International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

IoT Network Traffic Security Management Analysis

Ranjana[1], Dr. Sarvottam Dixit[2], Dr. Pooja Tripathi[3]

Submitted: 02/05/2024 **Revised**: 15/06/2024 **Accepted**: 22/06/2024

Abstract: The swift expansion of Internet of Things (IoT) devices has resulted in an unparalleled surge in network traffic, hence presenting noteworthy obstacles for the administration of security. This study examines the approaches used today to analyse and secure Internet of Things (IoT) network traffic, emphasising the critical role that machine learning (ML) and artificial intelligence (AI) techniques play in this process. These technologies provide strong solutions for dynamic and expansive IoT environments by improving anomaly detection, predictive maintenance, and real-time threat response.

Though they have potential, there are still a few drawbacks. The intricacy and diversity of Internet of Things networks pose difficulties for the standardisation of security standards. Furthermore, the incorporation of AI/ML models requires large amounts of data for training, which might present privacy issues and require a significant amount of processing power. The implementation of AI/ML models is further complicated by their vulnerability to adversarial attacks.

Future research should concentrate on creating AI/ML algorithms that are adaptable and lightweight for IoT devices with limited resources. Standardised frameworks that guarantee security and interoperability across various IoT systems should also be prioritised. Important research issues include federated learning to address data privacy concerns and strengthening the resilience of AI/ML models against adversarial threats. The next generation of IoT network security solutions can be more secure, efficient, and effective by addressing these restrictions.

Keywords: *IOT Traffic Management, Federated Learning, Intrusion Detection, Artificial Intelligence, Machine Learning*

1. Introduction

Modern society relies heavily on the IoT, which has a big impact on cybersecurity. As they are dispersed and networked, IoT devices are susceptible to various dangers and cyberattacks because many of them lack basic security safeguards. These vulnerabilities can be used by hostile actors to steal sensitive data, initiate denial-of-service (DDoS) assaults. A large-scale cyberattack on IoT networks can have detrimental consequences, such as major economic loss and disruption of essential services. The IoT, is a sophisticated network of individuals and linked things that collaborate to monitor and talk about how they are used and the surrounding environment.

The embedded systems in the smart devices comprises CPUs, sensors, and networking hardware. Within the IoT ecosystem, smart gadgets gather, send, and react to information received from their surroundings. Devices connected to the these things can share sensor data with other edge devices or gateways for either local processing or cloud-based analysis on the data. These devices communicate information continually and operate appropriately in response to that exchange. The Internet of Things often expands swiftly, necessitating safety as well as device interoperability and data privacy.

People that use IoT are not only more productive but also have greater control over their lives. Businesses can automate their work surroundings with the use of technological equipment made possible by the IoT. IoT may obtain real-time insight into the functioning of many systems, assisting in process optimization and labour cost reduction. IoT can save manufacturing and shipping costs, improve service, and visualize transactions. Intelligent IoT apps use ML techniques to analyse huge data collected from a variety of networked sensors, giving business users useful interfaces. Measuring performance metrics, MTBF rates (mean time between failure), and other critical performance indicators.

IoT devices can not only collect private information related to work but also related to personal usage at home. Hence, IoT data communications need to reliable. Sometimes, during storage and transmission, user and device data is handled improperly by a number of interconnected systems, making it susceptible to security breaches. Even well-established programs frequently have software bugs, but since many IoT devices may be updated, their vulnerability is never-ending. The inherent lack of security in IoT devices, such as routers and webcams, makes them increasingly accessible to hackers who use them for networked attacks.

