A study of Security & Authentication Mechanisms in IoTs: Research Challenges

***M.Ayasha* , M.C.A ,M.Phil,**
Asst.Professor Dept of Computer Science,
MGR College, Hosur, Krisnagiri Dist., TamilNadu

Dr.M.Savitha Devi, M.Sc,M.Phil,M.C.A,B.Ed,
Asst. Professor & HOD Department of Computer Science,
Periyar University Constituent College of Arts & Science Harur.

***Abstract*— At present, internet technology has become very pervasive, since multiple devices connected via the internet. With the emerging growth in internet technology, IoT applications are performing a significant role in the human day today life. However, many researchers stated that IoT is not secure, and various security problems are considered a major challenge for fully fledged IoT infrastructure. The existing IoT architecture faces a number of security challenges and not able to fulfill the futuristic security requirements. Therefore, to overcome such challenges, an efficient and promising "Routing Protocol for Low-power and Lossy Networks" (i.e., RPL) mechanism have been investigated to offer secure IoT infrastructure. The challenges are ever increasing, and the solutions have to be ever improving. Therefore, the contribution of this survey study is to discuss the evolution of IoT technology and security analysis over each layer of IoT infrastructure. Additionally, the survey study categorized into two folds, including secure routing in IoT and authentication mechanisms in the IoT environment. The last section concludes various research challenges that still exist in the literature, and provide guidelines to mitigate existing problems, also can help to understand new research directions to defend IoT against malicious security attacks.**

***Keywords*—Data transmission, Internet of Things, DDoS attacks, Routing protocols, IoT security.**

I. Introduction

At present, the "Internet of Things" (IoT) has emerged from technology jargon, into a high success across the range of industries. IoT is an architecture of interrelated sensor devices, digital and mechanical machines, physical objects, or humans that have the ability to communicate and transfer data entire the network without the need of human-to-human or human-to-computer interaction (Shown in Figure-1). IoT has developed with the convergence of wireless network technologies, micro-electromechanical systems (MEMS), micro-services, and the internet [1]-[5]. The following are the four key points that will be inherent in an IoT system, i) Ensuring continuous availability of IoT-based devices will be important to avoid potential operational failures and interruptions to enterprise services. ii) Disruptive cyber-attacks, such as distributed denial-of-service attacks (DDoS), could have new detrimental consequences for an enterprise. iii) Another big challenge for enterprises in an IoT environment will be figuring out how to quickly patch IoT device vulnerabilities -- and how to prioritize vulnerability patching. iv) The challenges for enterprises lie in identifying where security controls are needed for this emerging breed of Internet-connected devices and then implementing effective controls [6]-[9].

IoT is the one of the fastest globally emerged technology, with the specific research on how the security concerns for full-fledged IoT applications have been attracted to the researchers owing to the increasing requirements of secure IoT applications. There exists a number of security issues with existing models and technologies which strengthen IoTs. The security challenges in the IoT domain are enormous and interesting. Most of the IoT applications themselves are not well organized if we look from a security viewpoint. With the increasing growth of Distributed Denial of Service (DDoS) attacks in the era of IoT [10] has increased major interest in the internet world. Furthermore, the resource constraints make the restrictions upon security measurements, which included with automated devices. This is also one of the serious topic related to IoT application design and promotes further research in the development of an efficient security system.

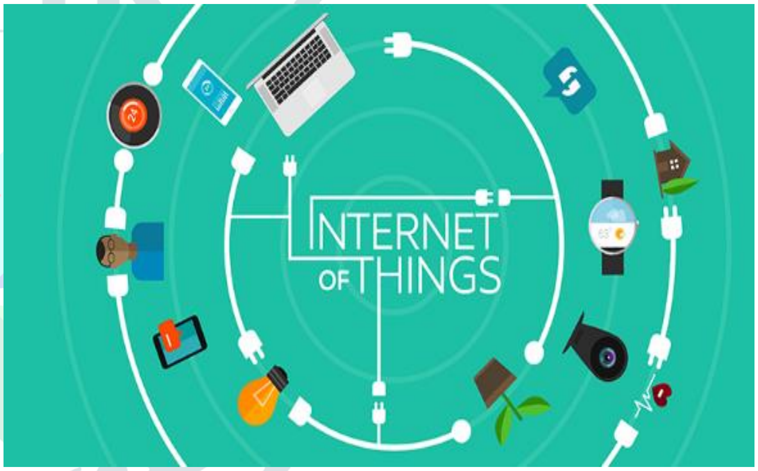

Figure 1 Rise of IoT Technology

Most of the existing studies have often considered security requirements to support the real-time IoT application as established. However, in the practical scenario of IoT analytics, which has a major constraint for processing task, selecting the appropriate protocol is very crucial. Therefore, this survey study has focused on security protocols required for real-time IoT applications.

