TMP UNIVERSAL JOURNAL OF RESEARCH AND REVIEW ARCHIVES

VOLUME 3 | ISSUE 1 | YEAR 2024 | JAN - MAR 2024

RECEIVED DATE	REVISED DATE	ACCEPTED DATE
30/10/2023	10/11/2023	10/01/2024

Article Type: Research Article

Available online: www.tmp.twistingmemoirs.com

ISSN: 2583-7214

CHALLENGES WITH INTERNET OF THINGS (IOT) SECURITY

[1] Munirah Abdullahi Said*, [2] Musa Dan-azumi Mohammed, [3]Muhammad Baballe Ahmad

[1,2]Department of Computer Science, Kano State Institute of Information Technology, Kura. Kano, Nigeria,
*[*3]Department of Mechatronics Engineering (NDA), Kaduna, Nigeria*

ABSTRACT

The phrase "Internet of Things Security" refers to a broad category of tactics, equipment, procedures, frameworks, and techniques utilized to safeguard every facet of the internet of things. The safeguarding of the hardware, software, data, and network connections to guarantee the availability, confidentiality, and integrity of IoT ecosystems is all part of IoT security. There are several security issues due to the large number of vulnerabilities that are frequently found in IoT systems. All aspects of protection, including as component hardening, monitoring, firmware updates, access control, threat response, and vulnerability remediation, are included in robust IoT security. IoT security is essential since these systems are widely dispersed and susceptible to attack, making them a highly focused attack vector. By preventing unwanted access, IoT devices can be protected from becoming entry points into the network and from leaking private data. Vulnerabilities in IoT security can be identified in watches, smart home appliances, cars, and smart grids.

Keywords: Leak information, Theft, Challenges of IoT, Security System, Protection.

CORRESPONDING AUTHOR

Name: Munirah Abdullahi Said

Affiliation: Department of Computer Science, Kano State Institute of Information Technology, Kura. Kano, Nigeria

Email: mb.ahmad@nda.edu.ng

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. IoTbased 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].

INTERNET OF THINGS (IOT) SECURITY CHALLENGES

IoT devices were not designed with security in mind, as was previously mentioned. This creates a plethora of IoT security issues that could have severe consequences. There aren't many guidelines or

regulations governing IoT security, in contrast to other technological solutions. Furthermore, the majority of individuals are unaware of the dangers that come with IoT systems. Furthermore, they are clueless about the complexity of IoT security issues. The following are a some of the numerous IoT security concerns:

Lack of visibility- IT departments are frequently unaware of IoT device deployments by users, which makes it hard to compile a comprehensive list of everything that has to be secured and tracked.

Limited security integration- The integration of IoT devices with security systems can be difficult or impossible due to their vast diversity and size.

Open-source code vulnerabilities- A common feature of firmware created for Internet of Things devices is open-source software, which is prone to errors and vulnerabilities.

Overwhelming data volume- The volume of data produced by Internet of Things devices makes data management, protection, and supervision challenging.

Poor testing- The majority of IoT developers don't emphasize security, hence they don't carry out efficient vulnerability testing to find holes in IoT systems.

Unpatched vulnerabilities- For a variety of reasons, including fixes not being available or trouble accessing and installing patches, many IoT devices contain unpatched vulnerabilities.

Vulnerable APIs- APIs are frequently utilized as ports of access to command-and-control centers, from which attacks like SQL injection, man-in-the-middle (MITM), distributed denial of service (DDoS), and network breaches are launched.

Weak passwords- IoT devices frequently come with default passwords that many users forget to update, making it simple for hackers to access them. In other instances, users generate easily guessed, weak passwords [41].

BENEFITS OF A HOME SECURITY SYSTEM WITH 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].

CONCLUSION

The Internet of Things (IoT)-based burglary detection system discussed in this paper has provided a dependable and efficient way to increase home security and deter burglaries by effectively resolving

the shortcomings of traditional security systems. There was also discussion of the benefits of IoT-enabled home security systems [40]. An explanation of the internet of things' security challenges is provided.