Over the next five years, 79.4 zettabytes of data will be generated by IoT devices. IDC predicts that a portion of this IoT data will be "compact and anomalous." This implies that it will only include brief updates, such those from smart

[1] *Research Scholar, Mewar University, Chittorgarh, Rajasthan, India*
[2] *Professor, Computer Science, Mewar University, Chittorgarh, Rajasthan, India*
[3] *Professor, Co-Supervisor Mewar University, Chittorgarh, Rajasthan, India*

meters or sensors. Furthermore, gadgets like security cameras with integrated computer vision may generate enormous volumes of data. IDC projects that in the upcoming years, the volume of data produced by IoT devices will explode. Although video surveillance leads the industry in data creation at the moment, other sectors and medical applications are expected to overtake it in the near future, according to the research. Drones that are networked are anticipated to be heavily involved in data collection and to be outfitted with cameras

IoT devices are highly vulnerable and hence have issue in ensuring security. These gadgets collect private data, such as your words and actions. Users depend on the IoT because of its dependability, despite its dismal track record when it comes to data protection. Because of poor management, all interconnected systems are unable to safeguard user data effectively while it is being sent and stored. Even well-established programs frequently have software flaws, and since many IoT devices are not able to receive updates, hackers who use routers and webcams as IDC tools can always take advantage of them.

The first step towards establishing an IoT enabled environment is to carry out a comprehensive vulnerability investigation which includes examining the infrastructure's devices and user backends protocols in order to find any potential weak points. Throughout the IoT implementation lifecycle, risk management and evaluation are essential, particularly if the deployment is expansive and covers multiple areas. As there are variety of data formats and processing mechanisms hence there is no one size fits all solution for IoT devices.

Figure 1 depicts that the majority of IoT solutions are affordable and targeted at consumers, with little consideration given to privacy and security concerns. Such weaknesses are easily exploited by cybercriminals, who might use them to spy on their owners or add them to a botnet. We therefore need to take action to protect this technology. Furthermore, as more and more IoT devices become available, the need for this will become more urgent. IoT devices have different designs and restricted capacities, which exposes them to different security concerns. Uncontrolled and potentially hazardous situations pose a greater threat to wireless ad hoc networks. Hetnets [3] frequently face attacks from blackholes, wormholes, sinkholes, and other wormholes, blackholes and node injection, denial-of-service (DoS), , node capture, and sybils.

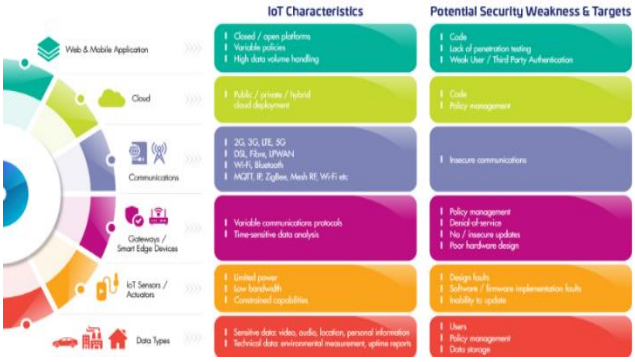

Fig 1. Security aspects for IoT (Source: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security (accessed in 2023)).

2. Literature Survey

Recently IoT has gained lot of interest in research. Although there is a significant security concern, the demand for large-scale IoT implementation is rising. Alaba, F. A., I. A. T., & Alotaibi, F. , Othman, M., Hashem (2017), focuses on the most recent risks and vulnerabilities related to IoT security by conducting a thorough survey of previous studies in the field. A taxonomy of contemporary security threats based on architecture, communication and application is presented. This paper discusses IoT security and contrasts possible dangers to it. It also analyses possible attacks.

For trustworthy data fusion, enhanced user privacy, and information security in the IoT, context awareness services are essential. It helps individuals get over their fears of risk and uncertainty, which increases user acceptance and adoption of IoT applications and services. There is now a lot of study to be done in IoT security. Yan, Zhang, and Vasilakos (2014) explore the nature of trust, offer objectives for managing trust in the IoT, and conduct a review of the most recent research on reliable IoT. Additionally, provide a research model for comprehensive IoT trust management in order to address open problems, pinpoint research gaps, and suggest future directions for the field.

