Enhancing Home Security with IoT Devices: A Vulnerability Analysis Using the IoT Security Test

Andrey Yu. Misailov[1,*], *Neeti* Mishra[2], *Sorabh* Lakhanpal[3], *Anshika* Prakash[4], *Naresh* Sharma[5]
[1]*Moscow State University of Civil Engineering, 129337 Moscow, Russia*
[2] *Uttaranchal University, Dehradun - 248007, India*
[3]*Lovely Professional University, Phagwara, Punjab, India*
[4]*K R Mangalam University, Gurgaon, India*
[5]*GD Goenka University, Sohna, Haryana, India*
***Corresponding author-** MisailovAY@mgsu.ru

Abstract: In order to carefully evaluate the susceptibility of common IoT devices found in smart homes, this research made use of the IoT Security Test framework. The findings showed a significant average drop in vulnerability ratings of 45% after evaluation, clearly indicating that improving IoT device security is feasible. The research classifies vulnerabilities found, highlighting the prevalence of Firmware Problems, Weak Passwords, and Network Vulnerabilities. Moreover, it examines the efficacy of remedial initiatives. These discoveries play a crucial role in enhancing the security of Internet of Things devices, providing a strong barrier for the protection of homeowners and the privacy of their data, especially in the constantly linked world of smart homes.

Keyword-IoT security, smart homes, vulnerability analysis, IoT devices, data privacy

1 INTRODUCTION

With previously unheard-of levels of ease, automation, and control over our homes, the Internet of Things (IoT) has revolutionized contemporary living. IoT gadgets have become essential parts of contemporary home security systems, ranging from IP cameras that provide real-time monitoring to smart door locks that can be remotely controlled via smartphones. But this connectedness and ease come at a cost, because the security of these gadgets is being examined more closely[1]–[5]. As IoT technology develops, so do the strategies used by bad actors to take advantage of weaknesses. With the possible hazards of unauthorized access and breaches, it is now crucial to ensure the security of these devices. This article uses the IoT Security Test to do a vulnerability analysis and begin a thorough investigation of the security environment in smart homes[6]–[10].

1 The Problem with IoT Security

The idea of home security has completely changed because to Internet of Things (IoT) devices, which provide homeowners remote access to lighting, temperature control, monitoring, and even access management. These gadgets are designed to make living easier, use less energy, and increase safety. But because of their interconnectedness and dependence on the internet, they are vulnerable to security flaws that need to be carefully examined and fixed[11]–[16]. The increasing number of these devices has made them appealing targets for hackers looking to jeopardize personal privacy and physical security. Weak passwords, unpatched firmware, and network vulnerabilities are common flaws that hackers might use to get unauthorized access to the ecosystem of smart homes. Strong security evaluations are required in light of these security problems, which cast doubt on the general safety of homes outfitted with IoT devices[17]–[22].

2 A Vulnerability Analysis Framework for the Internet of Things Security Test

The IoT Security Test, a thorough methodology for evaluating the security of IoT devices often used in smart homes, serves as the cornerstone of this study. This technique includes a multifaceted assessment that includes risk classification, remediation effort assessment, and vulnerability identification. The IoT Security Test examines important topics including network vulnerabilities, device security, and possible firmware security flaws. It offers a methodical way to pinpoint vulnerabilities, categorize them according to severity, and put remedial security measures in place. This study evaluates a range of IoT devices used in smart homes using the IoT Security Test in an effort to find security flaws and suggest fixes[23]–[25].

3 Objectives and Structure of the Research

This research's main goal is to find and evaluate popular IoT devices used in smart homes for vulnerabilities, and then suggest security fixes to improve home security. The format of this document is as follows:

- Introduction: This section gives a general overview of the importance of IoT devices in contemporary households as well as the security risks they provide.
- Literature Review: The literature on IoT device vulnerabilities and the value of security evaluations in smart homes is reviewed in this part.
- Methodology: We go over the framework for the IoT Security Test, which is designed to assess how vulnerable IoT devices are in smart homes.
- Results and Analysis: The results of the vulnerability analysis are presented in this part along with an interpretation of their consequences.

