International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Preventing Cyberattacks on Smart Home Devices Using Machine Learning and Edge Computing

Siddharth Pani

Abstract: ***It seems that the Internet of Things (IoT) has revolutionized the way of life in today's world and, more so, in the context of smart homes. On the contrary, IoT technology comes with major cybersecurity challenges. The sheer volume of smart home devices raises the risk of being targeted by various cyber offenders through the possibility of unauthorized intrusion, information leaks, or false data injection. Such attacks are usually complex and evolve according to the environment. Thus, most security solutions, such as Intrusion Detection Systems (IDS), must be up to par. This paper looks into recent advances in Artificial Intelligence (AI) and Machine Learning (ML) on smart home security. In particular, it looks for advanced frameworks that will utilize deep learning and edge technologies to strengthen intrusion detection and response in real-time. The paper recommend use of AI4SAFE-IoT Architecture techniques, and more recently federated learning as potential candidates for improving security and privacy of the data. Further, in some cases, because the edge computation is present, communication latency is decreased, allowing for swift threat detection and responsive action to be taken. Hence such solution types meets the increasing requirements for novel and robust security architectures for smart homes as compared to other traditional methods.***

Keywords: Internet of Things, Edge computing, Intrusion Detection System, Federated learning, AI4SAFE-IoT architecture, Convolutional Neural Networks, Long Short-Term Memory, Random forest classifier, Behavioral analysis, Real-time threat detection, Network segmentation, Tamper-proof installation, Secure socket layer, Secure File Transfer Protocol, Software Defined Networking, Device heterogeneity, Interoperability issues, Smart grid integration.

1. Introduction

Many changes have occurred regarding using and accessing the Internet with computer science. Today, almost every modern activity is linked with some services involving the Internet. Of late, the IoT has also been rapidly gaining a role in our lives. IoT technology aims to create, or at least work toward, a fully automated environment by leveraging the Internet and smart devices such as smartphones, home assistants, smart TVs, watches, smart doors, thermostats, vacuums, and more.

Smart sensors are useful in contacting smart machines, which aids in creating smart environments that can provide various services. These services increase operational effectiveness, ensure better service delivery, and improve safety when applied to smart homes. On the other hand, Cisco's report focuses on the increasing evolution of the number of Internet connected devices – 12 billion in 2010, 25 billion in 2015, 50 billion in 2020, with projections of 1 trillion by 2035 (Wong, n.d.).

IoT technology utilizes the rapid implementation of multiple devices by interconnected users into a single device like a mobile. Even so, with the sheer number of devices, managing and securing the smart home through IoT technology has its fair share of challenges. Devices meant for smart homes offer their services individually and not as needed, which is to interface and cooperate as one functional device. However, this may also be a major challenge to surmount, as the integration of technologies and protocols can account for some security vulnerabilities. As outlined by the ISO-27005 regulation, the security system has multiple deficiencies when considering its implementation in connected-device environments, which enables invasion of the whole system by unauthorized users and allows them to manage personal data and services from a remote location.

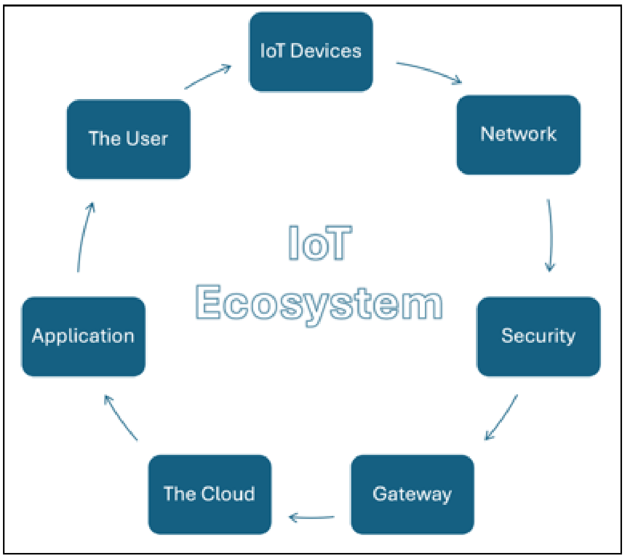

Figure 1: Home IoT Ecosystem

Since technology has become a core part of everyday life, advancements in cyber-physical systems have made possible the development of applications that create habitats that would have seemed like a dream only a few decades ago. Examples of this dramatic change are smart houses and other smart environments such as offices and hotels. These environments make use of sophisticated, intense automation, Artificial Intelligence (AI), and various interactive systems that include health and security services. In parallel with the increasing deployment of these solutions in homes or workplaces, the safety of the users against virtual as well as real threats has to be assured (Vardakis et al., 2024).

