# Integrated Security Trends In Iot Based Devices: A Survey

**S. Joseph[1], P. Roy Sudha Reetha[2], Dr. S. Pavalarajan[3]**
[1]Dept of Electronics and Communication Engineering
[2, 3]Dept of Information Technology
[1, 2] Christian College of Engineering and Technology, Dindigul
[3]PSNA college of Engineering and Technology, Dindigul.

***Abstract***- *The Internet of Things (IoT) is a network of physical objects or things which are connected or embedded with various sensors and software to exchange data about them through internet. The current – Covid 19 – situation brought new security issues in the system. As IoT devices increasing day by day, there may be near to 21 billion devices by 2025. It brings more critical situation to secure the IoT devices. The purpose of this survey is to understand the various IoT security related challenges as per the current practicing standards. We did a detailed study which focuses on Security Aspects, Identification of risks in the current IoT system and security protocols. We presented an updated review of the IoT Architecture in Security protocols which can be adopted in the future IoT devices. This study emphasis a need for a standard protocols that are able to handle the security issues in future. In this paper we added more light into the latest trends in the security. The research outcomes can benefit the IoT developers to ensure the most possible security for the data.*

***Keywords***- IoT, Protocols, Automation,UDS,USD,Fuzzy logic

## I. INTRODUCTION

Automation is developing technologies to produce and deliver goods and services with minimal human intervention. The automation helps to improve the efficiency, reliability and speed of many tasks that were previously performed by humans.

Adding IoT in the automation gives an edge to the technique by focusing on three important tasks – Transmitting Data, Receiving Data and Processing the received data. In the earlier days, local physical devices connected to the internet for real-time data analysis.

Nowadays, IoT’s scale has extended from the local workstation to Industrial IoT frameworks. More IoT projects are happening in the field of healthcare, education, industrial setup, etc. As of 2021, IoT has upgraded for wide area networks where it has the risks relative to expected surge in IoT devices in a diversified environment.

## II. CHALLENGES

Along with the primary purpose of this work we addressed identifying and characterizing the latest security risks in IoT. The noted research challenges in IoT is as follows.

- Heterogeneity
- Inter connectivity
- Ubiquitous Nature
- Security Standards

Trending technical domains like Artificial Intelligence as cluster-based fuzzy logic modules, Machine Learning, and Software Enabled Networking [23] have become the new research field for incorporating IoT. A notable development in IoT is the addition of ultra-lightweight protocols deployed for the core functioning and security reasons as well.

Research works pertaining to IoT security challenges cover a large area, and it is changing every day, with new loopholes being exposed regularly. Today, when we talk about IoT security, the main emphasis is on the access control methods, encryption methodologies used for transient phases, and hardware-specific security solutions, and SQL related input based attack controls. So, our research emphasizes the ever-changing security perspectives of IoT by giving IoT related security issues, proper definitions, classification, and searching for the solution present in the current scenario against them.

## III. CONTRIBUTION

The work has been motivated to explore security concerns in IoT based devices due to different IoT applications. First, to understand IoT's security aspect, it is important to have prior knowledge about the infrastructure we are dealing with; thus, we have discussed IoT architecture and made a comparative analysis of protocols and standards used in IoT. Our second research contribution includes exploring all possible aspects of recent research being made in IoT security, which will prove beneficial in developing an IoT security framework. A thorough review presented in this survey focuses on prominent threats prevailing in current IoT systems, along with the latest security models proffered for the IoT environment in recent years.

## IV. LITERATURE REVIEW

Due to the current industrial trends - wireless network with embedded capability - IoT gets more usages by integrating cloud based services. IoT Commercial sectors have seen a major boom in the market during the last few years, as smart system demands grew manifold because of its rich feature and one-click-away services. Smart systems like Smart Home appliances, AI-based smart devices, smart home automation, smart vehicles, smart labs, etc., offer ease of living but too much dependability on them often leads to high risks.

