for the digital world to provide highly advanced solutions by the interconnection of both physical and virtual objects depending on available and emerging data and transmission models".

Here, a “thing” is referred to either "the physical devices or virtual data that is detectable and combinable in transmission networks".

Internet of Things permits various things to be sensed or managed remotely in the network framework. Thus, generates numerous prospects for further combination into computerized devices. In addition to improved accuracy and efficiency, it also achieves cost-effective process and minimizes human interaction as explained . Each and every object is analyzed in a unique way based on integrated calculating object, but is capable of functioning in the available network framework. Most of researchers predict that, by the end of 2020, Internet of Things will comprise nearly 30,000 million of sensors, MEMS, and RFID objects.

The following graphical representation is given by Senior Research Analyst John Greenough in THE INTERNET OF EVERYTHING: 2015 [SLIDE DECK] manuscript. The contribution details about the IoT market growth outlook to 2019.

Table 1: Number of devices in internet of thing

	2014	2015E	2016E	2017E	2018E	2019E
Internet of Things	10	15	17	22	29	34
Connected Cars	6	8	10	10.5	11	12
Wearables	6	7.5	9	10	10.5	11
Connected/Smart TVs	5	6	7	7.5	**1.1 8**	10
Tablets	4.5	6	7	7.5	8	9
Smartphones	3	4	4.5	4.8	4.9	5
Personal Computers	2	2	2	2	2	2

The structural design of IoT must still be standardized. Various international organizations such as ITU and IEEE are majorly conducting their research on IoT to ensure that it is standardized. However, researchers already proposed few efficient technologies to perform as the basis for the IoT effectively. These technologies include Internet Protocol version 6, 6LoWPAN networks, a technical standard IEEE 802.15.4, a routing protocol (RPL) and etc. are together used to meet the diversified internet requirements in the future.

Accordingly, there exist efficient structural designs of IoT, which are proposed by various famous researchers and other research groups in internet field. Most of them are designed by employing both transportation and support layer to tap the requirements of IoT sensors, MEMS, and RFID objects. Moreover, these novel developments further employ the techniques of cloud computation for support layer. The general structural design of IoT, is depicted in below Figure 2.

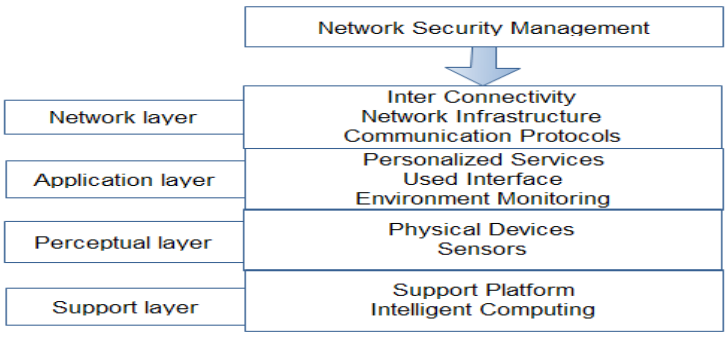

Figure 2: IoT Architecture

The structural design of the IoT is generally classified into four IoT layers. Few devices use various technologies like internet processing to support the network.

- Perception Layer is the most significant layer of Internet of Things. Perception layer is not only limited to the collection of data, but also involved in observing any kind of data which is employed in IoT network. This data is recorded by utilizing various smart devices like the RFID, pressure, rhythm, temperature sensors and GPS . Perception layer is categorized into two segments including the perception node and perception network. The Node is employed for controlling the information and the network transmits data to the specified controller [15].
- Network layer is also called as transportation layer. This layer has enough abilities to transmit information from bottom most layer to top-most layer, as depicted . Transport layer also has ability to conduct data transmission through the internet. Hence, as explained in , an efficient network layer combines a range of heterogeneous networks.
- The Support layer includes information processors, which are used to convert one data type to another. The final transformed data is saved in a massive database for further usage when it requires. It operates in close proximity with applications. Hence, many of research workers desire to locate it in proximity to application layer .
- Protection at application layer is also known as object security. It has the capability of maintaining end-to-end and the safety feature can be incorporated for each data packet. The COSE is significant and strong base for object security . This layer is also called as service layer. It is primarily engaged in altering certain data into value added content. In addition, it also offers an efficient UI to the end users. One of the major issue of service layer is that it involves in sharing information with adjacent groups in a most encrypted manner, thus, an intruder cannot access that data.