Nevertheless, the presence of the underlying technologies and their interrelations makes it difficult to protect these sophisticated systems. IoT and cloud services cause this complexity, as do several smart devices and sensors, various networking solutions, e-commerce, social networks, and AI. The development of technology has been faster than regulation and reasonable use practices, which puts users at risk. Authorities and organizations in charge of standardization face similar problems due to the possibility of developing regulations slower than the speed of progress. For the time being, end-users often need to appreciate the dangers involved, and the technology market needs to develop sufficient numbers of skilled technicians and engineers to implement the technology properly.

Smart-home security has its challenges. The major one is user education. Many of the users do not even understand their smart-home device's associated cyber threats which should not be the case. Because of this misunderstanding, many things like weak passwords, wrong installations, or software that still needs to be updated increase the chances of being attacked. Managing security and vulnerabilities is also a challenge owing to the sophisticated architecture of smart homes design consisting of multiple devices, sensors, and services. Smart-home devices face interoperability and heterogeneity challenges because they come from different manufacturers with different communication protocols so that they cannot all work together seamlessly. Remote access is also another concern, because many such home devices are Internet-connected, unauthorized access may result if users do not take adequate steps while communicating across the Internet with the devices. In addition, several smart-home devices have limited computing and memory resources and hence cannot support strong security measures. It is important to note that due to the lack of regulations, smart-home security levels are different from manufacturer to manufacturer, as well as that, between different devices or products leading protection from one tool or item to the other being remarkably different.

IoT device security, especially smart home device security will be examined in this paper while possible solutions to the gaps identified will be posited. Given the fact that nearly everything is internet enabled, users of smart devices have an obligation to learn the appropriate ways of using the gadgets and the hazards involved.

2. Background

Despite the numerous advantages associated with smart home devices, their security level can be considered to be relatively lower compared with other wired technologies. Lack of security measures allows attackers to launch various attacks. Other factors that pose risks include ransomware, eavesdropping, invasion of privacy, weaknesses in firmware. On top of that, brute force attacks, physical fiddling, malware, old firmware also pose a constant threat. Among the common practices users must adhere to for minimum attack include active encryption, timely update and unexposed network settings.

Unauthorized Access

Access to unauthorized smart home devices can be gained by resorting to weak or default passwords, a loophole which, translates into enjoying remote control over cameras, locks, thermostats and other devices at the expense of privacy and security (Ammar et al., 2018). Exactly in this connection, every user needs to make way for unique passwords and turn on Multi-Factor Authentication (MFA) (Da Xu et al., 2021).

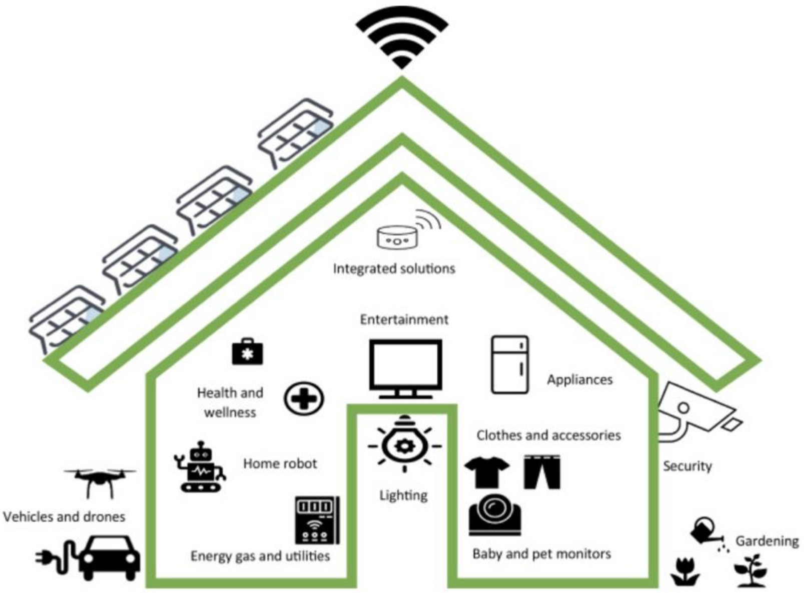

Figure 2: Smart Home (Rio et al., 2021)