Figure 1 based on statista [1] report gives an estimated graph of the expected upwelling in IoT devices.

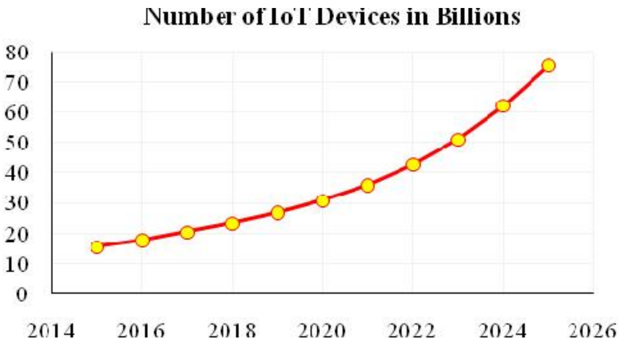
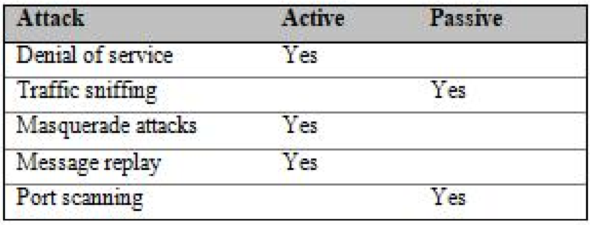


**Figure 1: Number of IoT Devices**

The technical report suggests IoT devices have become the new source hotspot for intrusion activities for the hackers as the protocols and standards existing on these devices are mainly lightweight protocols [2,3] and, on the other end, entities constituting it has more accessible access to the server [4]. These pose challenges to the technology as there is no proper addressing of the security for the latter.

It is observed that threat structure is not confined to a particular layer in IoT architecture [5]. Former network practices of integrating network security features in IoT have/had degraded IoT systems' performance. Table 1 comprises a set of recent novel models proposed in the wake of advanced threat reports coming for IoT.

**Table 1: Classification of Attacks**



| Attack | Active | Passive |
|---|---|---|
| Denial of service | Yes | |
| Traffic sniffing | | Yes |
| Masquerade attacks | Yes | |
| Message replay | Yes | |
| Port scanning | | Yes |

We have defined the security parameter concerning which certain research work offers a security model pertaining to conventional security models. The conventional model issue was—Inter-Compatibility among security tools deployed for IoT devices as they differed in Policy and implementation techniques and lack of Low- Powered device algorithms [6].

Recent research has proposed novel solutions using a different plethora of encryption methods and hardware-based methods [7] to overcome conventional security issues. Table 1 discusses some of these significant security models currently in research.

Xin Zhang and Fengtong Wen [8] proposes a novel anonymous user WSN authentication for the Internet of Things wherein two algorithmic models UDS (user-deviceserver) and USD (user-server-device), are constructed to ensure valid authentication for resolving trust centric threat models. This is a multi-functional method to provide security during the authentication process with lighter storage overheads, efficient communication costs, and faster computational speed. This work is limited in terms of the extent of the security solution provided, only for the lightweight sensor devices against the prominent network layer and physical layer based attacks.

A clusterbased fuzzy logic implementation model is proposed by Mohammad DahmanAlshehri and FarookhKhadeerHussain [9] and a secure messaging paradigm between IoT nodes where encrypted communication takes place utilizing hexadecimal values to cope with Port Scanning threats and other integrity specific vulnerabilities for AI-based IoT security solutions. This work effectively proffers the detection mechanism against the malicious IoT nodes present in the network, but risks pertaining to the data audit attack surface are not covered in this model. This study also falls short of addressing the performance analysis relative to communication costs and computation costs occurring in operation.

Priyanka et al. [10] propose a multi-stage security model making use of Elliptical curve cryptography (ECC) and fully homomorphic encryption (FHE) against cryptographic attacks, which ensures the integrity of the data transmitted in the IoT environment with less computation power. However, there is a lack of clearance on the increased data overheads generated during the process. Computational cost is another issue concerning this model.