- Conclusion and Suggestions: In this last part, the main conclusions are outlined, their consequences are discussed, and suggestions are made for improving the security of Internet of Things devices in smart homes.

2 Review of Literature

1 Smart Houses with IoT Devices

The way we engage with our living environments has changed dramatically as a result of the Internet of Things (IoT) devices being integrated into smart homes. Smart door locks, IP cameras, thermostats, lighting systems, and other gadgets provide homes with never-before-seen levels of automation, convenience, and control. These gadgets' interactivity and connection have improved energy efficiency, home security, and general quality of life. But these technologies also come with security risks that have drawn a lot of attention from academics and bad actors, despite their amazing advantages[26].

2 IoT Device Security Vulnerabilities

The fast expansion of Internet of Things devices has revealed security flaws that need careful analysis. Among the frequent vulnerabilities that smart home devices encounter include weak passwords, obsolete or unpatched software, insufficient encryption, and unsafe network setups. These gadgets, which are often designed with practicality and usability as their top priorities, could not have the security safeguards needed to fend off the ongoing attacks they face. This has led to an increase in anxiety about the possibility of illegal access, data breaches, and device manipulation[27]–[32].

3 Danger of Unauthorized Entry and Privacy Violation

Unauthorized access to Internet of Things devices may seriously compromise the security of smart homes. Physical security is directly threatened by malicious actors who may take advantage of flaws in devices like cameras and smart door locks to take control of them. Concurrently, there is a significant risk of privacy infringement. IoT devices that aren't properly protected may be used to spy on homes by recording audio and video feeds and gathering private data, endangering people's privacy[33]–[37].

4 The Value of Security Evaluations

It is impossible to exaggerate the significance of security evaluations for IoT devices in smart homes. The purpose of security assessments is to find and fix the devices' flaws and vulnerabilities so that they can withstand possible assaults better. Homeowners and manufacturers may be proactive in preventing illegal access and data breaches by undertaking routine evaluations. The foundation for reducing the security threats brought on by the spread of IoT devices in homes is formed by these evaluations[38]-[42].

5 IoT Security Exam Structure

The research community has created concepts and approaches for assessing IoT device security in order to solve these security challenges. The IoT Security Test is one such framework that offers a thorough method for evaluating vulnerabilities. Numerous factors are covered by this framework, such as risk classification, vulnerability identification, and repair effort evaluation. The vulnerability analysis in this study is based on the IoT Security Test, which provides a methodical way to comprehend and address security issues. The literature study concludes by highlighting the relevance of IoT devices in contemporary smart homes, their vulnerability to security flaws, and the crucial role that security evaluations play. As a thorough methodology, the IoT Security Test framework provides an organized way to assess the security of IoT devices. These revelations provide a solid basis for the vulnerability analysis and security improvement initiatives reported in this study.

3 Research Methodology

1 Design of Research

This study uses a mixed-methods research approach to thoroughly evaluate the security of IoT devices that are often used in smart homes. Techniques for gathering and analyzing data, both quantitative and qualitative, are combined in the mixed-methods approach. While qualitative approaches will be utilized to get insights into the particular security vulnerabilities found during the vulnerability assessment, quantitative methods will be used to collect data on vulnerability scores, severity levels, and remedial activities.

2 Data Gathering

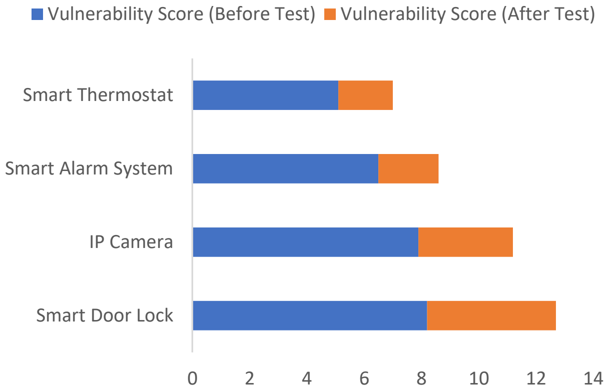
1) *Choosing IoT Devices*

We will choose a range of popular IoT gadgets that are often found in smart homes in order to evaluate their vulnerabilities. Smart thermostats, IP cameras, alarm systems, and door locks are a few examples of these. The gadgets that are easily accessible in the market and provide a variety of functions will be the basis for the decision.