A. The contribution of present survey study as follows

I. From the literature studies, have to identify the research challenges in the existing communication and secure data forwarding between the devices and users in IoT.

II. The study presents a comprehensive taxonomy of IoT architecture design and more focus on IoT analytics and discusses security requirement towards communication paradigm.

III. Next, discuss the existing secure routing mechanism for parallel data transmission. Also discussed the authentication systems in IoT which demonstrate how the real-time IoT applications work.

IV. In the last, have investigated multiple research challenges, and provide future directions where researchers can adapt to addresses the security requirements for real-time IoT system design.

Paper Organization: Section-II discuses about secure communication paradigm at IoT layered architecture. Section-III focused on secure routing for efficient data transmission, followed by authentication mechanism in real time IoT analytics in Section-IV. Section-V outlines the current trends in secure IoT application design, followed by open research challenges in Section-VI. The last section-VII provides the conclusion and future research scope.

II. SECURE COMMUNICATION IN IOT LAYER

From the researcher's point of view, an architecture of IoT is not standardized yet. Because of the increase in the security challenges are rapidly varying in the case of availability and dependability. Therefore, Suo et al. [11] considered four-layered architecture, which mainly concerned about security needs in IoT system (Figure-2).

The first bottom layer of IoT architecture is *Perceptual-Layer* (PL), is also referred to as the recognition layer. The initial role is to collect the essential information from various sensor devices and collaborate with the physical environment. The person to machine or machine to machine interaction performs data collection and communication. It embedded with various physical systems like e.g., RFID reader, sensors actuators, Bluetooth devices, and many more. The information collects using these devices can be environmental temperature or conditions or may information about any object. So in this layer, the key components are the sensor devices which sense and collects the information and represent the collected information in digital format. As these are considered a key source of information and security and authenticity of this layer are most essential [12]. The main challenge related to this layer is sensor collected data privacy. The user should be aware of data being sensed, and in that situation, the user should be able to remain anonymous. This is considered as the significance of key agreement at PL.

The next layer is *Network-Layer* (NL) is also terms as packet transmission layer. The main role is data/information transmission collected from the bottom layer (i.e., PL). The job is to transfer the data packets collected from the network securely. The transmission mode can be Bluetooth, Wi-Fi, or satellite communication. With the support of communication protocols, this layer provides connectivity between sensor devices. In the real scenario, the whole communication process occurs over the internet, and the sensor is distributed over the network. However, this layer also faces some security problems. For example; IoT will be network congestion owing to massive data transmission. To overcome such problems, some existing mechanisms like IP-Sec, TLS, and anti-DDoS can be utilized to prevent the IoT architecture from malicious activities [13]. In this, security can be measured in terms of authentication of sensors connected to the network. Also, different cryptography mechanisms, including End to End encryption or node to node encryption methods, have been introduced [14], [15].

The transport layer is mainly responsible for data segmentation in terms of data units, Error control, and Flow control, which maintain the data transmission process. All the data collected from sensor devices at the physical layer reaches the transport layer via the network layer. The data available at this layer may be in a plain or encrypted format. However, there are still major security concerns about improving data privacy. It reliably supports the various technologies like cloud computing, fog computing, which facilitates the transport layer at IoT infrastructure.

The topmost layer: Application-Layer (AL) directly deals with end users. This layer entirely depends upon users activities, their requirements, and services using various user interface (UI) applications. The UI can be a mobile device or any handheld device which uses the service of IoTs. These devices in the AL directly interact with the end user and provide service acceptance in real time IoT applications. At this layer, also some security measurements require so that Yan et al. [16] have introduced a multi-user authentication mechanism to ensure the strong security at this layer. Furthermore, encryption algorithms and anti-virus protocols can be utilized to maintain data privacy and security. These techniques ensure data security and privacy over the distributed IoT environment.