IOT and Security Protocols in IOT Layers

Data exchanges in IoT have to be secured through using various protection services, which are defined in the above section. By employing standard protection methods, transmission security at diversified network layers is offered. The Table 2 depicts different safety and IoT protocols at each layer.

Table 2: The above table depicts the various IoT with security protocols in diverse layers

IoT Layer	Security Protocol	IoT Protocol
Network	IPsec, RPL security	IPv6, RPL
Application	User-defined	CoAP
Data-link	802.15.4 security	IEEE 802.15.4
6LoWPAN	None	6LoWPAN
Transport	DTLS	UDP

IoT Security

Like sensor, internet and Cellular networks, the IoT networks also have various security problems. Additionally, it also deals with specific problems like, confidentiality problems, various verification as well as access control challenges, data storage and data administration and etc.

The IoT's security services are primary aimed at providing suitable verification methods and also have major focus on data privacy etc. In particular, for developing efficient protection methods, IoT comprises three major things including privacy, reliability and accessibility of information. A break-down in one of above parameters could result into face severe system

challenges. Hence, these parameters are crucial in developing security methods.

Information and privacy security is among the major application threats of Internet of Things, as explained in [43]. In IoT, RFID, WSNs sensors check for information technology that secures the data privacy through incorporating a security password . Different methods of data encryption like hash model, hash-chain protocol, obtaining secure key from network .

THE CONTEMPORARY MODELS OF IOT SECURITY

Efficient IoT mandates incorporation of robust safety measures, specifically for information transmission. However, several programmers often ignore the vital security aspect in the communication phase. The IoT equipment and appliances are often tiny and cannot accommodate much hardware mechanism to support the safety measures given their size restraints. To address this issue, multiple proposals have been put forward by researchers in the field but as the IoT is based on a discrete communication model, a single solution cannot be sufficient for ensuring complete safety.

A few of the prominent research works put forward in this context include . Codo solution is regarded as an extended version of Coffee solution. I.E Bagci put forward storage and transmission architecture, deploying the principles of the onIPv6/6LoWPAN protocol. This protocol details IPsec/ESP for security. In researchers investigated the applicability of tailor-made encapsulation approach. Their approach mixes cross-platform transmission and safety measures like data encrypting, including sign files and others so as to boost the extent of security mechanisms deployed in the entire communication process in IoT environment.

The first completely applied to and fro securitization approach was presented . The proposal is built on the basis of prevailing internet standards, mainly the Datagram based DTLS. This DTLS is applied between layer 4 and layer 7 in the OSI. RSA cryptosystem forms the basis for the securitization technique and it can work over IP version 6 in low-power WPANs.

To ensure the integrity of the communication system and ensure data to be free from unauthentic deliveries, the research work in the proposed an in-depth analysis on the process of extending the prevailing management concepts to the IoT securitization. Often, management concepts are studied under four sub-segments- primary pool phase, computational phase, discussion phase and public phase. However, after experimenting on these concepts, the investigators reached a conclusion that only a few of these management protocols could be extended for application in IoT environment.

A different technique that can be adapted in the real-time environment was put forward in . It developed a communication prototype with inbuilt data encryption, signature inclusion to cater the safety norms of IoT through ONS concept.

Based on the organized security control concept put forward by , the researchers came up with a novel approach involving an organized and calculated method for achieving safety in IoT environment. These ideas are built on the basic assumption that any safety mechanism for any given entity irrespective of its functioning commences from the micro-stage.

Further, advances to the work are proposed , who attempted to implement the organized and calculated method through framing contextual programs in the tetrahedron.

To strengthen position isolation in IoT context, k-anonymity opts for detecting devices on an intellectual basis.They depicted that maximum utilization of Snort abilities over WMN environment is not feasible in practice. The study suggested PRIDE to deploy Snort features to WMNs. The PRIDE approach divides the features throughout the network.