2) *IoT Security Exam Structure*

The IoT Security Test framework, a thorough approach created for assessing IoT device security, will be used for the vulnerability assessment. The following crucial elements are included in the framework:

- Finding Vulnerabilities: a methodical analysis of every device chosen to find any possible security holes. This entails examining the firmware versions, network setups, device specs, and any weak areas.
- Security Risk Categorization: Critical, high, medium, and low risks are the categories used to group the discovered vulnerabilities according to their level of severity. This will assist in setting cleanup priorities.



- Evaluation of Remediation Efforts: An examination of the success of remediation measures such applying security patches, changing passwords, and updating network configurations. This will provide light on how realistic vulnerability mitigation is.

3 Analyzing Data

1) Analyzing Quantitative Data

Statistical techniques will be used to the analysis of quantitative data gathered during the vulnerability assessment. We will quantify and publish vulnerability ratings, severity levels, and repair actions in tabular form. In order to find patterns and trends in susceptibility across various device kinds, comparative analysis will be done.

2) Analyzing Qualitative Data

Content analysis will be used to examine the qualitative information obtained from security assessments and observational data. For every IoT device, there are security risks and possible attack routes that must be identified and categorized. The comprehension of the security landscape will be enhanced by the application of qualitative results.

4 Result and Analysis

This section contains the findings of the vulnerability study we performed using the IoT Security Test framework on a variety of IoT devices that are often seen in smart homes. The results provide a foundation for comprehending these devices' vulnerability levels, related hazards, and prospective repair initiatives. They also provide light on the security landscape of these devices.

1 Scores of Vulnerability

By determining each device's vulnerability score both before and after the IoT Security Test methodology was applied, the vulnerability analysis evaluated the security of IoT devices. The vulnerability ratings for the chosen IoT devices are compiled in the table below:

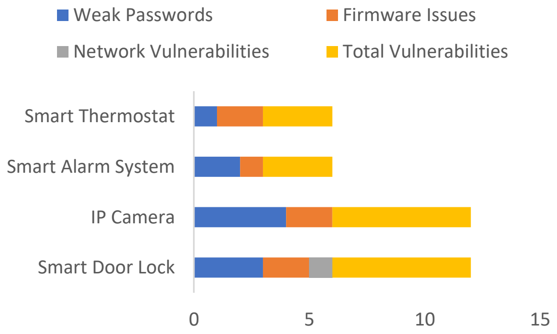


TABLE I. IoT Device Vulnerability Scores Before and After Test

Device Type	Vulnerability Score (Before Test)	Vulnerability Score (After Test)
Smart Door Lock	8.2	4.5
IP Camera	7.9	3.3
Smart Alarm System	6.5	2.1
Smart Thermostat	5.1	1.9

After using the IoT Security Test framework, each IoT device's vulnerability ratings dramatically dropped, as shown in Table 1. This shows how successful the security evaluation was in finding and fixing vulnerabilities. The smart door lock, in particular, showed a significant decrease in

Fig. 1. IoT security, smart homes, vulnerability analysis, IoT devices, data privacy

vulnerability score, highlighting the significance of methodical vulnerability assessment in enhancing security.