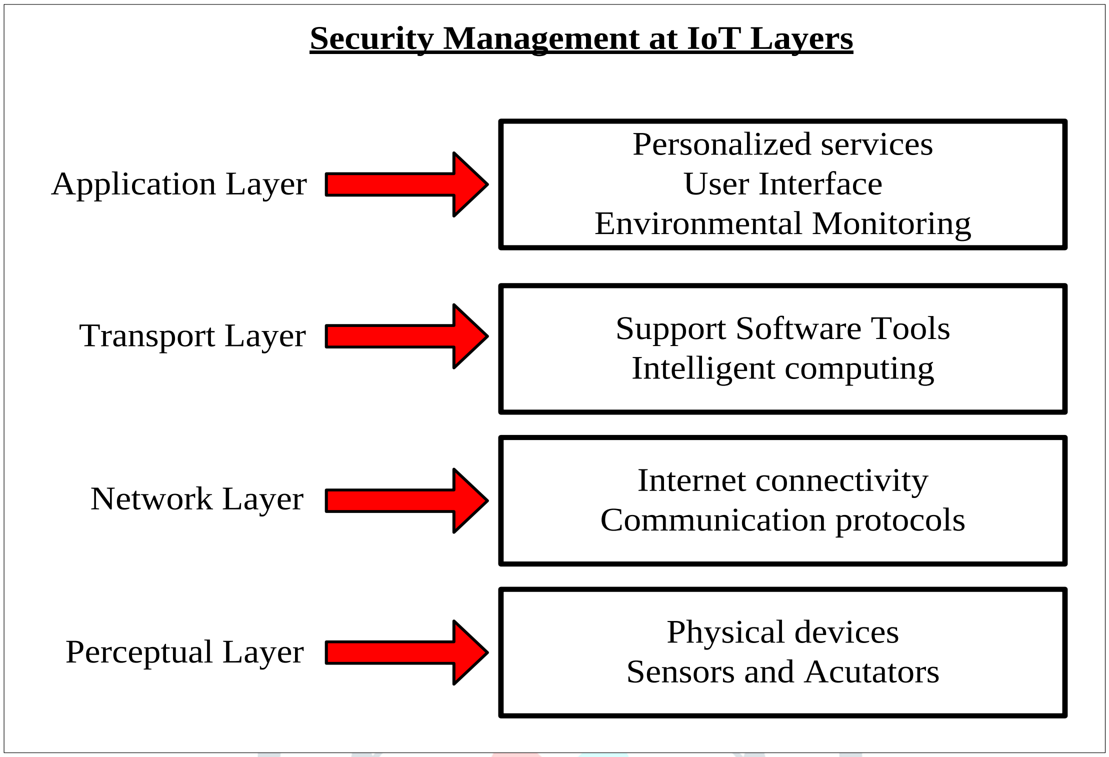

Figure 2 Security Management at IoT

III. SECURE ROUTING MECHANISM IN IOT

A Fully fledged IoT architecture is not standardized yet. Different organizations like IEEE and ITU are more focusing to develop a standardized IoT architecture. Existing studies introduced few technologies e.g., IPv6, IEEE 802.15.4, and RPL routing protocols are adapted to fulfill the need of future internet technology. The objective is, an efficient routing protocol should meet the security requirements and provide optimal routing strategy [16].

Furthermore, a security-based routing protocol for IoT is needed to identify and avoid single way communication and be optimize the transmission energy usage. Also, IPv6 and mobility are contained significant characteristics. The security solution used includes proactive routing protocol, which capable of viewing entire global network topology at real-time and reactive routing protocol, which identify the optimal routes on real demand [17-19] — the below table-1 highlights the most significant routing protocols in IoT environment.

A. RPL routing protocol: In the year of 2012, IETF introduced an RPL protocol [17]. It is a distance vector IPv6 routing protocols, where routing information is organized in terms of DAGs (Directed acyclic graphs), and further, it is classified into destination oriented DAGs [18]. The destination oriented DAGs consists of multiple sensor nodes with the sink node, which collects the information from these nodes. This protocol differentiated based on 4 factors including; destination oriented DAGs ID,

version number, instance id, and rank while destination oriented DAGs sink node is connected [19]. Optimal path selection in RPL is depended upon destination oriented DAGs link, information cost in terms of processing load, throughput, energy, and latency. The RPL can incorporate with variations in traffic and signal information exchange between the nodes. Moreover, it supports the point to multi-point, multi-point to point, and point to point traffics. [20].

B. Improved RPL protocol: The essential enhancements have been done to improvise the performance in the basic RPL routing protocol. A standardize point to point RPL protocol allows the IPv6 routers in an LLN to establish an optimal route in IPv6 routers [21]. An improved RPL protocol is aiming to improves reliability. Dynamic RPL is introduced for dynamic IoT applications [22]. The dynamic RPL protocol has the ability to improve the energy efficiency of the network and the end-to-end delay. The mobile-based RPL terminology is introduced with the purpose of mobility management over the IoT infrastructure. This protocol ignores the external metrics resulting in non-required handover operations and establishes unreliable communication links.