Regarding Industrial IoT, MunkenyiMukhandi et al. [11] discusses the novel security solution for robotic communication from an Industrial IoT perspective using MQTT and Robot Operating System protocols. Two primary methods–data encryption and authentication have been used for this purpose, which has proved their efficiency in securing communication phases. This work gives valuable insight into the effectiveness of the cryptographic methods in securing communication channels.

On the contrary part, this study states the inconsistency between the performance metrics and the cryptographic functions. Deep learning and Machine learning have made their insight in IoT environment with major products being Alexa, Echo, which abject the text commands and takes voice-over commands for action on a real-time basis.

But issues have arisen pertaining to the data packet leaks, and thus for that perspective, a voice recognition application is proffered by Pooja Shree Singh and Vineet Khanna [12], which is basedon Mel-frequency cepstral coefficients (MFCC) for user identification and authentication deployable in the IoT environment to ensure data integrity, confidentiality, and privacy security. This work is useful for securing voice-enabled IoT applications; however, large dependency on the hardware architecture required for the noise-free and quality input is its major down-point.

IoT has struggled with access control-related problems ever since its arrival. To address this problem, MichailSidorov et al. [13] proposed a novel secure ultra-lightweight RFID protocol targeted for integration in a supply chain management system that uses permissioned blockchain network along with encryption provided at different access levels. Performance analysis depicts promising results with lesser storage costs and high computational speed. This work is believed to impact secure IoT devices significantly; however, the entire setup cost is uncertain.

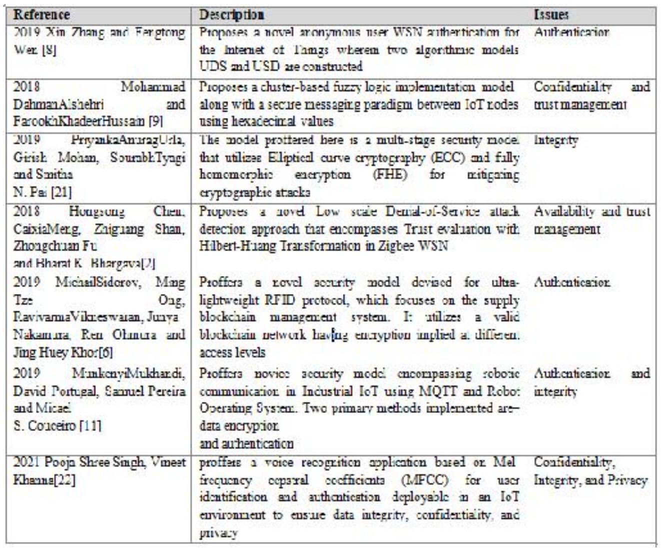
Chen et al. [14] proffers a novel Low scale Denial-of-Service attack detection approach that encompasses Trust evaluation with Hilbert-Huang Transformation in Zigbee WSN to resolve security issues pertaining to a plethora of low energy devices becoming the target of the attacks. This work is useful in refining the attack surface due to its low rate signal detection method. It features scalable architecture as it covers both cloud computing and edge computing IoT devices, which is an advantage, but larger storage overheads remain an issue.

Intrusion Detection Systems (IDS) are tasked with detecting and monitoring threat activities in the conventional network security domain [15]. Extension of which in IoT perspective is some proposed model like Snort [16], Suricata [17], and Bro [18]. Roesch [19] and Paxson talks about the model resulting from pattern-matching monitoring.

Suricata [19] is modeled on the semantic level matching of the network activities. Paradoxically, such models are designed for professional use and are not explicitly aimed at the IoT environment in terms of protocol analysis availability. It targets such advancements for expert users but not a regular citizen who lacks knowledge of the whole framework technology’s technical know-how.