A self-defending approach relying on attribute detection through virtual neurons and an anomaly driven detection system for WSNs through Dendritic -Cell programming was put forward.

The authors in suggested steaming tags that strengthen the original information flows. This enables consumers to use a wide range of language comprehension options to append data to occurred scenarios.

In the study put forward an extension of the solution suggested in terms of varying control of the information flowing on the basis of Aurora method. Architecture bears both real and aggregate type advantages along with general and window restrictions. The consumers are categorized on the basis of a role-driven method and accordingly, access authority is given on the basis of the role and not on the basis of the consumer like in RDBMS.

Further, the study devised a protocol for protected information transmission based on pre-fixed time durations for IoT environment along with VANET environment.

POSSIBLE RESEARCH OBJECTIVES

IoT is an emerging area of research with numerous queries yet to be addressed, with security challenges across multiple layers in the framework and from diverse forms of data safety to be handled. The below subchapters present observations and brief of general challenges ahead of researchers working for improving safety in the Internet of Things environment.

- Establishing interconnection between devices and persons using sensors and assuring connectivity between them remain major limitations in IoT. Further, unreliable and poorly stable internet connection remains tough task in the environment. Accordingly, the researchers need to focus on resource saving sensors, MEMS, and RFID objects to boost network connectivity with the assistance of power saving strategies
- Though studies aimed to handle this issue, no generally accepted standards have been framed in IoT.

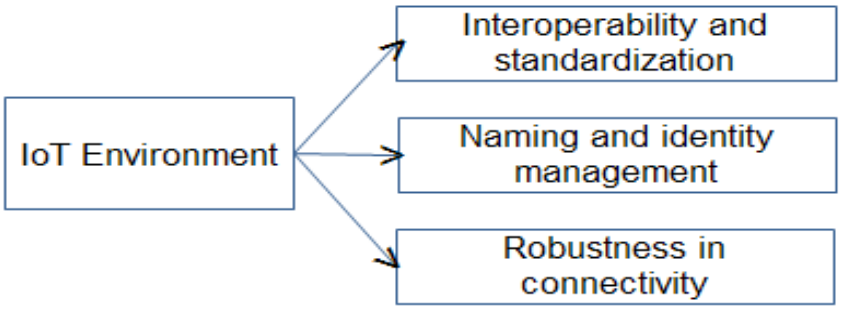

Figure 3: Analysis of current studies and Future scope of Research in IoT

- The sensing nodes function as automated sensors and then conduct data transmission to the sub-system in the connection. Accordingly, it requires engaging efficient data encryption techniques to ensure information integrity in the data processing layers. Further, defense techniques should be designed and extended to guarantee the data communication and safety against intrusion or unauthorized transmission data usage [90].
- Client information and user data confidentiality remain a priority challenge in IoT safety due to the omnipresent feature of IoT connectivity. Devices are interconnected, information is transmitted over the internet, leading to client privacy being a targetable aspect of several studies . Despite multiple studies being conducted addressing privacy issues, several areas need to be addressed as a future scope of research. Confidentiality in terms of information gathering coupled with information transmission and sharing, information safety measures continue to be present as future work issues to be addressed.
- The addressed the standard issue, as a complete over-time, combining safety mechanism of every infrastructure layer could not incorporate the safety in-depth of the structure, so this remains a key limitation and priority study area, to build safety infrastructure by integrating control and data.
- Several resource-limited sensors, MEMS, and RFID objects are often observed in the ‘Internet of Things’ environment that possesses small power backup and limited battery efficiency. Despite different

cryptosystems and safety protocols have been put forward for IoT devices, most of these mechanisms are unsuitable for sensors, MEMS, and RFID objects with limited power capacity. For example, studies attempted to provide solutions for handling such devices in the IoT context.