C. CO-RPL: This routing protocol is a non-standardize improved version of the RPL protocol in which mainly invested for cognitive networks [23]. CO-RPL utilizes an opportunistic transmission technique to send the data packets by selecting the optimal route. It will coordinate with neighboring nodes and selects an appropriate next hop to transmit the data packet to. Destination-oriented DAG is developed similar to the RPL protocol. Each sensor node continuously forwards the set of the packet instead of its root node only and informs to the neighboring nodes by changeling the DAG information object message. From this update information, every sensor node dynamically alters the node priorities to set an optimal route.

D. Channel aware routing protocol: CARP: CARP is a non-standardize distributed RPL protocol especially utilized for underwater WSNs [24]. It delivers the data packets in an optimal time period with minimum energy consumption. Additionally, it supports good quality communication link, which is computed from the successful transmission of data packets. The major drawback of this protocol is that it doesn't allow reusability of historical data. An improved version of the CARP protocol is introduced and allows the sink node to secure the historical sensor data [25]. Therefore, the enhanced CARP protocol minimizes the communication overhead.

E. Ad-Hoc on demand distance vector routing protocol" (AODVRP): AODVRP is classified into hop by hop reactive routing protocol. It uses route request (R_{req}), route reply (R_{rpl}) cycle, which is started each cyclic period of packet requires to be forward to the destination node [26]. Two types of AODVRP are; lightweight AODVRP next generation and AODVRP version-2. While AODVRP is only utilized for hop count and considered as routing metric, also possibly utilized as an energy-aware metric.

Furthermore, other routing protocols have make the simplifications over AODVRP in order to minimize the complexities and highly effective for dynamic and resource-limited WSNs. Such protocols are AODVRPbis, LOADng, TinyAODVRP, LoWPAN-AODVRP, and many more. The objective is to offer advanced metering infrastructure with the asymmetric bi-directional route between source to destination nodes while normal RPL path is not available.

In the literature, the multiple numbers of security-based routing protocols are available, which prevent the routing attacks. In the study of Leong [27] proposed a secure multi-hop routing protocol which enables the IoT devices to collaborate in a secure manner. It attains this by guaranteeing that IoT applications authentication before the network deployment.

Table 1 most significant routing protocols in the IoT environment

Protocol Name	**Functionality**	**Traffic type**	**Mechanism**	**Algorithm**	**IPv6 support**	**Routing challenges**	**Characteristics**	**Limitations**
RPL	Proactive	Multi-point to point, P2P	Energy-aware and multipath routing	Distance-vector, source routing	Yes	Local and global hosting, energy consumption, mobility, high scalability, storage	Self-configuration, schedule management	No security
Point to point RPL	Reactive	P2P	Energy-aware	Distance-vector, source routing	Yes	Local and global hosting, energy consumption, mobility, high scalability,	Finds a reliable route for any source to destination pair	More storage, no security
CORPL	Proactive	Multi-point to point, P2P	Energy-aware and multipath routing	Distance vector	Yes	Data management, sever technologies	Opportunistic forwarding	More storage, no security
CARP	Reactive	Multi-point to point, P2P	Energy aware and multipath routing	Link state	Yes	Data and storage management	Communication quality for packet transmission, high data delivery, minimum traffic delay	No security, no reusability for existing data
LOADng	Reactive	P2p	Energy-aware	Distance vector	Yes	Energy consumption, mobility, high scalability, storage	Applicable for generic traffic pattern	No security, more delay in route selection.

IV. AUTHENTICATION SYSTEM IN IOT

IoT plays a significant role to offer verities of smart services via the sensor devices, for example; smart home, smart vehicular systems, environment monitoring, smart healthcare systems, and many more. IoT infrastructure contains a number of distributed sensor devices which rapidly collects and forwards the information to perform multiple tasks. Built-in IoT applications provide reliable data transmission, e.g., Smart healthcare systems monitors, tracks, and diagnose human diseases. In the traffic monitoring systems, sensors collect a set of information related to the flow of road traffic, uses that information to manage the traffic. However, these smart systems are prone to cyber attacks as equipped with multiple sensor devices deployed in a distributed environment. An unauthenticated user may control the sensor to forged the information from the system, which may cause security issues. To overcome network security and privacy challenges over the IoT environment, it is essential to develop a security system to attain mutual authentication and create a secure communication link between the user's device and sensor nodes [31], [32].