Privacy Invasion

Microphone and camera equipped smart home gadgets are rather dangerous, and these devices, when compromised, may risk quite a lot of information and privacy (Liao et al., 2019). Not just videos, even audio is in play; they can hunker down and listen in to conversations with the help of CCTV footage that is already recorded or transmitted. Proper permissions and strong encrypted codes significantly lower exposure (Ammar et al., 2018).

Data Interception and Leakage

Information obtained through smart home devices such as activity and even the location of the user, can be intercepted by the attackers (Hossain et al., 2020). This data can be used for stealing one's identity or be traded on the dark market. Use of encryption such as secure sockets layer and secure file transfer protocol for data transfers could counter these measures (Sivaraman et al., 2020).

Firmware Attacks

This increases the high possibility of exploiting firmware applications since such numbers of smart devices make a lack of updates from providers a security risk. Cybercriminals can then manipulate and hack such weaknesses to gain access to the devices and embed harmful malware in them. Safe injection could be updating firmware partners also in order to cut this possibility.

Side-Channel Attacks

This is an attack where an attacker retrieves sensitive information, such as an encryption key, by using the physical or electromagnetic characteristics of the device. An example of attackers holding information power of lock due to smart changes in consumption techniques. Algorithms could be implemented in the system which made it impossible to execute side channel attacks (Hossain et al., 2020).

Network-Level Threats

Zhao et al. 2019 have stated, 'Several different types of devices are used in the smart home ecosystem and susceptible to combination attacks. For instance, a compromised smart camera might be used as a gateway to other devices like PCs or routers. Within these limits, damage can be secured also by implementing network segmentation and firewalls. (Liao et al., 2019).

Physical Attacks

However, low accessibility may not always be the case, for instance smart devices include some of the most used devices that are installed in quite an accessible location for operational use but are also exposed to surveillance (Da Xu et al., 2021) cyber and physical security attacks. Devices such as smart locks or cameras may be factory reset or intentionally rendered inoperable by the attacker. For physical attacks it is possible to use secure installation points and tamper proofing strategies. (Hossain et al., 2020).

Unavailability of fixes or updates

Any of the available updates makes a smart device vulnerable because several would not be able to receive any update thus allowing exploitation by various attackers. (Sivaraman et al., 2020). For these factors exploitations can be made to such devices by the attackers. Consumers have to choose devices properly, as they need to ensure that the manufacturer releases security updates and patches actively (Zhou et al., 2019).

Malware Injection

Intelligent devices can be infected with malicious software which enables the attackers to have remote access or control various functionalities of the devices (Hossain et al., 2020). Interconnectivity of all devices means that such malware may also target multiple devices in a menace. On the other hand, proper management of the software, such as updating and configuration to install the latest editions, and network security will provide availing protection against the risk of malware infection (Liao et al., 2019).

3. Literature Review

According to study of Tawfik et al. (2021), established in their research, IoT devices' architecture is rudimentary and resource-limited, and given their duvet coverage of security mechanisms, they are easily targeted by various cyber-attack tools and techniques, primarily. Traditional security measures which have to do with intrusion detection systems have brought dissatisfaction to customers in many areas where attacks are occurring, including IoT. The authors outline a middleware-based approach for mitigating cyber-attacks in real-time in smart home IoT infrastructure. Centralized control and dynamic management of the network are enabled by interaction with the Software Defined Networking (SDN) architecture and the use of Zodiac-Fx SDN OpenFlow switch and Raspberry Pi 4 as a gateway device for IoT-based hardware components. It allows integration with deep learning models Convolution Neural Networks (CNN) and Long-Short Term Memory Modules (LSTM) to categorize commonplace and aberrant traffic behaviors. They also proposed a non-advanced authentication method for the gateway where such IoT devices are situated. This will be based on continuous network monitoring to identify and neutralize threats by analyzing the pattern of the traffic and identifying the threat with machine learning models.

