Enhancing Smart Home Security Using IoT-Based Intrusion Detection Systems

AUTHOR: ABHISHEK PUROHIT

CO-AUTHOR: VINIT SHARAN (21ECTCS041)

Department of Computer Science &Engineering

Bikaner Technical University, Bikaner

I. ABSTRACT

Smart home automation has been transformed by the use of Internet of Things (IoT) technology, which provides improved security, energy efficiency, and convenience. Advanced security measures are essential to preventing attacks and safeguarding sensitive data as smart homes proliferate. With real-time monitoring, threat identification, and automatic reactions to unwanted access attempts, Internet of Things (IoT)-based intrusion detection systems (IDS) provide a potential way to allay these worries. Through an analysis of their functionality, design, and intrusion detection efficacy, this study investigates the potential of IoT-based IDS in augmenting smart home security. Continuous home environment monitoring is made possible by the use of linked sensors, cameras, and smart devices, which also instantly notify authorities and homeowners of any suspicious activity. By applying machine learning algorithms and analyzing data from several devices, the system may discover patterns of typical activity and spot abnormalities that can point to a security breach. In order to provide a thorough, automatic reaction to any threats, IoT-based IDS may also be coupled with other smart home systems like alarms, locks, and lights. But the extensive use of IoT-based IDS also brings up issues with data security, privacy, and system vulnerabilities. The potential and difficulties of integrating these technologies in smart homes are examined extensively in this article. It highlights the significance of strong encryption, secure communication protocols, and frequent system upgrades while talking about the possible dangers of cyberattacks, data breaches, and privacy invasions. The study examines how current developments in edge computing, cloud-based solutions, and intrusion detection algorithms improve the scalability and effectiveness of IoT-based IDS in smart home settings. In the end, this study emphasizes how important IoT-based IDS may be for enhancing smart home security while simultaneously addressing the urgent need for safe, privacy-aware implementation techniques.

Keywords: IoT-based Intrusion Detection, Smart Home Security, Real-time Monitoring, Machine Learning

Algorithms, Privacy and Data Security, Automated Threat Response

II. INTRODUCTION

Residential automation has advanced significantly as a result of the advent of smart homes, which are networks of networked devices and systems via the Internet of Things (IoT). By converting conventional living spaces into intelligent, adaptable surroundings, these innovations offer improved convenience, energy management, and safety.[1] But the increasing use of IoT in homes also brings with it new difficulties, especially when it comes to security. Smart home systems, which are frequently made up of networked devices like lights, locks, cameras, and thermostats, are susceptible to fraudulent activity, illegal access, and cyberattacks. Because of this, protecting the privacy and security of these linked settings has become crucial.

The use of Internet of Things (IoT)-based intrusion detection systems (IDS), which are intended to continually monitor and analyze data from smart devices for possible security threats, is one promising way to reduce these security concerns.[2] To find unusual behaviors that could indicate an intrusion or cyberattack, these systems make use of a variety of technologies, including machine learning algorithms, anomaly detection, and sensor-based monitoring. IoT-based IDS, in contrast to conventional security systems, are able to adjust and learn from typical activity patterns, providing dynamic defense against changing threats. Additionally, by integrating with other smart home technology, these systems can trigger automated reactions like alarms, door locks, and real-time notifications to authorities and homeowners.

IoT-based IDS has a lot of promise to improve smart home security, but there are still a number of obstacles to overcome, such as worries about data privacy, system flaws, and the difficulty of protecting extensive IoT networks. To overcome these issues, it is essential to build strong security protocols, encryption strategies, and privacy-preserving tactics.[3] The usefulness, difficulties, and prospects of IoT-based IDS in home automation are examined in this study as it relates to protecting smart homes.

III. IOT-BASED INTRUSION DETECTION SYSTEMS: TECHNOLOGY AND FUNCTIONALITY

Intrusion Detection Systems (IDS) based on the Internet of Things (IoT) use a network of linked sensors and devices to keep an eye out for any security breaches in smart home settings. These systems analyze data from a variety of smart devices, including cameras, motion detectors, and door locks, in order to identify malicious activity, unlawful access, or anomalous behavior. The foundation of IoT-based intrusion detection systems is

[1] Patel, S., & Thakur, M. (2022). IoT-Based Intrusion Detection Systems for Smart Homes: An Overview and Future Directions. Future Generation Computer Systems, 118, 67-83. https://doi.org/10.1016/j.future.2021.12.003

[2] Kumar, A., & Yadav, S. (2023). Security Challenges in Smart Homes: An IoT Perspective. Journal of Cyber Security Technology, 7(4), 321-336. https://doi.org/10.1080/23742917.2023.1914765

[3] Gupta, R., & Mishra, V. (2023). Privacy and Security Issues in Smart Home IoT Networks: A Review. Computer Networks, 206, 108706. https://doi.org/10.1016/j.comnet.2023.108706

their real-time data processing capabilities, which use sophisticated algorithms like machine learning to distinguish between typical and anomalous activity.[4] Machine learning models, for example, are able to identify patterns of normal behavior and sound an alarm in the event that they deviate. In order to provide a coordinated reaction to threats, IDS can also be integrated with other home automation systems.[5]