In the literature, multiple authentication mechanisms have been designed to ensure data transmission security. A general authentication and key generation elliptic curve cryptographic approach is introduced by Liu et al. [33], where the open-ID mechanism is utilized to allows the users to maintain a single account and an authorized user can login. Later Ndibanje et al. [34] demonstrated that the proposed study of [33] couldn't resist replay and compromised with malicious nodes, to overcome this problem authors [34] proposed a symmetric encryption method which contains the additional procedure to update the password. Farash et al. [35] introduced an efficient authentication mechanism to resolve the existing security protocols weaknesses. The proposed authentication protocol supports the IoT environment and mitigates the security mentioned above shortcomings. Then Amin et al. [36] have listed limitations of the existing scheme and proved that Farash's scheme is susceptible to offline password guessing, smart card issue, and user impersonation attacks. As a solution, Amin et al. investigated a modified security model for remote user authentication in IoT using bio hashing approach.

Liu et al. [37] introduced a bilinear authentication and secured data transmission scheme for wireless healthcare systems. Authors claimed about the existing scheme which can resist malicious attacks, including replay attack, offline password guessing attack, etc. In [38], Li et al. proposed an improved authentication protocol for IoT based healthcare systems. In this study, the authors used a lightweight mathematical model, including hash function and XoR operations. In another study of Kalra and Dhillon [39] have introduced a multi-factor remote user authentication mechanism for IoT application using XoR and hash function scheme. In the recent year, Mishra and others [40] presented a robust authentication model for IoT applications, which employs hash values and pre-distributed keys to attain authentication between the sink node to the receiver node. An anonymous authentication scheme is introduced by Li et al. [41], which uses biometric information, users password, and smart card as basic elements and construct a model with simple computations of hash functions. A bi-linear signature pairing scheme is investigated for commercial IoT infrastructure without employing hash operations, and provide a secure data transmission with minimum cost [42].

A lightweight authentication and secure routing mechanism are introduced by Mick et al. [43]. The contribution was to analyze the authentication and routing protocols in the domain of data networking IoT. Authors presented a model of efficient and secure routing strategy in data networking and demonstrated its effectiveness and significances by analyzing the proposed data networking model. Zhou et al. [44] proposed a key agreement and authentication mechanism which provide un-linkability for IoT applications by employing the bilinear pairing approach. The existing security mechanism demonstrated that the proposed security protocol is un-forgeable in selecting the data attack. The experimental study evaluated the computation and communication cost and compared with existing studies. Another lightweight approach of authentication and session key establishment paradigm is introduced for smart home systems [45]. The proposed system incorporated with the Diffie-Hellman protocol for session key establishment and utilized an alternative approach. Through this mechanism, authors conquered some security challenges and provided an efficient solution in the domain of smart home system development.

The existing authentication protocols have high computational challenges, and most importantly, all are instantiated by user authentication. It is quite challenging to apply in the state of art of the current IoT environment where sensing devices collaborate and fulfill the lightweight authentication. In this context, Ning et al. [46] introduced an initial approach of communication key sharing method for sensor networks employing symmetric operations. With permutation functions, the proposed method can establish the sequence of characteristics to improve the accuracy of key sharing over sensor networks.

In the study of [47] Xue et.al, have designed a secure and handover authentication protocol for space information networks, in which satellites are given the capability to authenticate users to avoid the online involvement of the network control center (NCC) when authenticating users, thereby reducing long authentication delay and avoiding a single point of bottleneck in NCC. The existing authentication schemes don't achieve the security and privacy goals in terms of offline password guessing attacks and to enhance the security with minimum time consumption for authentication have proposed an authentication model for indeed security with formal proof [48].

V. CURRENT TRENDS IN SECURE IOT DESIGN

The primary intention of adopting security mechanism over the IoT environment is to maintain privacy, authenticity and ensure the security of the device, users and entire IoT model and to ensure the confidentiality and availability of the services offered from IoT infrastructure. Thus, security measures are applied according to the threat vectors. The below figure-3 represents the statistical graph of the various trends and techniques which have been proposed from 2016 to 2019.