These experiments were conducted by the authors of this work using classifiers based on a random forest and deep learning techniques. The random forest classifier recorded UDP flood attacks and TCP SYN flood attacks as 92.2 and 93.1, respectively. As noted by Tawfik et al. (2021), the deep learning model in question (Lstm with Adam optimizer) achieved 98.3% and 86.1 levels of accuracy in binary classification of traffic (normal vs abnormal) and multi-class classification of attacking types, respectively.

The work by Pazouki et al. (2021) in their research demonstrates how the integration of smart grid technologies into contemporary power systems has led to more effective, cost-efficient, and environmentally friendly electric power distribution schemes. Still, there are some disadvantages of these advantages — vulnerabilities have become more sophisticated because of the fact that smart grid technology is based on heavy network comm. Such interactions create windows of opportunity for hackers to compromise the different aspects of the communication network, thereby compromising the reliability, stability, and survivability of the grid. To reduce the impacts of such incidents, other authors proposed numerous models that detect many different types of cyberattacks aimed at smart grids and smart homes. Price manipulation cyberattacks are found to be among the biggest threats to smart grid systems. It is also evident that energy theft is pervasive in smart grid systems. For example, attackers may manipulate the figures on energy used in households to cut down on energy bills. A method was proposed to detect inconsistencies in the behavior of customers who consume more energy than normal. Instances of abnormal consumption were recorded, which fell under the category of energy theft. The design of smart homes potentially lets in cyberattack threats that arise out of the convergence of many devices and DERs. Smart homes are continuously growing in popularity as owners can customize their living spaces with devices that not only automate tasks but are also useful in protecting the family or home from intrusions. Concerning the possibility of intelligent interaction with a smart home, there may be a need to collect further information that is useful in establishing activity anomalies in the event of an attack. For that reason, the authors developed a model based on the user's behavior with the equipment located in the house. Such an approach is useful in determining how and in what patterns energy and appliances have been used to detect abnormal use patterns caused by an attack. One type of cyberattack is called False Data Injection (FDA) attack, which targets the injection of data variations during the transfer stage between the components of the smart grid. These attacks will often be very difficult to locate because attacks of this nature have a low impact upon the first deployment.

A key issue is the current cyber-attack models, which need to provide for the evolution of the smart grid network's architecture and the level of integration and complexity (Pazouki et al., 2021). The work conducted by Alasmari and Alhogail (2024) revealed that due to a high number of interconnected systems in smart grids, they are also vulnerable to cyber-attacks that target these weaknesses, such as energy price manipulation, energy siphoning, and demand-side management. The range of attack vectors is wide, targeting many grid areas, including transmission lines, load balance, and energy consumption data. Research efforts have also been made to develop various detection mechanisms, including the energy use pattern and pricing load management, to detect anomalies and activities. Essential to them is reasonable research. The focus is on anomaly and Intrusion Detection Systems (IDS) that analyze energy usage and pricing metrics for possible attacks. This paper attempts to provide evidence indicating that smart houses equipped with This paper tries to give evidence that smart houses with Distributed Energy Resources (DER) have a higher attack risk. Buildings of this kind store energy by themselves through batteries, solar cells, or other devices and thus can become an attractive target for a hacker and prone to attack.

To solve this issue, the authors suggested applying net metering technologies to sell surplus power to the grid and reduce cyber threats against smart homes. Regular operational processes of energy flows and pricing data records are obtained. These records possess the capability to exhibit anomalies that are associated with attacks. This method has attained a high accuracy level for detection in smart home environments and hence is viewed as a feasible approach to smart home cybersecurity. Similar approaches include automated anomaly detection on the home appliance's status. Cues and patterns of interaction from the users of these devices help perform behavioral analysis to detect activities that suggest a cyber-attack. However, it is necessary to move toward increasingly more sophisticated models of cyberattacks that will reflect the level of modernity of power systems. Consequently, new methods of attack will need to develop, and so will new ways of detection without losing efficacy (Alasmari & Alhogail, 2024).