IoT applications have grown dramatically during the last 20 years. Globally, there are around 50 billion linked devices. Due to their Internet connectivity, IoTs apps were frequently attacked by a variety of conventional threats, including as Trojan horses, malware, worms, viruses, spyware, and backdoor assaults. Traditional threats offer necessary functions like responsibility, authorization, and authentication. The procedure of confirming that a person is attached to an item is known as authentication and authorization. Conventional methods of authorization and authentication rely on three distinct aspects of a person's identification to confirm whether or not the subject is authorized to access the object. Furthermore, it is established that malware includes computer viruses. Trojan horses, worms, computer viruses, and spyware are examples of malware. Therefore, it is imperative that these security

vulnerabilities be addressed since depending solely on antiquated, conventional methods is not a smart idea. It is imperative that manufacturers and researchers consider ways to address these security and privacy concerns. Above all, this study highlights the knowledge and research vacuum in this field. Arif et.al. (2022), proposed systematic literature about the many dangers that IoT systems face. The most crucial objective is to comprehend how these hazards operate and create a recovery plan to mitigate the harm. This review article uses comparative research to capture, classify, and analyze IoT security risks. Additionally, the study project ends with the expansion of cutting-edge technologies, such as blockchain, AI, and ML, to ensure security, privacy, and IoTs systems.

Smart cities improve public services administration by utilizing cutting-edge technology including AI, IoT, Big Data, Cloud. The detection and reporting of certain factors pertaining to several municipal domains, including waste management, energy, transportation, agriculture, and health is possible with the application of IoT. For example, LoRa technologies are used to build IoT solutions for several smart city sectors due to their properties. Sometimes, nevertheless, people (including locals, IT managers, or city managers) might think that these characteristics are a threat to cybersecurity. Roberto Omar Andrade et. al. (2020), investigates the cybersecurity elements that make up an evaluation framework of the cybersecurity IoT systems and conducted a thorough evaluation of the literature using a top-down methodology for incident response in Internet of Things ecosystems. Additionally, suggested a risk-based approach to assess the maturity of cybersecurity of IoT in a smart city.

Devices and systems connected to the Internet of Things (IoT) use data collection and communication capabilities to connect virtual and real items. IoT systems and devices are increasingly being used in a wide range of commercial (like industry 4.0 and smart and connected cities) and national security (like critical infrastructure and military or battlefield IoT) applications. Choo, K.-K. R., Gai et. al. (2020), studies the cruciality to protect the security of IoT and the supporting systems because of how interconnected they are with society as a whole.

The idea of developing smart cities is becoming more and more popular as a way to address issues with urban growth. Nevertheless, there are obstacles to overcome in the deployment of smart cities, particularly in underdeveloped nations. It is believed that urban computing would facilitate innovation and the development of smart cities. Yusuf A. Aina, (2022), investigates the use of urban computing to solve Saudi Arabia's smart city and urban development issues. It outlines the framework for urban computing and applies it to an analysis of how Saudi cities are using it to advance sustainability. Although Saudi Arabia has made significant progress in the area of urban computing, particularly in the provision of services, more work is required to enable the country's transformation into smart, sustainable cities.

Industrial Internet of Things (IIoT), offers fresh possibilities to boost production and process efficiency and generate revenue. Simultaneously, the high degree of decentralization and cross-linking leads to new risks and increases the complexity of IIoT systems. As such, enterprises are exposed to a wide range of novel, IIoT-specific attacks in addition to traditional IT vulnerabilities. However, there is currently a dearth of a literature-based, experimentally assessed knowledge of IIoT assaults. Berger (2020), study creates a multi-layer taxonomy that aids in the distinction and identification of patterns among IIoT assaults by practitioners and researchers. Through the integration of IIoT, risk management, and IT security research added descriptive knowledge in these domains.