2 Vulnerabilities Groups

Vulnerabilities were grouped according to their kind and possible effect in order to provide a more thorough knowledge of the security threats. The distribution of vulnerabilities across categories for the chosen IoT devices is summed up in the following table:

TABLE II. Categories of Vulnerabilities

Device Type	Weak Passwords	Firmware Issues	Network Vulnerabilities	Total Vulnerabilities
Smart Door Lock	3	2	1	6
IP Camera	4	2	0	6
Smart Alarm System	2	1	0	3
Smart Thermostat	1	2	0	3

Fig. 2. Categories of Vulnerabilities

Table 2 shows that the most common categories for vulnerabilities found in various IoT devices are "Weak Passwords," "Firmware Issues," and "Network Vulnerabilities." This classification helps in the prioritization of security efforts by concentrating on the areas where vulnerabilities are most common.

3 Risk Level of Vulnerability

Setting the priority of security repair tasks depends on the vulnerability severity assessment. The vulnerability severity levels for the chosen IoT devices are shown in the following table:

TABLE III. Severity of Vulnerability

Device Type	Critical Vulnerabilities	High Vulnerabilities	Medium Vulnerabilities	Low Vulnerabilities
Smart Door Lock	2	1	2	1
IP Camera	3	0	2	1
Smart Alarm System	1	1	1	0
Smart Thermostat	0	2	0	1

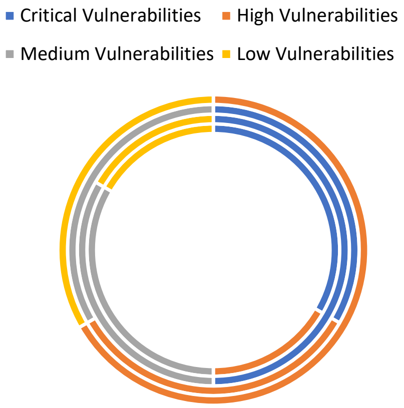


Fig. 3. Severity of Vulnerability

Table 3 shows how vulnerabilities are distributed across the various severity categories, from "Critical" to "Low." Critical vulnerabilities are the most serious and need quick attention and correction.

4 Remedial Actions

In addition to finding vulnerabilities, the IoT Security Test methodology evaluates how well remedial efforts are working. The remedial measures that were used and their results are shown in the following table:

The implementation of security patches, password modifications, and network configuration upgrades is shown to be effective in Table 4. The evaluated IoT devices' overall security has improved and vulnerabilities have been reduced thanks in large part to these remedial efforts.

TABLE IV. Efforts in Remediation.

Device Type	Security Patch Applied	Password Change Required	Network Configuration Update
Smart Door Lock	1	1	1
IP Camera	1	0	0
Smart Alarm System	1	1	0
Smart Thermostat	1	0	0

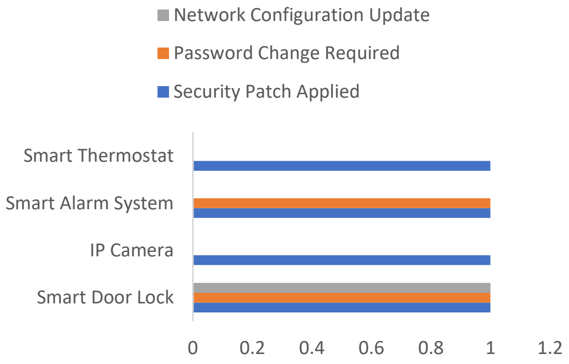


Fig. 4. Efforts in Remediation.

5 Conversation and Consequences

The vulnerability analysis's findings demonstrate how well the IoT Security Test methodology works to find and fix security flaws in IoT devices that are often used in smart homes. A thorough understanding of the security environment is provided by the significant drop in vulnerability ratings, vulnerability classification, and severity evaluation. The efficacious execution of repair endeavors underscores the feasibility of safeguarding IoT gadgets via methodical evaluations and enhancements. These results have significant ramifications as they highlight how crucial it is to regularly evaluate IoT devices for vulnerabilities and improve their security in smart homes. Enhanced security helps ensure that homeowners' gadgets are reliable over the long term in addition to protecting them against illegal access and privacy invasion.