- Key Management is a primary basis of high safety functioning and continues to remain the primary study topic. Among cryptographic safety mechanisms, this area is the most complex issue. However, no optimal suggestions are put forward for this study. Low weight cryptographic programming or better efficiency of sensor nodes is yet to be implemented. To date, the actual large-scale network is not often implemented. The challenges of internet safety must be given high preference to and emerge as the potential points and challenges of study in the IoT context .
- Laws and norms of safety measures are yet to be the main focus, and standardization is yet to be achieved regarding the IoT device operations. It is mainly linked up with country-level safety data, potential secrets and individual confidentiality. Accordingly, a nation requires legal support to support IoT growth and therefore, government policies gain utmost importance. This provides huge research scope.
- IoT environment is always susceptible to attacks from malware programmers due to limited security support currently being provided for devices in the network. One such intrusion was recently detected in 2013. The studies in advocated the possible challenges and the need for effective malware defines mechanisms for uninterrupted and confidential transmission of information in IoT.The study put forward the problem of malicious software for IoT.

Ensuring system efficiency: Growth in WSNs, RFID, persistent calculating solutions, a transmission mechanism, and DCS, CPS- an evolving type of IoT, is evolving as an actuality. Accordingly, potential safety is required for ensuring system efficiency.

Numerous shortcomings , which should be managed are provided in the following Table.

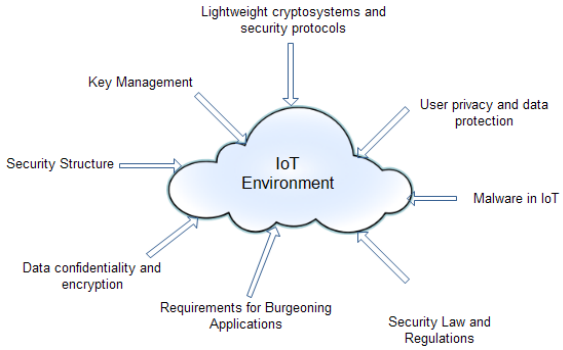

Figure 4: Confidentiality and Data security in IoT Network

Table 3: Security Limitations

Resource Limitations:	In IoT framework, several nodes do not have adequate storage, energy and computing power. The frameworks typically utilize minimum bandwidth transmission paths. Accordingly, it is challenging to implement certain a few safety mechanisms like frequency hopping transmission and universal data encryption program. In such conditions, implementing safety mechanisms is challenging.
Ensuring Confidentiality:	As a large volume of RFID schemes lack adequate authentication methods, an intruder can always trace tags and detect the ID of the devices holding these IDs. Malware writers can both access the information as well as tinker the information or completely erase
Automatic management:	Conventional systems require consumers to configure and

	implement these systems to diverse domains and transmission networks. But, the devices must set up interconnections on a real-time basis, and configure the systems to operate over different applications. Such control includes different methods like auto-configuring, auto-optimizing, auto-protecting etc .
Device-to-Device Compatibility:	Related safety mechanisms must not restrict the operability of different sensors, MEMS, and RFID objects connected in the IoT environment
Achieving Scalability:	As numerous devices and nodes are prevalent in IoT environment, suggested safety techniques must achieve adequate scalability
Information amount	Despite a few IoT functions utilize simple and non-frequent transmission paths, multiple IoT mechanisms like sensor-driven, transportation and huge-scale conditions, which possess large ability to handle bulk information in servers.

Safety mechanisms are evaluated in research works in various aspects. The concepts handled in multiple works are presented in the Table 4. Further, the safety needs are provided in the Table 5.

Table 4: Security Requirements

Permission:	Limited number of permissions should be given to sensors, MEMS, and RFID objects and platforms to ensure that they cannot access the non-required applications
Non-tampered:	Associated data must be ensured that it is not tampered
Legitimacy:	Only authentic consumers must be permitted to use the network and confidential data
Privacy:	Data transfer among nodes must be shielded from malware attacks
Sustainability and Accessibility:	Evading all possible operational issues and ensure sustained availability of safety mechanisms must be guaranteed

CONCLUSION

The environment permits sensors, MEMS, and RFID objects to interconnect instantaneously on a real-time basis, through any possible channels and solutions. Most IoT targets involve generating smart networks and authorized sensors, MEMS, and RFID objects. Multiple issues associated with IoT are being observed. Based on this research, we can depict that it is important to set up the optimal safety infrastructure. The primary purpose of the research work has been to present the overview and analysis of the prominent issues and dimensions of IoT with primary emphasis on the potential issues associated with the context. Key management in the huge-scale environment remains a tough task, and the laws associated with IoT operating environment remains a tough task. A strong constraint of the present IoT networks is the intrusion detection, defence and prevention strategies, which observed through the review carried in this manuscript. Unlike the other networks, the device placement and dynamic inclusion of the devices are two critical factors in IoT, which are often provides scope for vulnerability at network access and communication. This indicates the obvious scope for future research, which is in the direction of providing novel intrusion detection strategies for IoT.