IoT has been around for decades, and the same is true of its application to healthcare. In the medical field, the Internet of Things is a desirable target due of its significant potential for increasing treatment. Unfortunately, because patient-specific data is accessible, the use of IoT in healthcare is rife with a variety of difficulties and vulnerabilities that, when exploited, could result in larger attack surfaces and more serious harm to patients' confidence in health systems. Furthermore, a wide range of assaults are feasible while developing IoT health devices, or IoTHDs. It's critical to comprehend the operations, social dynamics, and IoTHD architecture in order to assess the dangers in this new environment. Affia (2023), study attempts to better identify security concerns in new IoTHD modalities by using a multi-layer approach, record and map IoTHDs, and provide recommendations for enhanced governance and interaction.

Massive volumes of data are being contributed by wireless sensor networks. The recent integration of WSN into infrastructures for smart solutions has resulted in the daily generation of enormous volumes of data, such as transportation, healthcare, and environmental monitoring. In order to use the growing volumes of data, new approaches and strategies for efficient data administration and analysis are required in order to provide information that may help with controlling resource usage strategically and dynamically. Gaur, A et. al. (2015), research leads to Multi-Level Smart City design based on DempsterShafer uncertainty theory and semantic web technologies. The functionality of the suggested architecture is outlined and clarified, along with a few real-time context-aware situations.

Many sectors are changing as a result of the convergence of blockchain technology with the IoT. The potential for this confluence to enhance security, speed operations, and improve privacy has prompted a great deal of scholarly

research and the production of an astounding volume of literature. However, there is a noteworthy lack of research that examines and categorizes this topic using Latent Dirichlet Allocation (LDA). A spike in IoT and blockchain research is highlighted by Abderahman Rejeb et. al. (2023), underscoring the growing significance of this technology combo in logistics management and in healthcare data security and administration. This shows that there is a significant chance that this convergence may alter supply chains and safeguard patient information. Meanwhile, less discussed topics include access management and administration in blockchain-based IoT systems, as well as energy efficiency in wireless sensor networks that make use of blockchain technology.

The cybersecurity of the IoT, machine learning (ML) is crucial for identifying malicious and intrusive traffic. ML algorithms are frequently used in IoT risk management for the detection of IoT traffic. However, in smart IoT networks for protected smart applications, ML approaches misclassify a lot of harmful data due to erroneous feature selection. It is crucial to choose a feature set that has sufficient data for precise smart IoT anomaly and intrusion traffic identification in order to solve the issue. Shafiq et. al. (2020) suggested a unique CorrACC feature selection metric technique, algorithms produced gives accuracy of 95%.

The quantity of data being gathered and exchanged about specific customers has drastically changed since the introduction of the IoT. IoT breaches of personally identifiable information (PII) are one of the unforeseen consequences of such massive data aggregation, despite the fact that many users view the growth of IoT as convenient and crucial informational value. Wang et. al. (2020), study covered that users of the Internet of Things (IoT) handle privacy concerns about their IoT devices differently than they do about accessing the Internet, and that raising respondents' awareness of data sharing procedures affected respondents' views on privacy and their plans to use IoT in the future. The study provide useful recommendations for IoT developers and consumer education on IoT-based privacy risks.

Daniel W. Engels, Shaibal Chakrabarty (2016), describe an architecture for the IoT for making cities smart and safe. The extensive integration of IoT technology in urban areas has the potential to enhance municipal operations and elevate the standard of living for city dwellers. To avoid cyberattacks that might impair municipal operations, steal personal information, and cause irreversible damage, mission-critical Smart municipal data that is collected from and sent via IoT networks has to be protected. This study provides a study of four fundamental of IoT architectural blocks for safe Smart Cities.

The legislators and local authorities are investigating possible solutions to provide the new services to society in effective, responsive, and sustainable manner. The study looks at every service that may be provided by the many city aspects to make a city smarter.

3. Discussion

We were able to pinpoint a number of significant research gaps in IoT security throughout our literature study, including:

1. Security solutions for IoT devices are very few. Due to the limitation in computational power of many IoT devices implementation of advanced security solutions is challenging.

2. An IoT ecosystem, which consists of various kinds of device, protocols for communication and apps, is challenging to secure in the absence of a uniform taxonomy and is prune to be exploited by attackers.