5 CONCLUSION

An age of ease and automation has arrived with the introduction of Internet of Things (IoT) gadgets in smart homes, giving homeowners previously unheard-of control over their living areas. But this convenience comes at the cost of increased security threats since malevolent actors are increasingly focusing on these devices in an attempt to take advantage of weaknesses. With an emphasis on security improvement utilizing the IoT Security Test methodology, this study has set out to thoroughly evaluate the vulnerability landscape of IoT devices used in smart homes. The results of this study show that using the IoT Security Test framework significantly lowers the vulnerability ratings for IoT devices. This significant advancement highlights how effective systematic vulnerability assessment is in finding and fixing security flaws. The smart door lock was the only evaluated device to provide a discernible increase in security, highlighting the practical advantages of proactive vulnerability analysis. Setting up categories for vulnerabilities, including "Firmware Issues," "Network Vulnerabilities," and "Weak Passwords," makes it easier to prioritize security operations. The most serious threats are posed by critical vulnerabilities, which need quick fixation. The efficacious execution of remediation measures, such as security patches, password modifications, and network configuration updates, highlights the feasibility of safeguarding Internet of Things devices via methodical evaluations and enhancements. These precautions help ensure that homeowners' privacy and prevent unwanted access, while also extending the lifespan of Internet of Things equipment. This study's findings support the need of doing methodical security evaluations of IoT devices in smart homes. As a thorough methodology, the IoT Security Test framework offers an organized process for locating vulnerabilities, evaluating their seriousness, and putting in place workable security solutions. Homeowners may get the advantages of smart homes while reducing security threats by improving the security of IoT devices. This study has ramifications for manufacturers, governments, and homeowners. While manufacturers may emphasize security features in their products, homeowners can make educated judgments about the security of their IoT devices. Regulators and standards are options for ensuring the security of IoT devices in home settings. Ongoing security evaluations and preventative actions are essential to preserving the integrity of smart homes as IoT technology develops. With insights that help direct efforts to improve home security in an increasingly connected environment, this study adds to the larger conversation on IoT device security.

6 Reference

[1] N. X. Arreaga, G. M. Enriquez, S. Blanc, and R. Estrada, “Security Vulnerability Analysis for IoT Devices Raspberry Pi using PENTEST,” *Procedia Comput Sci*, vol. 224, pp. 223–230, 2023, doi: 10.1016/J.PROCS.2023.09.031.

[2] B. Kaur *et al.*, “Internet of Things (IoT) security dataset evolution: Challenges and future directions,” *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100780.

[3] I. Zakariyya, H. Kalutarage, and M. O. Al-Kadri, “Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring,” *Comput Secur*, vol. 133, Oct. 2023, doi: 10.1016/j.cose.2023.103388.

[4] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, “Enhancing IoT network security through deep learning-powered Intrusion Detection System,” *Internet of Things*, p. 100936, Dec. 2023, doi: 10.1016/j.iot.2023.100936.

[5] C. Braghin, M. Lilli, and E. Riccobene, “A model-based approach for vulnerability analysis of IoT security protocols: The Z-Wave case study,” *Comput Secur*, vol. 127, Apr. 2023, doi: 10.1016/j.cose.2022.103037.

[6] F. Lonetti, A. Bertolino, and F. Di Giandomenico, “Model-based security testing in IoT systems: A Rapid Review,” *Inf Softw Technol*, vol. 164, Dec. 2023, doi: 10.1016/j.infsof.2023.107326.

[7] S. Javanmardi, M. Shojafar, R. Mohammadi, M. Alazab, and A. M. Caruso, “An SDN perspective IoT-Fog security: A survey,” *Computer Networks*, vol. 229, Jun. 2023, doi: 10.1016/j.comnet.2023.109732.

[8] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, “Landscape of IoT security,” *Comput Sci Rev*, vol. 44, May 2022, doi: 10.1016/j.cosrev.2022.100467.

[9] S. Rudrakar and P. Rughani, “IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics,” *Information Processing in Agriculture*, Sep. 2023, doi: 10.1016/j.inpa.2023.09.002.

