GJR Publication
OPEN ACCESS

Global Journal of Research in Engineering & Computer Sciences
ISSN: 2583-2727 (Online)
Volume 05| Issue 03 | May-June | 2025
Journal homepage: https://gjrpublication.com/gjrecs/

Review Article

Security Challenges faced using Internet of Things (IoT)

[1]Livingston Sunday Aduku, [2]Aliyu Surajo, [3]Sarafadeen Leye Lawal, [4]Muhammad Ahmad Baballe*

[1, 2, 3, 4]Department of Mechatronics Engineering, Nigerian Defence Academy (NDA), Kaduna, Nigeria.

DOI: 10.5281/zenodo.15366753 **Submission Date: 02 April 2025 | Published Date: 08 May 2025**

Corresponding author:** ***Muhammad Ahmad Baballe
Department of Mechatronics Engineering, Nigerian Defence Academy (NDA), Kaduna, Nigeria.
https://orcid.org/0000-0001-9441-7023

Abstract

The term "Internet of Things Security" encompasses a wide range of strategies, tools, processes, structures, and methods used to protect all aspects of the Internet of Things. IoT security includes protecting the network connections, data, hardware, and software to ensure the availability, confidentiality, and integrity of IoT ecosystems. Due of the numerous vulnerabilities that are commonly discovered in IoT systems, there are a variety of security concerns. Robust IoT security encompasses all facets of protection, such as vulnerability remediation, firmware updates, access control, component hardening, monitoring, and threat response. Since these systems are extensively distributed and vulnerable to attack, making them a highly targeted attack vector, IoT security is crucial. IoT devices can be shielded from becoming network entry points and from disclosing personal information by blocking unauthorized access. IoT security flaws can be found in smart grids, automobiles, smart home appliances, and watches.

Keywords: *Internet of Things, Information, Theft, Challenges, Security System, Protection.*

I. INTRODUCTION

Smart houses are defined as residential buildings that have a variety of networked systems and devices that allow for the automation, control, and monitoring of numerous household chores and appliances. Homeowners can remotely or via voice commands manage and improve their living space thanks to this sophisticated technology. Smart thermostats, lighting systems, security cameras, door locks, and home entertainment systems are common components of smart homes. These devices can be connected to and managed by a central hub or smartphone app. Convenience, energy efficiency, improved security, and the capacity to modify and personalize the home environment in accordance with personal preferences are all provided by this integration. Greater comfort, efficiency, and peace of mind are all benefits of smart homes, which are transforming the way we interact with our living spaces [1]–[8]. The adoption of smart homes must take security seriously. It is essential to make sure that the data and privacy of homes are protected given the rise in linked devices and systems. Potential security risks for smart homes include illegal device access, hacking attempts, and data breaches [26, 27]. Strong authentication systems, encrypted communication protocols, routine software updates, and secure network settings must all be put in place in order to reduce these dangers. Homeowners should also adhere to recommended practices including using strong passwords that are unique, activating two-factor authentication, and being cautious when allowing access to third-party programs. Systems of constant observation and surveillance can also aid in the fast detection of any security breaches [28]. Smart houses can give homeowners piece of mind by emphasizing security measures, ensuring that their living areas are shielded from potential threats [9–12]. Security based on the Internet of Things (IoT) [29] is essential for safeguarding smart homes and all of their linked gadgets. A smart home's numerous systems and equipment may communicate and share data thanks to IoT technology, which improves ease and automation [17]. However, this interconnection also offers possible weaknesses that malevolent actors may exploit. IoT based security is concerned with putting safeguards in place to protect these gadgets and the communication networks they depend on. This involves taking precautions including using strong authentication and authorization mechanisms, encrypting data transmissions, updating software often, and watching out for any unusual activities. Implementing secure gateways, intrusion detection systems, and firewalls can also aid in defending against external attacks. Smart homes may make sure that the advantages of connected devices are maximized while limiting the dangers associated with illegal