3. For IoT devices, there are no comprehensive security solutions. A complex ecosystem that is challenging to secure has been formed by a multitude of devices and their myriad applications. This intricacy is further compounded by the low capacity of computation in many IoT devices.

4. There is no standardized protocol for IoT device security. Attackers can take advantage of weaknesses in the absence of universal security measures, raising the possibility of security lapses. Without a unified taxonomy, ensuring IoT security is challenging.

5. There is requirement of identifying the vulnerabilities due to the interoperability of IoT devices with the other devices in the communication system and the solutions and the research is required to found and fixed.

6. Further deep research is required for the identification of anomalies and countermeasure through the access control IoT device and the development of protection techniques for preserving the data in the IoT devices.

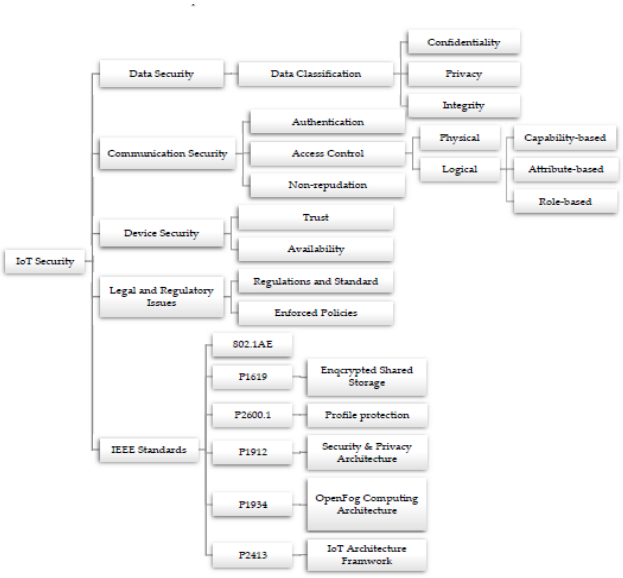

Fig 2. taxonomy for the Basic security of IoT.

Malicious actors' dangers to security increase in tandem with technological advancements.

4. Conclusions

ML and AI are two technologies that can be used to defend IoT devices against future cyberattacks. AI and ML can together capable of analysing data for possible anomalies or suspicious activity that might point to a security protocol breach.to protect before the harm is caused. When standard cybersecurity solutions, like firewalls or antivirus software, are used in conjunction with novel tactics or strategies used by attackers, this kind of proactive strategy with ML algorithms will assist guarantee that networks stay safe by providing an additional layer of defence against cyber-attacks. In the end, scalability is a feature of both machine learning and artificial intelligence. This means that these technologies can adapt to changing parameters over time, meaning you won't always need to add more resources.

5. Future Work

Given ML, AI, and pervasive computing, we see the following directions for IoT security:

(a) Creating effective, lightweight machine learning and artificial intelligence models for low-resource IoT devices while maintaining their privacy and security.

(b) Researching novel protocols and models to protect data sharing and communication between diverse Internet of Things networks and devices.

(c) Using ubiquitous solutions, like secure boot, trusted execution environments, and secure storage, to bolster IoT device security and thwart physical attacks and tampering.

(d) Integration of Block chain allow safe and transparent data management and sharing between IoT stakeholders and devices.

(e) Creating and developing new access control and authentication mechanisms, such as context awareness, user-centric, decentralized, and lightweight quantum encryption, to guarantee the security and privacy of Internet of Things data and stop illegal access and use.

(f) Researching novel frameworks and models to address ethical and privacy issues in the gathering, analyzing, and distribution of Internet of Things data, especially in pervasive computing.

References

[1] M.Sadeeq, M. A., Zeebaree, S. R. M., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018). Internet of Things Security: A Survey. 2018 International Conference on Advanced Science and Engineering (ICOASE). doi:10.1109/icoase.2018.8548785

[2] 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. doi:10.1016/j.jnca.2014.01.014

[3] Aqeel, Muhammad & Ali, Fahad & Iqbal, Muhammad waseem & Rana, Toqir & Arif, Muhammad & Auwul, Md. (2022). A Review of Security and Privacy Concerns in the Internet of Things (IoT). Journal of Sensors. 2022. 1-20. 10.1155/2022/5724168.