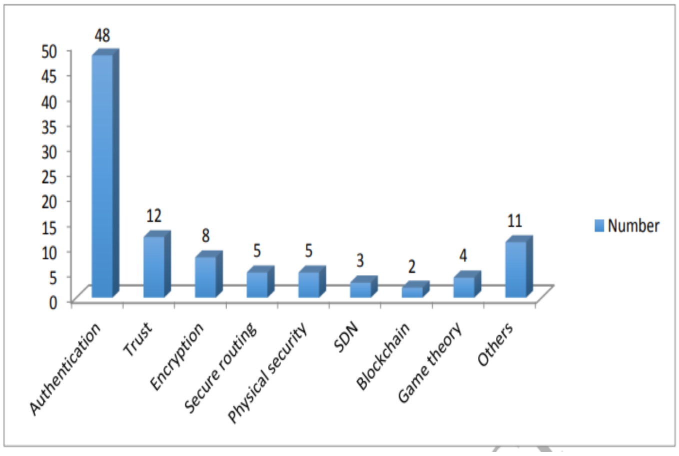

Figure 3 Research trends in IoT security from 2016-2019

It can be noticed that authentication is becoming more popular with a security concern, whereas trust management policy is gaining more popularity, owing to its defeat or detection technique of malicious node. Furthermore, the study on encryption method is more focusing on lightweight encryption policies for low constrained devices. Authentication is a method of mitigation of various attacks that occurred at IoT architecture e.g., replay attack, and many more. The popularity of authentication scheme reaches 60% to allow the authorized users to access an application layer of the IoT system.

VI. RESEARCH CHALLENGES

At present, IoTs plays a significant role in various fields ranging from Education to Research area, Health care to Business and Government to Private sectors and it has become most essential part all over the world for various purpose. As already stated, day by day number of devices connected and possess like digital identity. In the future, everything is represented as virtually (e.g., digital money transfer). By the use of digital devices, humans can perform any task from anywhere over the globe, and physical presence doesn't exist anymore. However, usually, the security requirement and vulnerabilities are also rapidly increasing with advanced technology. In the literature, a number of security problems have been discussed, and a promising solution is not provided. Usually, sensor devices have limited storage with less computational capacity. Therefore, a lightweight authentication mechanism is required for new IoT architecture. An ECC has appeared as an optimal solution for resource constrained IoT applications. Furthermore, the invention of quick response (QR) codes provide a secure authentication protocol for IoT infrastructure. It is quite a similar line barcode technique, but it has more storage capacity. Even more, this technique can be implemented very easily and connected with anything by the user itself. Hence, sensor, if attached with QR-code, can be very easily utilized by any person through scanning the QR code. Therefore, as privacy and security concern, an efficient and highly secured QR-code method is required.

From the survey study, have noted that secure RPL protocol only responsible for securing the control messages, there is no additional security mechanism has been implemented in the existing version of RPL protocol [19]. In the survey study of David et al. [49], have outlined that existing RPL security scheme suffers from various attacks including; routing replay attacks, Byzantine attacks, Falsification attacks, Selective forwarding, sinkhole, black-hole attacks and so on. In the comprehensive study of [18], analyzed various internal attacks on RPL and identified the drawbacks of RPL protocol. Also, various research proposals have identified the security challenges in RPL and 6LoWPAN, which point out about internal attacks and threat modeling. All these research studies can guide in the adoption of secure routing protocol for IoT architecture deployment.

The RPL and 6LoWPAN are the promising security solution for future IoTs. The network with low powered devices should be more secure for network security. Since the IoT world will be internet connected network, the RPL based network infrastructure could be a significant part of future IoT world. Relatively, very less research has been done in RPL security system. Even more, Le et al. [50] presented a security mechanism over RPL. Furthermore, improvements are required.

Above these research proposal considerations, there is one more essential concern is related to the security of sensor devices, that is a person's carefulness. In the practical scenario of BotNet creation and DDoS attacks generated from IoT devices, an attacker can easily access the smart devices using Brute-Force method. The problem of default password settings are never changed, and port information kept open for networks where attackers can hack into the user device. Therefore, essential guidelines and more security practices are to be followed by authorized users while operating their devices. It should be well secured with security policies, and privacy measures should be mandatory.

VII. CONCLUSION

With the tremendous growth of automated and digital devices, the entire world is considered an internet connected environment, and everything is collaborating. An IoTs referred to as ubiquitous computing technology where actuators and sensor devices are connected with living as well as non-living things. However, the security requirement in IoT architecture and related technologies have a significant role in the deployment of it. In this comprehensive study, have discussed the evolution and importance of IoT technology. Also analyzed the various security challenges and requirement of IoT architecture. The analysis of the security mechanism is categorized into two folds viz; security based on routing protocols and authentication mechanism in the IoT environment. From the literature, studies have found various research challenges that are not solved yet. These research challenges can provide a better solution to understand the problems and could be a future research direction to safeguard the IoT environment against various security attacks.