REFERENCES

1. Alfatemi, S.M.H., Motamedifar, M., Hadi, N. and Saraie, H.S.E. (2014).Analysis of virulence genes among methicillin resistant *Staphylococcusaureus*(MRSA)strains. Jundishapur Journal of Microbiology, 7(6):e10741.
2. Alkhafaji, B.A. and Alsaimary, I.E.(2020).Comparative Molecular Analysis of Mecca, Sea and Seb Genes in Methicillin-Resistant *Staphylococcus aureus* (MRSA).Journal of Clinical & Biomedical Research,2(3):1-8.
3. AL-Khzarji, N. Z. R. (2020). Detection of Bio film formation and qacgenes in Staphy lococcusspp and inhibition of efflux pump using Ananas comosus extract.Thesis,University of Baghdad,IRAQ.
4. Al Laham NA. Species identification of clinical coagulase-negative staphylococci isolated in Al-Shifa hospital Gaza using matrix-assisted laser desorption/ionization-time of flight mass spectrometry. *Curr Res Bacteriol.* 2017;10:1–8.
5. Almwafy, A. (2020). Preliminary Characterization and Identification of Gram Positive Hemolysis Bacteria. Al-Azhar Journal of PharmaceuticalSciences, 62(2):96-109.
6. Anderson MJ, Lin YC, Gillman AN, Parks PJ, Schlievert PM, Peterson ML (2012) Alpha-toxin promotes Staphylococcus aureus mucosal bio film formation. *Front Cell Infect Microbiol* 2: 64.
7. Aryal,S.(2018).CatalaseTest-Principles,Uses,Procedure,Result Interpretation with precautions.
8. Bello, C. S. S., and Qahtani, A.(2005). Pitfalls in the routine diagnosis of *Staphylococcus aureus*. African Journal of Biotechnology, 4(1): 83-86.
9. Brown,A.E.;andSmith,H.(2014)Benson'smicrobiologicalapplications:laboratorymanualingene ralmicrobiology.14th.McGrawHillEducation.
10. Carroll, K. C., Morse, S. A., Mietzner, T. and Miller, S. J. (2016).Melnick and Adelberg's Medical Microbiology: (27th ed.). McGraw-HillEducation.US.pp.127,146.
11. den Reijer, P. M., Haisma, E. M., Lemmens-den Toom, N. A., Willemse, J., Koning, R. A., Demmers, J. A., et al. (2016). Detection of alpha-toxin and other virulence factors in biofilms of *Staphylococcus aureus* on polystyrene and a human epidermal model. *PLoS ONE* 11:e0145722. doi: 10.1371/journal.pone.0145722
12. Gao,M.;Sang,R.;Wang,G.andXu,Y.(2019).Association of pvlgene with incomplete hemolytic phenotype in clinical *Staphylococcusaureus*.Infection And DrugResistance,12:1649.
13. Hata, D. J. and Thomson, R. B. (2017). Gram Stain Benchtop Reference Guide:AnIllustrated Guide to Microorganisms and Pathology Encountered in Gramstained Smear.John &WileySons,NY,USA.
14. Jahan, M., Rahman, M., Parvej, M. S., Chowdhury, S. M., Haque, M. E., Talukder, M. A. and Ahmed, S. (2015). Isolation and characterization of *Staphylococcus aureus* from raw cow milk in Bangladesh, Journal of Advanced Veterinary and Animal Research, 2(1): 49- 55.
15. Karmakar,A.,Dua,P.,and Ghosh,C.(2016).Biochemical and Molecular Analysis of *Staphylococcusaureus* Clinical Isolates from Hospitalized Patients. The Canadian Journal of Infectious Diseases and Medical Microbiology, 2016: 9041636.
16. Kobayashi,S.D.,Malachowa,N.,andDeLeo,F.R.(2015).PathogenesisofStaphylococcusaureusab scesses.TheAmericanJournalofPathology,185(6):1518–1527.
17. Plata,K.,Rosato,A.E.,andWegrzyn,G.(2009).*Staphylococcusaureus*as an infectious agent: overview of biochemistry and molecular genetics of its pathogenicity. Acta Biochimica Polonica, 56(4), 597–612.
18. Prescott, L. M., Harley, J. P., and Klein, A. (2007). Microbiology of fresh water.Mc Graw Hill, New-York,(56): 669–682.

19. Suhaili, Z., Rafee, P. '.MatAzis, N.,Yeo, C. C., Nord in, S. A., AbdulRahim,A.R.,Al-Obaidi,M.,andMohdDesa,M.N.(2018).Characterizationofresistancetoselectedantibiotics andPanton-Valentine leukocid in-positive *Staphylococcusaureus* in a healthy student population ata Malaysian University.Germs,8(1): 21–30.
20. Tong, S.Y., Holden, M.T., Nickerson, E.K., Cooper, B.S., Köser, C.U.,Cori, A., Jombart, T., Cauchemez, S., Fraser, C., Wuthiekanun, V. and Thai padungpanit, J. (2015). Genome sequencing defines phylogeny and spread of methicillin-resistant *Staphylococcusaureus* in a high transmission setting.GenomeResearch,25(1):111-118.
21. Zhang H, Zheng Y, Gao H, et al. Identification and characterization of Staphylococcus aureus strains with an incomplete hemolytic phenotype. *Front Cell Infect Microbiol*. 2016;6:146.
22. Wijesundara, W. M. D. A., Rajapakse, R. G. S. C., Jayatilake, J. A. M.A., &Jayatilake, J. A. M. S. (2019). A preliminary study of mecA gene expression and methicillin resistance in staphylococci isolated from thehuman oral cavity. Sri Lankan Journal of Infectious Diseases, 9(1): 42–48.
23. Yan,X.,Li,Z.,Chlebowicz,M.A.,Tao,X.,Ni,M.,Hu,Y.,Li,
24. Z.,Grundmann,H.,Murray,S.,Pascoe,B.andSheppard,S.K.(2016).Genetic features of livestock-associated *Staphylococcusaureus* ST9 isolates from Chinese pigs that carry the lsa(E) gene for quinupristin/dalfoprist in resistance.International Journal of Medical Microbiology,306(8): 722-729.