access, data breaches, and privacy concerns [13]–[18] by emphasizing IoT-based security. A network of linked systems, sensors, and gadgets that communicate and share data makes up the Internet of Things structure. Everyday items like refrigerators, cars, and even clothing are integrated with sensors [30], software, and connection capabilities in this complex ecosystem. These gadgets collect and transmit data online, enabling seamless automation and integration. The devices themselves, the network infrastructure that facilitates connectivity, and the cloud-based platforms or apps that process and analyze the gathered data make up the three primary parts of the IoT system. Real-time monitoring, remote control, and data-driven decision-making are made possible by this networked system. Businesses and individuals can use the IoT structure to take advantage of connectivity's capacity to streamline operations, boost productivity, and open up new opportunities across a range of sectors [19]–[25]. The design and implementation of an effective system aimed at securing homes and other institutions against the risk of theft may be summed up as the research contribution in this work. The suggested solution is based on two main strategies: the first one makes use of fingerprint technology [31, 32], while the second one makes use of cameras built within the Telegram app. The camera records the intruder's image and sends it to the homeowner via Telegram if there is an attempt at theft or tampering [33]. This study uses ESP-Mesh and the Internet of Things to monitor housing. Although the system developed for this study has been functioning successfully, there is a noticeable latency because the ESP-Mesh protocol is used [34]. Because of the ESP-Mesh protocol's ability to self-heal, when one node is not connected, the remaining nodes will establish a connection to the Mesh server [35, 36]. Due to each node's responsibility for message delivery, the ensuing latency will be extremely substantial, especially for the nodes that are farthest distant from one another [37]. The method that has been developed allows both homeowners and the head of security to keep tabs on the state of the housing stock. Additionally, when something goes wrong in the monitored home, the head of security and homeowners are alerted via the LINE messaging service, allowing them to take the appropriate action right away [38].

II. SECURITY CHALLENGES FACED USING INTERNET OF THINGS

The proliferation of Internet of Things (IoT) devices, while offering numerous benefits, also presents significant security and privacy challenges. These challenges arise from the interconnected nature of IoT, its reliance on often insecure communication protocols, and the vast amount of personal data collected by these devices. These vulnerabilities can lead to unauthorized access, data breaches, and privacy violations.

1. Security Challenges:

- **Vulnerability to Attacks:**
  IoT devices often have limited processing power, memory, and security features, making them susceptible to various attacks like DoS (Denial of Service), malware, and unauthorized access.
- **Insecure Communication:**
  Many IoT devices use default passwords, lack strong authentication mechanisms, and employ insecure communication protocols, increasing the risk of eavesdropping and data interception.
- **Lack of Control:**
  Organisations may struggle to control and manage security and privacy settings on IoT devices, especially when dealing with third-party services or rogue devices brought in by employees.
- **Data Breaches:**
  The vast amount of data collected by IoT devices, including personal information and location data, can be vulnerable to data breaches, leading to privacy violations and potential harm.

2. Privacy Challenges:

Unauthorized Surveillance:

- IoT devices, like smart cameras and voice assistants, can be used to collect personal data without the individual's knowledge or consent, raising concerns about surveillance and privacy violations.
- **Data Collection and Use:**
  IoT devices collect a wide range of personal data, including location, habits, preferences, and health information, which can be used for various purposes, some of which may be detrimental to individuals.
- **Lack of Control over Data:**
  Individuals often lack control over how their data is collected, used, and stored by IoT devices and services, making it difficult to protect their privacy.
- **Data Sharing and Third-Party Access:**
  Data collected by IoT devices may be shared with third parties, potentially leading to misuse or unauthorized access to personal information.
  Mitigating the Risks:
- **Strong Authentication and Authorization:**
  Implementing robust authentication and authorization mechanisms, such as multi-factor authentication and strong passwords, can help protect against unauthorized access.
- **Securing Communication:**

Using secure communication protocols, such as TLS/SSL, and encrypting data in transit and at rest can help protect against eavesdropping and data breaches.

- **Regular Updates and Patches:**
  Keeping IoT devices and software updated with the latest security patches is crucial to address known vulnerabilities and prevent attacks.
- **Data Minimization and Privacy Settings:**
  Implementing data minimization principles and providing users with control over their privacy settings can help protect their data.
- **Consumer Education and Awareness:**
  Educating users about the potential risks of IoT devices and how to protect their privacy is essential.
- **Regulation and Policy:**
  Governments and regulatory bodies can play a role in setting standards and regulations for IoT security and privacy to ensure consumer protection [41].