The issue of access to smart homes and systems connected to the Internet of Things networks is also brought forward by Vardakis et al. (2024). Such networked devices have security vulnerabilities unprofessional access, data theft, or loss and even sabotage of the device due to an array of different devices and modes of communication. This use of devices creates also a problem because by their very nature they increase the weaknesses of smarthomes. As a consequence, this gives rise to the frequency of attacks of cyber etiologies, unauthorized access, data or file thefts and also event infiltration of malware.

They consider these challenges relevant and propose applying different safeguard strategies, especially for the data being transmitted between devices. They also recommended the use of multi-factor authentication in order to protect devices from being accessed by unauthorized personnel. They are currently developing systems that enable automatic prevention and response for attempts of unauthorized access intrusions while improving user knowledge and awareness on security measures to mitigate risks associated with weak passwords and old applications. The above strategy aims at realizing the set goals of smart houses while ensuring security, privacy and strength from the emerging threats (Vardakis et al., 2024).

4. Problem Statement

The smart home trend and IoT applications have brought about great ease and automation for users but simultaneously brought a significant risk regarding cyber-attacks. Lacking sophisticated security features, IoT devices present attractive targets for unauthorized access, and False Data Injection (FDI) attacks because of resource constraints. It is now a reality that traditional security techniques such as IDS do not deal effectively with these evolving threats, especially in the environment of smart homes and smart grids, which are integrated and networked with a complex interdependence.

Earlier researchers have investigated applications of machine learning and deep learning models, such as CNN and LSTM, for identifying and responding to cybersecurity threats, and even though such approaches help in the implementation of security mechanisms, the demand for smart home structural changes calls for more innovative, scalable and real-time frameworks. In addition to that, current trends show that homes are increasingly adopting solar panels and other Distributed Energy Resources. This creates an opportunity for the attackers to distort the energy consumption patterns and create disruption through energy price manipulation or energy theft, further increasing the vulnerability risk.

Today's world needs increased precision of real-time threat detection and higher-level verification methods to address the escalating volume of cybercrimes targeting smart homes and IoT environments. This study intends to respond to some of the cyber security gaps by exploring new or future advancements in AI/ML, deep learning, and edge computing for smart homes.

5. Proposed Solution

AI/ML-Based Intrusion Detection

The heart of the solution lies in employing AI and ML algorithms within the Intrusion Detection System (IDS). AI-based IDS systems, especially those using deep learning models such as Convolutional Neural Networks (CNNs) or Long Short-Term Memory (LSTM) networks, can learn from vast datasets of normal and abnormal network behaviors. These models can detect patterns, anomalies, and even previously unknown attacks, ensuring timely identification and mitigation of cyber threats. In smart home environments, where IoT devices communicate continuously, AI/ML algorithms can detect abnormal traffic patterns, potentially identifying threats. For instance, anomaly detection algorithms can model the expected behavior of IoT devices and flag deviations that could indicate cyberattacks. This approach allows the system to catch known threats and emerging ones, a critical feature given the constant evolution of IoT vulnerabilities.

Edge Computing for Real-Time Threat Mitigation

Edge computing plays a crucial role in mitigating network-level cyberattacks by processing data locally at or near the device, reducing latency and enabling faster responses to detected threats. In smart homes, the large number of interconnected IoT devices necessitates a distributed security framework. By employing edge nodes—such as routers, gateways, or dedicated edge devices—data generated by IoT devices can be processed in real-time without the need to send it to centralized cloud servers.

This edge-based approach allows IDS systems to detect threats closer to the source of data generation, thereby minimizing the attack window. Furthermore, edge computing helps overcome the resource limitations of IoT devices, which often lack the computational power to implement advanced security measures on their own. The edge infrastructure offloads this burden, running resource-intensive AI models to protect the entire IoT ecosystem within the home (Edakulathur & Sheeja, 2023).

Federated Learning and Data Privacy

A key advantage of combining AI/ML with edge computing is the potential to implement federated learning techniques. Federated learning allows machine learning models to be trained on decentralized data located at edge devices without sharing raw data across the network, addressing privacy concerns. This is particularly beneficial for smart homes where personal and sensitive data is frequently generated by IoT devices. Federated learning can ensure that each device contributes to improving the overall security model without exposing private information to external networks.