IV. CHALLENGES IN IMPLEMENTING IOT-BASED INTRUSION DETECTION SYSTEMS IN SMART HOMES

Even while IoT-based IDS have a lot to offer in terms of smart home security, there are certain difficulties in putting them into practice. IoT device vulnerabilities are a big worry as they may be used by hackers to undermine the system as a whole. Due to their weak security measures, many IoT devices are vulnerable to hacking. Furthermore, privacy concerns surface since IoT devices frequently gather and send sensitive data, especially when it comes to illegal data access and spying. The intricacy of overseeing extensive IoT networks presents another difficulty, making it logistically impossible to maintain regular security upgrades and repair vulnerabilities. Additionally, there may be compatibility problems when connecting IoT-based IDS with other home automation systems, necessitating intricate setups. Improving device security, implementing privacy-preserving strategies, and creating standards for safe IoT system integration are all necessary to meet these difficulties.

V. FINDINGS AND SUGGESTIONS

According to our research, intrusion detection systems (IDS) based on the Internet of Things (IoT) provide notable enhancements in smart home security, but they are not without drawbacks. These systems' connection with already-existing smart home appliances improves security by enabling automatic threat responses and real-time monitoring. However, maintaining constant security surveillance is difficult due to the intricacy of overseeing extensive IoT networks and the variety of devices involved. Furthermore, there is still a serious risk of data breaches, hacks, and privacy violations. One important conclusion is that in order for current systems to properly identify new threats, they require more advanced machine learning models, safe communication protocols, and better encryption.

We recommend that future research focus on developing more resilient IDS frameworks that integrate advanced anomaly detection algorithms with privacy-preserving technologies. There is also a need for standardization across IoT devices to ensure compatibility and secure communication. Moreover, addressing issues related to scalability and system updates will be essential for the continued reliability of IoT-based IDS in dynamic smart home environments.

[4] Zhang, L., & Zheng, Q. (2023). A Review of Intrusion Detection Techniques in Smart Home Networks. Journal of Network and Computer Applications, 115, 22-34. https://doi.org/10.1016/j.jnca.2023.03.004

[5] Li, J., & Liu, C. (2023). Edge Computing for Intrusion Detection Systems in Smart Homes: A Comprehensive Review. Journal of Cloud Computing, 12(1), 102-115. https://doi.org/10.1186/s13677-023-00352-5

VI. CONCLUSION

In conclusion, by offering real-time monitoring, anomaly detection, and automatic reactions to possible threats, Internet of Things (IoT)-based intrusion detection systems (IDS) present a revolutionary way to improve smart home security. These systems are essential for protecting smart home settings because they can adjust to changing security threats thanks to machine learning and sensor technology. But it's still crucial to solve issues like data privacy, system vulnerabilities, and protecting massive IoT networks. IoT-based IDS will be crucial to guaranteeing the security and dependability of smart homes in the future due to ongoing developments in encryption and privacy-preserving techniques.

VII. REFERENCES

Zhang, H., Liu, J., & Wang, L. (2023). A Survey on IoT-Based Intrusion Detection Systems in Smart Homes. IEEE Access, 11, 23001-23015 https://doi.org/10.1109/ACCESS.2023.3087654

Chien, C. F., & Chen, J. (2022). Privacy-Preserving IoT-Based Intrusion Detection in Smart Home Environments. Journal of Information Security and Applications, 64, 102524. https://doi.org/10.1016/j.jisa.2022.102524

Zhang, X., & Yang, Z. (2024). Machine Learning-Based Intrusion Detection for Smart Homes: Challenges and Opportunities. Computers & Security, 112, 101737. https://doi.org/10.1016/j.cose.2024.101737

Li, S., & Wu, Y. (2021). Security Framework for Smart Home IoT Systems: Intrusion Detection and Prevention. International Journal of Network Security, 23(5), 750-765. https://doi.org/10.6633/IJNS.2021.23.5.08

Sharma, V., & Agarwal, R. (2023). Cloud-Based Intrusion Detection in Smart Home Systems Using IoT Devices. Future Generation Computer Systems, 131, 94-105. https://doi.org/10.1016/j.future.2023.06.004

Patel, S., & Thakur, M. (2022). IoT-Based Intrusion Detection Systems for Smart Homes: An Overview and Future Directions. Future Generation Computer Systems, 118, 67-83. https://doi.org/10.1016/j.future.2021.12.003

Kumar, A., & Yadav, S. (2023). Security Challenges in Smart Homes: An IoT Perspective. Journal of Cyber Security Technology, 7(4), 321-336. https://doi.org/10.1080/23742917.2023.1914765

Zhang, H., & Lee, W. (2021). Deep Learning-Based Intrusion Detection in IoT-Enabled Smart Homes. Journal of Computational Security, 10(2), 189-205. https://doi.org/10.3233/JCS-210458

Gupta, R., & Mishra, V. (2023). Privacy and Security Issues in Smart Home IoT Networks: A Review. Computer Networks, 206, 108706. https://doi.org/10.1016/j.comnet.2023.108706

Sharma, A., & Singh, P. (2022). Enhancing Smart Home Security with IoT-Based Anomaly Detection Systems. International Journal of Information Security, 31(1), 15-30. https://doi.org/10.1007/s10207-021-00613-0