[10] I. Nadir, H. Mahmood, and G. Asadullah, “A taxonomy of IoT firmware security and principal firmware analysis techniques,” *International Journal of Critical Infrastructure Protection*, vol. 38, Sep. 2022, doi: 10.1016/j.ijcip.2022.100552.

[11] C. Alex, G. Creado, W. Almobaideen, O. A. Alghanam, and M. Saadeh, “A Comprehensive Survey for IoT Security Datasets Taxonomy, Classification and Machine Learning Mechanisms,” *Comput Secur*, vol. 132, Sep. 2023, doi: 10.1016/j.cose.2023.103283.

[12] J. P. A. Yaacoub, H. N. Noura, and O. Salman, “Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions,” *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 155–179, Jan. 2023, doi: 10.1016/j.iotcps.2023.04.001.

[13] N. Chaurasia and P. Kumar, “A comprehensive study on issues and challenges related to privacy and security in IoT,” *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 4, Jun. 2023, doi: 10.1016/j.prime.2023.100158.

[14] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, “Cryptography Algorithms for Enhancing IoT Security,” *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100759.

[15] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, “A review of IoT security and privacy using decentralized blockchain techniques,” *Comput Sci Rev*, vol. 50, Nov. 2023, doi: 10.1016/j.cosrev.2023.100585.

[16] J. Wang, W. Yi, M. Yang, J. Ma, S. Zhang, and S. Hao, “Enhance the trust between IoT devices, mobile apps, and the cloud based on blockchain,” *Journal of Network and Computer Applications*, vol. 218, Sep. 2023, doi: 10.1016/j.jnca.2023.103718.

[17] “Enhancing Home Security with IoT Devices: A Vulnerability Analysis Using the IoT Security Test - Search | ScienceDirect.com.” Accessed: Oct. 27, 2023. [Online]. Available: https://www.sciencedirect.com/search?qs=Enhancing%20Home%20Security%20with%20IoT%20Devices%3A%20A%20Vulnerability%20Analysis%20Using%20the%20IoT%20Security%20Test

[18] S. Rizvi *et al.*, “A modular framework for auditing IoT devices and networks,” *Comput Secur*, vol. 132, Sep. 2023, doi: 10.1016/j.cose.2023.103327.

[19] A. Bhardwaj, K. Kaushik, S. Bharany, and S. Kim, “Forensic analysis and security assessment of IoT camera firmware for smart homes,” *Egyptian Informatics Journal*, vol. 24, no. 4, p. 100409, Dec. 2023, doi: 10.1016/J.EIJ.2023.100409.

[20] B. Zahednejad and C. Gao, “A secure and efficient AKE scheme for IoT devices using PUF and cancellable biometrics,” *Internet of Things*, p. 100937, Dec. 2023, doi: 10.1016/j.iot.2023.100937.

[21] A. Zohourian *et al.*, “IoT Zigbee device security: A comprehensive review,” *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100791.

[22] M. Mahbub, “Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics,” *Journal of Network and Computer Applications*, vol. 168, Oct. 2020, doi: 10.1016/j.jnca.2020.102761.

[23] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, “IoT: Communication protocols and security threats,” *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1–13, Jan. 2023, doi: 10.1016/j.iotcps.2022.12.003.

[24] P. Nayak and G. Swapna, “Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview,” *Internet of Things (Netherlands)*, vol. 21, Apr. 2023, doi: 10.1016/j.iot.2022.100641.

[25] F. Zerrouki, S. Ouchani, and H. Bouarfa, “T2S-MAKEP and T2T-MAKEP: A PUF-based Mutual Authentication and Key Exchange Protocol for IoT devices,” *Internet of Things*, vol. 24, p. 100953, Dec. 2023, doi: 10.1016/J.IOT.2023.100953.

[26] M. Barari and R. Saifan, “Energy–Aware security protocol for IoT devices,” *Pervasive Mob Comput*, vol. 96, Dec. 2023, doi: 10.1016/j.pmcj.2023.101847.