GHOST [20] is a Development project (Safeguarding home IoT environments with personalized real-time risk control) that challenges the conventional network security solutions for the IoT by proposing novel reference architecture. This model’s feature is–embedded network environment in an adequately adapted smart home network gateway and is vendor-independent. The issues regarding this integrated model are many attacks like impersonation attacks, offline password attacks, and hardware-based anomaly attacks still pertain to pose a threat to the whole architecture.

**Table 2: Consolidated Survey Report**



| Reference | Description | Issues |
|---|---|---|
| 2019 Xin Zhang and Fengtong Wen [8] | Proposes a novel anonymous user WSN authentication for the Internet of Things wherein two algorithmic models UDS and USD are constructed | Authentication |
| 2018 Mohammad DahmanAlshehri and FarookhKhadeerHussain [9] | Proposes a cluster-based fuzzy logic implementation model along with a secure messaging paradigm between IoT nodes using hexadecimal values | Confidentiality and trust management |
| 2019 PriyankaAnuragUrla, Girish Mohan, SourabhTyagi and Smitha N. Pai [21] | The model proffered here is a multi-stage security model that utilizes Elliptical curve cryptography (ECC) and fully homomorphic encryption (FHE) for mitigating cryptographic attacks | Integrity |
| 2018 Hongsong Chen, CaixiaMeng, Zhiguang Shan, Zhongchuan Fu and Bharat K. Bhargava[7] | Proposes a novel Low scale Denial-of-Service attack detection approach that encompasses Trust evaluation with Hilbert-Huang Transformation in Zigbee WSN | Availability and trust management |
| 2019 MichailSidorov, Ming Tze Ong, RavivarmaVikneswaran, Junya Nakamura, Ren Ohmura and Jing Huey Khor[6] | Proffers a novel security model devised for ultra-lightweight RFID protocol, which focuses on the supply blockchain management system. It utilizes a valid blockchain network having encryption implied at different access levels | Authentication |
| 2019 MunkenyiMukhandi, David Portugal, Samuel Pereira and Micael S. Couceiro [11] | Proffers novice security model encompassing robotic communication in Industrial IoT using MQTT and Robot Operating System. Two primary methods implemented are–data encryption and authentication | Authentication and integrity |
| 2021 Pooja Shree Singh, Vineet Khanna[22] | proffers a voice recognition application based on Mel frequency cepstral coefficients (MFCC) for user identification and authentication deployable in an IoT environment to ensure data integrity, confidentiality, and privacy | Confidentiality, Integrity, and Privacy |

## V. CONCLUSION

This work highlighted the recent security trends in the IoT network domain by surveying the newly proffered models, protocols, and encryption methods implied in securing the IoT network. Our research findings on security risks in IoT emphasize the extension of the attack surface of the IoT threats and vulnerabilities in protocol-based and data-based attacks, which conveys the fact that conventional means are no longer as efficient as they were earlier against dynamic attacks prevalent in heterogeneous IoT environments like malicious node, DDoS attack, and botnet attacks. Investigations of contemporary research models show that majority of security solutions are sought through the implication of alternative forms of encryption methods, which have proved to be effective in securing communication channel attack surfaces in IoT and promoting lower energy consumption in the process. Integration of technologies like machine learning, artificial intelligence-based fuzzy logic methods, elliptical cryptographic functions, and blockchain has assisted in firming the security of the IoT networks. On the negative side, it has increased the complexity factor of the entire system. Because of the high level of abstraction of such complex solutions, the transparency in the intent of security provisions has decreased. In this work, efforts have been made to address the evolution of existing communication technologies, protocols, and internationally accepted worldwide standards, relentless efforts that have been (and are being) made by the scientific researchers globally in antecedent discussed topics. Still, there is always a scope of exploration.

## VI. ACKNOWLEDGEMENT

Sincere thanks to my Research guide Dr.S.Pavalarajan, Professor/Head/ Department of Information Technology, PSNA college of Engineering and Technology, Dindigulfor his constant support and guidance.