[4] Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garces, I. (2020). A Comprehensive Study of the IoT Cybersecurity in Smart Cities. IEEE Access, 8, 228922–228941. doi:10.1109/access.2020.3046442

[5] Choo, K.-K. R., Gai, K., Chiaraviglio, L., & Yang, Q. (2020). A Multidisciplinary Approach to Internet of Things (IoT) Cybersecurity and Risk Management. Computers & Security, 102136. doi:10.1016/j.cose.2020.102136

[6] Habib M. Alshuwaikhat, Yusuf A. Aina, Lolwah Binsaedan,Analysis of the implementation of urban computing in smart cities: A framework for the transformation of Saudi cities,Heliyon,Volume 8, Issue 10,2022,e11138, ISSN 2405-8440,https://doi.org/10.1016/j.heliyon.2022.e11138. (https://www.sciencedirect.com/science/article/pii/S2405844022024264)

[7] Stephan Berger, Olga Bürger, Maximilian Röglinger, Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy, Computers & Security,Volume 93,2020,101790,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101790. (https://www.sciencedirect.com/science/article/pii/S0167404820300754)

[8] Affia, A.-a.O.; Finch, H.; Jung, W.; Samori, I.A.; Potter, L.; Palmer, X.-L. IoT Health Devices: Exploring Security Risks in the Connected Landscape. IoT 2023, 4, 150-182. https://doi.org/10.3390/iot4020009

[9] Aditya Gaur, Bryan Scotney, Gerard Parr, Sally McClean, Smart City Architecture and its Applications Based on IoT,Procedia Computer Science,Volume 52,2015,Pages 1089-1094,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.05.122. (https://www.sciencedirect.com/science/article/pii/S1877050915009229)

[10] Abderahman Rejeb, Karim Rejeb, Andrea Appolloni, Sandeep Jagtap, Mohammad Iranmanesh, Salem Alghamdi, Yaser Alhasawi, Yasanur Kayikci, Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions,Internet of Things and Cyber-Physical Systems,Volume 4,2024,Pages 1-18,ISSN 2667-3452,https://doi.org/10.1016/j.iotcps.2023.06.003.

(https://www.sciencedirect.com/science/article/pii/S2667345223000366)

[11] Muhammad Shafiq, Zhihong Tian, Ali Kashif Bashir, Xiaojiang Du, Mohsen Guizani,IoT malicious traffic identification using wrapper-based feature selection mechanisms,Computers & Security, Volume 94,2020,101863,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2020.101863. (https://www.sciencedirect.com/science/article/pii/S0167404820301358)

[12] Philip Menard, Gregory J. Bott,Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment,Computers & Security,Volume 95,2020,101856, ISSN 0167-4048,https://doi.org/10.1016/j.cose.2020.101856. (https://www.sciencedirect.com/science/article/pii/S0167404820301280)

[13] Eric Ke Wang, RuiPei Sun, Chien-Ming Chen, Zuodong Liang, Saru Kumari, Muhammad Khurram Khan,Proof of X-repute blockchain consensus protocol for IoT systems,Computers & Security, Volume 95,2020,101871,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2020.101871. (https://www.sciencedirect.com/science/article/pii/S0167404820301449)

[14] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for Smart Cities," 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2016, pp. 812-813, doi: 10.1109/CCNC.2016.7444889

[15] Harish Kumar, Manoj Kumar Singh, M.P. Gupta, Jitendra Madaan,Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework,Technological Forecasting and Social Change,Volume 153,2020, 119281, ISSN 0040-1625,https://doi.org/10.1016/j.techfore.2018.04.024. (https://www.sciencedirect.com/science/article/pii/S004016251731394X)