III. BENEFITS OF A HOME SECURITY SYSTEM WITH INTERNET OF THINGS (IOT) CAPABILITY

1. Control and observe security by using AI to improve the functionality of gadgets like CCTV cameras, smart lights, doorbells, and fire sensors, IoT offers smart home security. Data loss protection, secure connectivity, and device control are typical use cases for IoT smart security solutions.
2. Alert and attempt The IoT-connected devices connected to remote monitoring alert you to any unexpected behavior and keep you updated on every little detail of your home in real time. Thanks to excellent IoT app development, you hold the key to the future of home security in your hands. AI is used by home IoT devices to detect environmental changes and notify consumers. Even from a distance, you can keep an eye on your house. In reaction to the alarm, the gadgets take some sort of action.
3. Visitor identification You can speak with visitors using smart IoT devices with video capabilities. Even while you are gone, you can see the guests on your smartphone and communicate with them without having to unlock your door. It guarantees total convenience and security [39].

IV. CONCLUSION

By successfully addressing the drawbacks of conventional security systems, the Internet of Things (IoT)-based burglary detection system covered in this paper has offered a reliable and effective means to improve home security and discourage burglaries. The advantages of IoT-enabled home security systems were also covered [40]. The security issues with the internet of things are explained [42].

V. REFERENCES

1. Sahrab and H. M. Marhoon, “Design and fabrication of a low-cost system for Smart Home Applications,” Journal of Robotics and Control (JRC), vol. 3, no. 4, pp. 409–414, 2022, https://doi.org/10.18196/jrc.v3i4.15413.
2. L. Babangida, T. Perumal, N. Mustapha and R. Yaakob, "Internet of Things (IoT) Based Activity Recognition Strategies in Smart Homes: A Review," in IEEE Sensors Journal, vol. 22, no. 9, pp. 8327-8336, 2022, https://doi.org/10.1109/JSEN.2022.3161797.
3. P. K. Sattaru, K. V. Burugula, R. Channagiri and S. Kavitha, "Smart Home Security System using IoT and ESP8266," 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 469-474, 2023, https://doi.org/10.1109/ICSSIT55814.2023.10061059.
4. W. Li, T. Logenthiran, V. -T. Phan and W. L. Woo, "A Novel Smart Energy Theft System (SETS) for IoT-Based Smart Home," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5531-5539, 2019. https://doi.org/10.1109/JIOT.2019.2903281.
5. V. Bianchi, M. Bassoli, G. Lombardo, P. Fornacciari, M. Mordonini and I. De Munari, "IoT Wearable Sensor and Deep Learning: An Integrated Approach for Personalized Human Activity Recognition in a Smart Home Environment," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8553-8562, 2019, https://doi.org/10.1109/JIOT.2019.2920283.
6. Q. I. Sarhan, "Arduino Based Smart Home Warning System," IEEE 6th International Conference on Control Science and Systems Engineering (ICCSSE), pp. 201-206, 2020, https://doi.org/10.1109/ICCSSE50399.2020.9171939.
7. S. S. Tippannavar, S. N and P. K. M. S, "Smart Home Automation Implemented using LabVIEW and Arduino," International Conference on Electronics and Renewable Systems (ICEARS), pp. 644-649, 2022, https://doi.org/10.1109/ICEARS53579.2022.9752265.
8. B. Santhikiran, L. Nagaraju, S. Abdul Sattar, D. Bharath Chandra, and Y. Jayasankar, “Design and Implementation of Smart Home System Based on IoT and Esprainmaker,” International Transactions on Electrical Engineering and Computer Science, vol. 2, no. 2, pp. 70-79, 2023. https://www.iteecs.com/index.php/iteecs/article/view/45.