AI4SAFE-IoT Architecture

An example of an advanced AI-based security model is the AI4SAFE-IoT architecture, which uses edge AI to secure IoT networks. This architecture applies AI modules at the edge layer to interpret and mitigate threats based on stages of the attack cycle. By combining different AI-powered modules at various levels of the network such as the perception and network layers AI4SAFE-IoT can effectively handle threats in real-time without relying on cloud computing (Tiwari, & Waoo, 2023).

6. Conclusion

Given the dominance of smart homes, the importance of powerful cybersecurity measures will be ardent. The weaknesses posed by IoT devices contribute to the security threats of smart homes and other domains that traditional security measures systems cannot effectively manage. This paper has presented a comparative analysis of the descriptive visual language of artificial intelligence, including deep learning techniques such as CNNs and LSTMs and machine learning for security concerns. Equally noteworthy is the suggestion of edge computing and federated learning as possible integrated frameworks to reduce performance challenges and privacy issues. The advanced AI-based security model is the AI4SAFE-IoT architecture is the future to mitigate the issue. The utilization of these technologies can increase the security in smart homes by allowing data processing to be internalized and further, the detection of threats is improved in technical terms. With the ever-increasing IoT landscape, further advancements in smart artificial intelligence and cyber security were needed for such smart homes to stand against more sophisticated cyber threats.

References

[1] Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. *Electronics*, *13*(16), 3343.

[2] Alasmari, R., & Alhogail, A. A. (2024). Protecting Smart-Home IoT Devices From MQTT Attacks: An Empirical Study of ML-Based IDS. *IEEE Access*, *12*, 25993-26004.

[3] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27. https://doi.org/10.1016/j.jisa.2017.11.002

[4] Da Xu, L., He, W., & Li, S. (2021). Internet of Things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243. https://doi.org/10.1109/TII.2014.2300753

[5] Del Rio, D. D. F., Sovacool, B. K., & Griffiths, S. (2021). Culture, energy and climate sustainability, and smart home technologies: A mixed methods comparison of four countries. Energy and Climate Change, p. 2, 100035.

[6] Hammi, B., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. Computers & Security, p. 117, 102677.

[7] Hossain, M., Fotouhi, M., & Hasan, R. (2020). Towards an analysis of security issues, challenges, and open problems in the Internet of Things. Future Generation Computer Systems, 82, 395-411. https://doi.org/10.1016/j.future.2017.11.031

[8] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84. https://doi.org/10.1109/MC.2017.201

[9] Liao, Y., Desmet, L., & Joosen, W. (2019). A study of the security practices in IoT device firmware development. International Journal of Information Security, 18(2), 227-239. https://doi.org/10.1007/s10207-018-0410-0

[10] Pazouki, S., Bibek, K. C., Alkhwaildi, H. A., & Asrari, A. (2021, April). Modelling of smart homes affected by cyberattacks. In 2020 52nd North American Power Symposium (NAPS) (pp. 1-6). IEEE.

[11] Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2020). Network-level security and privacy control for smart-home IoT devices. IEEE Wireless Communications, 23(5), 54-61. https://doi.org/10.1109/MWC.2016.7721743

[12] Tawfik, M., Al-Zidi, N. M., Alsellami, B., Al-Hejri, A. M., & Nimbhore, S. (2021, December). Internet of things-based middleware against cyber-attacks on smart

homes using software-defined networking and deep learning. In 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST) (pp. 7–13). IEEE.

[13] Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. Electronics, 13(16), 3343.

[14] Zhao, J., Zheng, J., Peng, Y., & Liu, Z. (2019). Enhancing security for smart home environments: A combined approach for security enhancement. Journal of Network and Computer Applications, 145, 102437. https://doi.org/10.1016/j.jnca.2019.102437

[15] Zhou, W., Zhang, Y., & Liu, P. (2019). The effect of network security on smart homes. Computers & Security, 87, 101588. https://doi.org/10.1016/j.cose.2019.101588

[16] Wong, G. (n.d.). A network for a new planet. TATA COMMUNICATIONS. https://www.tatacommunications.com/blog/2014/12/a-network-for-a-new-planet/

[17] Edakulathur, G. F. & Sheeja, S. (2023). Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review. 50. 633-645. 10.14456/easr.2023.66.

[18] Tiwari, A. & Waoo, A. (2023). IoT based Smart Home Cyber-Attack Detection and Defense.