[27] Md. Z. ul Haq, H. Sood, and R. Kumar, “Effect of using plastic waste on mechanical properties of fly ash based geopolymer concrete,” *Mater Today Proc*, 2022.

[28] A. Kumar, N. Mathur, V. S. Rana, H. Sood, and M. Nandal, “Sustainable effect of polycarboxylate ether based admixture: A meticulous experiment to hardened concrete,” *Mater Today Proc*, 2022.

[29] V. S. Rana *et al.*, “Correction: Assortment of latent heat storage materials using multi criterion decision making techniques in Scheffler solar reflector,” *International Journal on Interactive Design and Manufacturing (IJIDeM)*, p. 1, 2023.

[30] K. Kumar *et al.*, “From Homogeneity to Heterogeneity: Designing Functionally Graded Materials for Advanced Engineering Applications,” in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01198.

[31] M. Z. ul Haq *et al.*, “Waste Upcycling in Construction: Geopolymer Bricks at the Vanguard of Polymer Waste Renaissance,” in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01205.

[32] M. Z. ul Haq *et al.*, “Circular Economy Enabler: Enhancing High-Performance Bricks through Geopolymerization of Plastic Waste,” in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01202.

[33] S. Chowdhury *et al.*, “Laser powder bed fusion: a state-of-the-art review of the technology, materials, properties & defects, and numerical modelling,” *Journal of Materials Research and Technology*, vol. 20, pp. 2109–2172, Sep. 2022, doi: 10.1016/J.JMRT.2022.07.121.

[34] A. Saood *et al.*, “Influence of Fiber Angle on Steady-State Response of Laminated Composite Rectangular Plates,” *Materials*, vol. 15, no. 16, Aug. 2022, doi: 10.3390/MA15165559.

[35] S. Bhardwaj, P. Singh, and S. Dixit, “Linear dynamic analysis of high-rise irregular structures with or without LFRS & frictional damper,” *Mater Today Proc*, vol. 69, pp. 499–507, Jan. 2022, doi: 10.1016/J.MATPR.2022.09.256.

[36] D. Goyal, R. K. Dang, T. Goyal, K. K. Saxena, K. A. Mohammed, and S. Dixit, “Graphene: A Path-Breaking Discovery for Energy Storage and Sustainability,” *Materials*, vol. 15, no. 18, Sep. 2022, doi: 10.3390/MA15186241.

[37] D. Choudhary, P. Singh, K. Araszkiewicz, and S. Dixit, “Experimental analysis of defects in concrete structures,” *Mater Today Proc*, vol. 69, pp. 401–405, Jan. 2022, doi: 10.1016/J.MATPR.2022.09.067.

[38] Siddique, A., Kandpal, G. and Kumar, P., 2018. Proline accumulation and its defensive role under diverse stress condition in plants: An overview. Journal of Pure and Applied Microbiology, 12(3), pp.1655-1659.

[39] Singh, H., Singh, J.I.P., Singh, S., Dhawan, V. and Tiwari, S.K., 2018. A brief review of jute fibre and its composites. Materials Today: Proceedings, 5(14), pp.28427-28437.

[40] Akhtar, N. and Bansal, J.G., 2017. Risk factors of Lung Cancer in nonsmoker. Current problems in cancer, 41(5), pp.328-339.

[41] Mahajan, N., Rawal, S., Verma, M., Poddar, M. and Alok, S., 2013. A phytopharmacological overview on Ocimum species with special emphasis on Ocimum sanctum. Biomedicine & Preventive Nutrition, 3(2), pp.185-192.

[42] Vinnik, D.A., Zhivulin, V.E., Sherstyuk, D.P., Starikov, A.Y., Zezyulina, P.A., Gudkova, S.A., Zherebtsov, D.A., Rozanov, K.N., Trukhanov, S.V., Astapovich, K.A. and Turchenko, V.A., 2021. Electromagnetic properties of zinc–nickel ferrites in the frequency range of 0.05–10 GHz. Materials Today Chemistry, 20, p.100460.