9. R. Sarmah, M. Bhuyan and M. H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System," IEEE 5th World Forum on Internet of Things (WF-IoT), pp. 59-63, 2019, https://doi.org/10.1109/WF-IoT.2019.8767229.
10. S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir and M. Imran, "Investigating Smart Home Security: Is Blockchain the Answer?," in IEEE Access, vol. 8, pp. 117802-117816, 2020, https://doi.org/10.1109/ACCESS.2020.3004662.
11. E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042-9053, 2019, https://doi.org/10.1109/JIOT.2019.2926365.
12. H. M. Marhoon, M. I. Mahdi, E. Dh. Hussein, and A. R. Ibrahim, "Designing and implementing applications of Smart Home Appliances," Modern Applied Science, vol. 12, no. 12, pp. 8–17, 2018. https://doi.org/10.5539/mas.v12n12p8.
13. D. Rani, N. S. Gill, P. Gulia, F. Arena and G. Pau, "Design of an Intrusion Detection Model for IoT-Enabled Smart Home," in IEEE Access, vol. 11, pp. 52509-52526, 2023. https://doi.org/10.1109/ACCESS.2023.3276863.
14. A. H. Mukalaf, H. M. Marhoon, I. Suwarno, and A. Ma'arif, "Design and Manufacturing of Smart Car Security System with IoT-Based Real-Time Tracking," Int J Intell Syst Appl Eng, vol. 11, no. 6s, pp. 745-752, 2023, https://www.ijisae.org/index.php/IJISAE/article/view/2909.
15. I. Antzoulis, M. M. Chowdhury and S. Latiff, "IoT Security for Smart Home: Issues and Solutions," IEEE International Conference on Electro Information Technology (eIT), pp. 1-7, 2022. https://doi.org/10.1109/eIT53891.2022.9813914.
16. M. Murad, O. Bayat, and H. M. Marhoon, "Design and implementation of a smart home system with two levels of security based on IOT Technology," Indonesian Journal of Electrical Engineering and Computer Science, vol. 21, no. 1, pp. 546–557, 2021, https://doi.org/10.11591/ijeecs.v21.i1.pp546-557.
17. Q. I. Sarhan, "Arduino Based Smart Home Warning System," IEEE 6th International Conference on Control Science and Systems Engineering (ICCSSE), pp. 201-206, 2020. https://doi.org/10.1109/ICCSSE50399.2020.9171939.
18. P. K. Sattaru, K. V. Burugula, R. Channagiri and S. Kavitha, "Smart Home Security System using IoT and ESP8266," 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 469-474, 2023, https://doi.org/10.1109/ICCSSE50399.2020.9171939.
19. Q. Li, Q. Zhang, H. Huang, W. Zhang, W. Chen and H. Wang, "Secure, Efficient, and Weighted Access Control for Cloud-Assisted Industrial IoT," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 16917-16927, 2022, https://doi.org/10.1109/JIOT.2022.3146197.
20. S. E. Mathe, A. C. Pamarthy, H. K. Kondaveeti and S. Vappangi, "A Review on Raspberry Pi and its Robotic Applications," 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), pp. 1-6, 2022, https://doi.org/10.1109/AISP53593.2022.9760590.
21. V. Kamath and R. A., "Performance analysis of the pre-trained EfficientDet for real-time object detection on Raspberry Pi," International Conference on Circuits, Controls and Communications (CCUBE), vol. 11, no. 1, pp. 834–838, 2021, https://doi.org/10.1109/CCUBE53681.2021.9702741.
22. P. Daponte, F. Lamonaca, F. Picariello, L. De Vito, G. Mazzilli and I. Tudosa, "A Survey of Measurement Applications Based on IoT," Workshop on Metrology for Industry 4.0 and IoT, pp. 1-6, 2018. https://doi.org/10.1109/METROI4.2018.8428335.
23. L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 16-32, 2020, https://doi.org/10.1109/JIOT.2019.2948888.
24. Z. Wang et al., "A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses," in IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2292-2328, 2022. https://doi.org/10.1109/COMST.2022.3201557.
25. D. Pavithra and R. Balakrishnan, "IoT based monitoring and control system for home automation," Global Conference on Communication Technologies (GCCT), pp. 169-173, 2015. https://doi.org/10.1109/GCCT.2015.7342646.
26. M. A. Baballe, A. Hussaini, M. I. Bello, U. S. Musa," Online Attacks Types of Data Breach and CyberAttack Prevention Methods", Current Trends in Information Technology, Volume 12, Issue 2, 2022, DOI (Journal): 10.37591/CTIT.
27. M. A. Baballe, et al., "Management of Vulnerabilities in Cyber Security", Global Journal of Research in Engineering & Computer Sciences ISSN: 2583-2727 (Online) Volume 03| Issue 02 | March-April | 2023 Journal homepage: https://gjrpublication.com/gjrecs/.
28. M. B. Ahmad, et al., "Need for Security Alarm System Installation and their Challenges Faced", International Journal of New Computer Architectures and their Applications (IJNCAA) 9(3): 68-76 The Society of Digital Information and Wireless Communications, 2019.
29. M. Çavaş, M. B. Ahmad, "A Review Advancement of Security Alarm System using Internet of Things (IoT)", International Journal of New Computer Architectures and their Applications (IJNCAA) 9(2): 38-49 The Society of Digital Information and Wireless Communications, 2019.