## REFERENCES

[1] https ://www.stati sta.com/statistics /47126 4/iot-numbe r-ofconnected-devices-world wide

[2] Wang K-H, Chen C-M, Fang W, Tsu-Yang Wu (2018) On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. J Supercomput 74(1):65–70

[3] Singh S, Sharma PK, Moon SY, Park JH (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient IntellHumanizComput. https ://doi.org/10.1007/s1265 2-017-0494-4

[4] Grooby S, Dargahi T, Dehghantanha A (2019) Abibliometric analysis of authentication and access control in IoTdevices.Handbook of big data and IoT security. Springer, Cham, pp 25–51

[5] Atlam HF, Wills GB (2020) IoT security, privacy, safety and ethics. Digital twin technologies and smart cities. Springer, Cham, pp 123–149

[6] Bembe M, Abu-Mahfouz A, Masonta M, Ngqondi T (2019) A survey on low-power wide area networks for IoT applications. TelecommunSyst 71(2):249–274

[7] Shamsoshoara A, Korenda A, Afghah F, Zeadally S (2019) A survey on hardware-based security mechanisms for internet of things. arXiv preprint

[8] Zhang X, Wen F (2019) An novel anonymous user WSN authentication for Internet of Things. Soft Comput 23(14):5683–5691

[9] Alshehri MD, Hussain FK (2019) A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing 101(7):791–818

[10] Urla PA, Mohan G, Tyagi S, Pai SN (2019) A novel approach for security of data in IoT environment. In: Computing and network sustainability. Springer, Singaporem, pp 251–259

[11] Mukhandi M, David P, Pereira S, and MS Couceiro (2019) A novel solution for securing robot communications based on the MQTT protocol and ROS. In: IEEE/SICE International Symposium on System Integration (SII), pp 608–613

[12] Singh P S, and V Khanna (2019) A MFCC based Novel approach of User Authentication in IOT. In: 2nd International Conference on Emerging Trends in Engineering and Applied Science, ISSN: 2454-4248, 5(1)

[13] Sidorov M, Ong MT, Sridharan RV, Nakamura J, Ohmura R, Khor JH (2019) Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access 7:7273–7285

[14] Chen H, Meng C, Shan Z, Zhongchuan Fu, Bhargava BK (2019) A Novel low-rate denial of service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang transformation and trust evaluation. IEEE Access 7:32853–32866

[15] Aldaej A (2019) Enhancing cyber security in modern Internet of things (IoT) using intrusion prevention algorithm for IoT (IPAI). IEEE Access. https ://doi.org/10.1109/ACCES S.2019.28934 45

[16] Roesch M (1999) Snort: lightweight intrusion detection for networks. In: 13th Systems Administration Conference on LISA, pp 229–238

[17] (OISF), Open information security foundation: Suricata. https ://suric ata-ids.org/

[18] Paxson V (1999) Bro: a system for detecting network intruders in real-time. ComputNetw 31(23–24):2435–2463

[19] Roesch M (1999) Snort: lightweight intrusion detection for networks. In: 13th Systems Administration Conference on LISA, pp 229–238

[20] Collen A, Nijdam NA, Augusto-Gonzalez J, Katsikas SK, Giannoutakis KM, Spathoulas G, Gelenbe E, Votis K, Tzovaras D, Ghavami N, Volkamer M (2018) Ghost-safe-guarding home IoT environments with personalised real-time risk control. International ISCIS Security Workshop. Springer, Cham, pp 68–78

[21] https://manipal.pure.elsevier.com/en/publications/a-novel-approach-for-security-of-data-in-iot-environment

[22] https://link.springer.com/article/10.1007/s42452-021-04156-9

[23] Sinh D, Le LV, Lin BSP, Tung LP (2018) SDN/NFV—a new approach of deploying network infrastructure for IoT. In: Wireless and optical communication conference (WOCC), IEEE, 27th, pp 1–5