REFERENCES

1. Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions." Journal of Cleaner Production 140 (2017): 1454-1464.
2. Botta, Alessio, et al. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684-700.

3. Odelu, Vanga, et al. "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size Keys and ciphertexts." IEEE Access 5 (2017): 3273-3283.
4. Kong, Linghe, et al. "Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: Overview, design, and challenges." IEEE Communications Magazine 55.1 (2017): 62-68.
5. Ab Malek, Muhammad Syafiq Bin, et al. "On privacy verification in the IoT service based on PN 2." Consumer Electronics, 2016 IEEE 5th Global Conference on. IEEE, 2016.
6. Tewari, Aakanksha, and B. B. Gupta. "A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices." International Journal of Advanced Intelligence Paradigms 9.2-3 (2017): 111-121.
7. Internet of Things (IoT).” [Online]. Available:http://www.cisco.com/c/en/us/solutions/internet-ofthings/overview.html. [Accessed: 12-Jan-2016].
8. Tsai, Chun-Wei, Chin-Feng Lai, and Athanasios V. Vasilakos. "Future Internet of Things: open issues and challenges." Wireless Networks 20.8 (2014): 2201-2217.
9. M. Lawton, “The symbiosis of digital and physical security,” 19 February 2015. [Online]. Available: http://futurelab.assaabloy.com/en/thesymbiosis- of-digital-and-physical-security/. [Accessed 31 July 2015].
10. Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems 29 (2013): 1645-1660.
11. TRUSTED Computing Group, “ARCHITECT’S GUIDE: IOT SECURITY,” July 2015. [Online]. Available: http://www.trustedcomputinggroup.org/files/static_page_files/93061BAE- 1A4B-B294-D0F3EBD27DB68FAB/IOT_Security_Architects_Guide_TCG.pdf. [Accessed 30 July 2015].
12. Roman, Rodrigo, Pablo Najera, and Javier Lopez. "Securing the Internet of Things." IEEE, Computer 44.9 (2011): 51-58.
13. Wright, Alex. "Hacking cars." Communications of the ACM 54.11 (2011): 18-19.
14. Albrecht, Katherine, and Liz Mcintyre. "Privacy nightmare: When baby monitors go bad [opinion]." IEEE Technology and Society Magazine 34.3 (2015): 14-19.
15. Glisson, William Bradley, et al. "Compromising a medical mannequin." arXiv preprint arXiv:1509.00065 (2015).
16. Dhanjani, N. "Hacking lightbulbs: Security evaluation of the Philips hue personal wireless lighting system." (2013).
17. Bojinov, Hristo, et al. "Mobile device identification via sensor fingerprinting." arXiv preprint arXiv:1408.1416 (2014).
18. Aysu, Aydin, et al. "Digital fingerprints for low-cost platforms using MEMS sensors." Proceedings of the Workshop on Embedded Systems Security. ACM, 2013.
19. Dey, Sanorita, et al. "AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable." (2014).
20. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
21. Feldhofer, Martin, Sandra Dominikus, and Johannes Wolkerstorfer. "Strong authentication for RFID systems using the AES algorithm." CHES. Vol. 4. 2004.
22. Deering, Stephen E. "Internet protocol, version 6 (IPv6) specification." (1998).
23. Molisch, Andreas F., et al. "IEEE 802.15. 4a channel model-final report." IEEE P802 15.04 (2004): 0662.
24. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
25. Winter, Tim. "RPL: IPv6 routing protocol for low-power and lossy networks." (2012).
26. Le, Anhtuan, et al. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach." International Journal of Communication Systems 25.9 (2012): 1189-1212.