REFERENCES

[1] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," *International Conference on Computer Science and Electronics Engineering*, Hangzhou, pp. 648-651, 2012

[2] R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," 10th International Conference on Frontiers of Information Technology, Islamabad, pp. 257-260, 2012

[3] T. Xu, J. B. Wendt and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, pp. 417-423, 2014

[4] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", Computer Networks 57.10, pp.2266-2279, 2013

[5] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of Internet of Things", arXiv preprint arXiv:1501.02211, 2015

[6] M. Kranz, P. Holleis, and A. Schmidt, "Embedded interaction: Interacting with the internet of things", *IEEE internet computing*, vol. 14.2, pp.46-53, 2010

[7] J. Gubbi, "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future generation computer systems*, vol. 29.7, pp.1645-1660, 2013

[8] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", Telecommunication Systems, pp.1-19, 2017

[9] S. Verma, "A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues*", IEEE Communications Surveys & Tutorials* , 2017.

[10] Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58–63

[11] Suo, H.,Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet
of Things: A review. In International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012, IEEE (Vol.3, pp. 648–51).

[12] Asplund, Mikael, and Simin Nadjm-Tehrani. "Attitudes and perceptions of IoT security in critical societal services." IEEE Access 4 (2016): 2130-2138.

[13] Weber, R. H. (2010). Internet of Things-new security and privacy challenges. Computer Law & Security Review, 26(1), 23–30.

[14] Hu, Z. (2011). The research of several key question of Internet of Things. In International Conference on Intelligence Science and Information Engineering (ISIE), 2011, IEEE (pp. 362–365).

[15] Gan, G., Lu, Z., & Jiang, J. (2011). Internet of Things security analysis. In International Conference on Internet Technology and Applications (iTAP), 2011, IEEE (pp. 1–4).

[16] Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120–134.

[17] H.-S. Kim, J. Ko, D. E. Culler, and J. Paek, “Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): a survey,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2502–2525, 2017.

[18] Anhtuan L, Loo J, Lasebae A, Vinel A, Yue C, Chai M. The impact of rank attack on network topology of routing protocol for low-power and lossy networks. Sens. J. IEEE 013;13:3685–92.

[19] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., et al., 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Available:.

[20] D. Evans. (2011, 29 November, 2014). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Available: 〈 http://www.cisco. com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[21] M. Zhao, A. Kumar, P. H. JooChong, andR. Lu, “Acomprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities,” Peer-to-Peer Networking and Applications, vol. 10, no. 5, pp. 1232–1256, 2017.

[22] H. Kharrufa, H. Al-Kashoash, Y. Al-Nidawi,M. Q. Mosquera, and A. H. Kemp, “Dynamic RPL for multi-hop routing in IoT applications,” in Proceedings of the 13th Annual Conference on WirelessOn-DemandNetwork Systems and Services (WONS ’17), pp. 100–103, February 2017.

[23] A. Aijaz and A. H. Aghvami, “Cognitive machine-to- machine communications for internet-of-things: a protocol stack perspective,” IEEE Internet of Things Journal, vol. 2, no. 2, pp. 103– 112, 2015.

[24] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, “CARP: a channel-aware routing protocol for underwater acoustic wireless networks,” Ad Hoc Networks, vol. 34, no. supplementC, pp. 92–104, 2015, Advances in Underwater Communications and Networks.

[25] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, “E-CARP: an energy efficient routing protocol for UWSNs in the internet of underwater things,” IEEE Sensors Journal, vol. 16, no. 11, pp. 4072–4082, 2015.

[26] M. Talwar, “Routing techniques and protocols for internet of things: a survey,” in Proceeding of theNCRIET-2015, pp. 417–423, 2015.

[27] Chze PLR, Leong KS. A Secure Multi-Hop Routing for IoT Communication. IEEE World Forum Internet Things (WF-IoT) 2014:428–32.

[28] Hummen R, Wirtz H, Ziegeldorf JH, Hiller J, Wehrle K. Tailoring end-to-end IP security protocols to the Internet of Things. Netw Protoc (ICNP), 2013 21st IEEE Int Conf 2013:1–10.

[29] Krentz, K.-F., Rafiee, H., Meinel, C., 2013. 6LoWPAN security: adding compromise resilience to the 802.15.4 security sublayer Zurich, Switzerland. Present Proc Int Workshop Adapt Secur

[30] G. The 6LoWPAN architecture. Cork, Ireland. Present Proc 4th workshop Embed networked sensors 2007.

[31] H. Hu, Y. Liu, H. Zhang, and R. Pan, “Optimal network defense strategy selection based on incomplete information evolutionary game,” IEEE Access, pp. 29806–29821, vol. 6, 2018, DOI: 10.1109/ACCESS. 2018.2841885.