30. M. B. Ahmad, et al., "The Various Types of sensors used in the Security Alarm system", International Journal of New Computer Architectures and their Applications (IJNCAA) 9(2): 50-59 The Society of Digital Information and Wireless Communications, 2019.
31. M. B. Ahmad, F. A. Nababa, "The need of using a Radio Frequency Identification (RFID) System", International Journal of New Computer Architectures and their Applications (IJNCAA) 11(2): 22-29 The Society of Digital Information and Wireless Communications, 2021.
32. M. B. Ahmad, F. A. Nababa, "A comparative study on radio frequency identification system and its various applications", International Journal of Advances in Applied Sciences (IJAAS) Vol. 10, No. 4, December 2021, pp. 392~398 ISSN: 2252-8814, DOI: 10.11591/ijaas.v10.i4.pp392-398.
33. M. M. Jassem, M. I. Al-Nouman, "Design and Implementation of IoT-Based Burglary Detection System", Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI) Vol. 9, No. 3, September 2023, pp. 549-557 ISSN: 2338-3070, DOI: 10.26555/jiteki.v9i3.26602.
34. M. F. Wicaksono and M. D. Rahmatya, "Smart Cluster Housing Monitoring with ESP32, ESP-Mesh and Django," J. Eng. Res., vol. 9, pp. 1–16, 2021, https://doi.org/10.36909/jer.ASSEEE.16099.
35. Z. Guo, X. Ma, P. Zhang, and Z. Liu, "A dust sensor monitoring system using Wi-Fi mesh network," J. Phys. Conf. Ser., vol. 1754, pp. 1–7, 2021, https://doi.org/10.1088/1742-6596/1754/1/012129.
36. R. Muhendra, A. Rinaldi, M. Budiman, and Khairurrijal, "Development of WiFi Mesh Infrastructure for Internet of Things Applications," Procedia Eng., vol. 170, pp. 332–337, 2017, https://doi.org/10.1016/j.proeng.2017.03.045.
37. Y. Chia, R. Arjadi, E. Setyaningsih, P. Wibowo, and M. Sudrajat, "Performance Evaluation of ESP8266 Mesh Networks," J. Phys. Conf. Ser., vol. 1230, p. 12023, Jul. 2019. https://doi.org/10.1088/1742-6596/1230/1/012023.
38. M. F. Wicaksono, M. D. Rahmatya, "IoT for Residential Monitoring Using ESP8266 and ESP-NOW Protocol", Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI) Vol. 8, No. 1, March 2022, pp. 93-106 ISSN: 2338-3070, DOI: 10.26555/jiteki.v8i1.23616.
39. https://www.intuz.com/blog/iot-smart-home-security-benefits-use-cases-and-top-devices.
40. A. Zainab., I. Amina, M. Abdulmuhaimin, M. A. Baballe, and A. S Sadiku, "Contribution of the IoT to the Security System", Global Journal of Research in Engineering & Computer Sciences, vol. 3, no. 4, pp. 1–4, 2023. https://doi.org/10.5281/zenodo.8161017.
41. https://www.google.com/search?sca_esv=b5b85f1110a5fb0d&sxsrf=AHTn8zqNF55SNs3nPsublXcuTaE_L9c0cA:1746630831605&q=impact+of+internet+of+things+iot+for+security+and+privacy&source=lnms&fbs=ABzOT_CWdhQLP1FcmU5B0fn3xuWpA-dk4wpBWOGsoR7DG5zJBnsX62dbVmWR6QCQ5QEtPRrN1KFHti9EP_dqC742rxzHRLBZCil0j9azScQIqAr91EcV61Nz6944hIXaRIdewVJT47mn_rPShm_6xOZ7zhscCrn1lEXvAoYv4dughcRpNTcRMfwkFCjerPUYeN0qIk-AaRHo9IaKh4X7-UEXGunI0c2lUQ&sa=X&ved=2ahUKEwjU9ZXy0pGNAxVUa0EAHTdzM5YQ0pQJegQIDRAB&biw=1366&bih=641&dpr=1.
42. M. A. Said, M. D. Mohammed, M. B. Ahmad, "Challenges with Internet of Things (IoT) Security", Global Journal of Research in Engineering & Computer Sciences, Volume 04, Issue 02, March-April 2024, Journal homepage: https://gjrpublication.com/gjrecs/.

CITATION

Livingston S. A., Aliyu S., Sarafadeen L. L., & Muhammad A. B. (2025). Security Challenges faced using Internet of Things (IoT). In Global Journal of Research in Engineering & Computer Sciences (Vol. 5, Number 3, pp. 20–24). https://doi.org/10.5281/zenodo.15366753