[32] H. Hu, Y.L. Liu, and H.Q. Zhang, “Security metric methods for network multistep attacks using AMC and big data correlation analysis,” Security and Communication Networks, pp. 1–14, vol. 2018, 2018, DOI: 10.1109/ACCESS.2018.2841885.

[33] J. Liu, Y. Xiao, and C. L. P. Chen, “Authentication and access control in the internet of thing,”, vol. 34, no. 1, pp. 588–592, June. 2012, DOI: 10.1109/ICDCSW.2012.23.

[34] B. Ndibanje, H. J. Lee, and S. G. Lee, “Security analysis and improvements of authentication and access control in the internet of things,” Sensors, vol. 14, no. 8, pp. 14786–14805, 2014.

[35] M. S. Farash, M. Turkanovic, S. Kumari, and M. Holbl, “An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,” Ad Hoc Networks, vol. 36, pp. 152–176, 2016, DOI: 10.1016/j.adhoc.2015.05.014.

[36] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N.Kumar, “Design of an anonymity-preserving three-factor authenticated key xchange protocol for wireless sensor networks,” Computer Networks, vol. 36, pp. 42–62, 2016, DOI: 10.1016/j.comnet.2016.01.006

[37] C. H. Liu, and Y. F. Chung, “Secure user authentication scheme for wireless healthcare sensor networks,” Computers & Electrical Engineering, vol. 59, pp. 250–261, 2017, DOI: 10.1016/j.compeleceng.2016.01.002.

[38] C. T. Li, T. Y. Wu, C. L. Chen, C. C. Lee, and C. M. Chen, , “An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system,” Sensors, vol. 17, no.17, pp. 1482, 2017

[39] P. K. Dhillon, and S. Kalra, “Secure multi-factor remote user authentication scheme for Internet of Things environments,” International Journal of Communication Systems, vol. 30, no. 16 pp. e3323, 2017.

[40] D. Mishra, P. Vijayakumar, V. Sureshkumar, and R. Amin, “Efficient authentication protocol for secure multimedia communications in IoTenabled wireless sensor networks,” Multimedia Tools & Applications, vol. 77, no. 14, pp. 18295–18325, Jul. 2018, DOI: 10.1007/s11042-017-5376-4.

[41] X. Li, J. Niu, S. Kumari, and F. Wu, “A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments,” Journal of Network and Computer Applications, vol. 103, pp. 194–204, 2018, DOI: 10.1016/j.jnca.2017.07.001.

[42] A. Karati, S. K. H. Islam, and M. Karuppiah, “Provably secure and lightweight certificateless signature scheme for IIoT environments,” IEEE Transactions on Industrial Informatics, 2018.

[43] Mick, Travis, Reza Tourani, and Satyajayant Misra. "Laser: Lightweight authentication and secured routing for ndn iot in smart cities." IEEE Internet of Things Journal 5, no. 2 (2017): 755-764.

[44] Zhou, Yousheng, Tong Liu, Fei Tang, and Magara Tinashe. "An Unlinkable Authentication Scheme for Distributed IoT Application." IEEE Access 7 (2019): 14757-14766.

[45] Dey, Shreya, and Ashraf Hossain. "Session-Key Establishment and Authentication in a Smart Home Network using Public Key Cryptography." IEEE Sensors Letters (2019).

[46] Ning, Zhenhu, Guangquan Xu, Naixue Xiong, Yongli Yang, Changxiang Shen, Emmanouil Panaousis, Hao Wang, and Kaitai Liang. "TAW: Cost-Effective Threshold Authentication With Weights for Internet of Things." IEEE Access 7 (2019): 30112-30125.

[47] Xue, Kaiping, Wei Meng, Shaohua Li, David SL Wei, Huancheng Zhou, and Nenghai Yu. "A Secure and Efficient Access and Handover Authentication Protocol for Internet of Things in Space Information Networks." IEEE Internet of Things Journal (2019).

[48] Zhang, Lei, Qianhong Wu, Agusti Solanas, and Josep Domingo-Ferrer. "A scalable robust authentication protocol for secure vehicular communications." IEEE Transactions on vehicular Technology 59, no. 4 (2009): 1606-1617.

[49] Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "Secure routing for internet of things: A survey." Journal of Network and Computer Applications 66 (2016): 198-213.

[50] Le, A., Loo, J., Luo, Y., & Lasebae, A. (2011). Specification-based IDS for securing RPL from topology attacks. In Wireless Days (WD), 2011 IFIP, IEEE (pp. 1–3).