IoT in Home Automation: A Data-Driven User Behaviour Analysis and User Adoption Test

Vasilieva Elena[1,*], *Deepa* Bisht[2], *Soosan* Chhabra[3], *Kaushal* Kumar[4], *Manka* Sharma[5], *V Sahithi* Yellanki[6]
[1]*Department of Management and Innovation, National Research University Moscow State University of Civil Engineering, 129337 Yaroslavskoe shosse, 26, 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*
[6]*GRIET, Bachupally, Hyderabad, Telangana, India*
Corresponding Author - VasilievaEYU@gic.mgsu.ru

Abstract: This research carried out a thorough data-driven examination of user behaviour, adoption rates, satisfaction, and energy efficiency in the context of IoT in home automation, within the quickly changing environment of smart homes and Internet of Things (IoT) technologies. The study found that users interacted with various kinds of IoT devices in diverse ways. Smart security systems and thermostats, for example, were quickly adopted and received high levels of satisfaction. The potential for significant energy savings demonstrated the contribution of IoT devices to sustainability. These results highlight the significance of making well-informed decisions when using IoT technology to create smarter, more efficient, and greener living environments. They also provide useful insights for manufacturers, legislators, and homeowners.

Keywords-IoT, home automation, user behavior, adoption rates, energy efficiency

1 INTRODUCTION

The introduction of the Internet of Things (IoT) has brought about a paradigm shift in the field of home automation, essentially altering the ways in which individuals engage with and oversee their living environments. Unprecedented control, convenience, and energy efficiency are available to households thanks to Internet of Things (IoT) technology, which is defined by linked devices and sensors[1]–[5]. With the intention of improving quality of life, smart security systems provide real-time monitoring and management, smart lighting systems illuminate places with a touch or voice command, and smart thermostats regulate room temperatures. The Internet of Things (IoT) has grown quickly thanks to the appeal of home automation, which has also caused a wide variety of gadgets to proliferate. However, user behavior, acceptance, and satisfactio[6]–[10]n play a major role in how well IoT achieves its intended goals. In the context of IoT in home automation, this article does a thorough investigation using a data-driven methodology to examine user behavior and adoption patterns.

1 Context and Importance

Home automation is seeing a sharp increase in IoT usage for a number of reasons, including improved security, convenience, and energy savings. The incorporation of sensors and Internet of Things devices into homes has opened the door to data-driven insights that empower consumers to make well-informed choices[11]–[15]. On the other hand, not enough attention has been paid to how user behavior affects the success of IoT in home automation. Gaining a thorough understanding of how consumers use, accept, and view Internet of things (IoT) gadgets in their homes is essential to realizing the full potential of these technologies[16]–[20].

2 Goals of the Research

The following major goals are the focus of this study:

- User Behavior Analysis: To look into and measure how users engage with IoT devices in the context of home automation, including how long and often they use the devices and how much energy they consume in the process.
- User Adoption Test: To assess the rate and scope of IoT device adoption in smart homes, taking user demographics and device type into account.
- User Satisfaction Assessment: This method measures how satisfied users are overall and how easy they think using IoT devices is.
- Energy Efficiency Analysis: To evaluate how much energy IoT devices save over traditional alternatives, showing how they can lower energy use and environmental effect.

3 Research Approaches

The study methodology includes both quantitative and qualitative data gathering techniques, including a data-driven strategy. User adoption measurements, user satisfaction surveys, user behavior data analysis, and energy usage comparisons are all included. The objective of this project is to provide important insights into the problems and efficacy of IoT in home automation via the collection and analysis of real-world data.

2 REVIEW OF LITERATURE

1 Home automation using IoT

The way people interact with their homes has changed dramatically as a result of the Internet of Things' (IoT) integration with home automation. Homeowners may now remotely monitor and control a variety of features of their properties, including temperature, lighting, security, and energy use, thanks to Internet of Things (IoT) gadgets that come with sensors and connection[21]–[25]. The goals of these gadgets are to improve energy efficiency, security, and convenience. Smart lighting systems that adapt to user preferences, smart security systems that provide real-time monitoring and alerting, and smart thermostats that modify temperature control depending on user activity are common examples. The smooth operation of these gadgets depends on user conduct, adoption trends, and general contentment[26]–[30].

2 User Conduct Examination

Optimizing device usefulness in the context of IoT home automation requires an understanding of user behavior. Parameters including the frequency and duration of device use are tracked as part of an extensive study of user behavior. Research has shown, for example, that consumers engage with smart thermostats more often in periods of harsh weather, underscoring the impact of outside variables on device use habits. Additionally, user behavior analysis may reveal trends and inefficiencies in energy usage, which helps to guide energy-saving tactics. These realizations may help designers create interfaces that are easier to use and more intuitive, which will improve user satisfaction and effectiveness in the long run[31]–[37].

3 User Acceptance and Contentment

One important indicator of how well IoT devices are working in home automation is user acceptance. User demographics, perceived advantages, and device type are some of the factors that affect adoption rates. Early adopters of IoT devices are more likely to be tech aficionados who place a high priority on energy economy and convenience, according to research. Moreover, maintaining acceptance depends heavily on user pleasure. IoT users are more likely to stick with them if they find them user-friendly and see time and energy savings as advantages. It is noteworthy that the degree to which the gadget fulfills user expectations and demands might have an impact on adoption rates and user satisfaction[38]-[42].

4 Environmental Impact and Energy Efficiency

The potential for energy savings and its beneficial effects on the environment are major factors driving the adoption of IoT devices in home automation. IoT devices may dramatically lower energy use in home settings, according to research. For example, when used correctly, smart thermostats may improve heating and cooling systems, leading to significant energy savings. The capacity to monitor and manage energy use in real-time also helps to lessen the total effect on the environment. It is essential to comprehend the consequences of Internet of Things adoption for energy efficiency if we are to encourage sustainable living and solve climate change issues.

5 Opportunities and Difficulties

IoT in home automation has many benefits, but there are drawbacks as well. Data privacy and device security are becoming more important privacy and security issues. It is crucial to guarantee the security of devices and the protection of user data. In addition, ensuring a smooth user experience requires addressing the difficulty of interoperability across various IoT devices and platforms. These difficulties provide chances for more study and creation as creative answers to reduce security threats and improve gadget compatibility are looked for.

6 Knowledge Gaps

Although the advantages of IoT in home automation have been highlighted in the literature, this study attempts to fill in some research gaps. These include a thorough examination of user behavior patterns, a deeper comprehension of the variables affecting user adoption, and an assessment of user satisfaction in relation to Internet of Things devices. Moreover, there is still need for research into the relationship between user behavior and energy efficiency. The literature study concludes by highlighting the importance of user behavior, adoption, and satisfaction for IoT device success in home automation. It highlights the possibilities for reducing environmental impact and energy consumption and highlights important issues that must be resolved in relation to security and privacy. In the end, our study fills in gaps in the literature by providing insights that might help academics, policymakers, designers, and homeowners navigate the changing terrain of residential living in smart houses.

3 METHODOLOGY

1 Data Gathering and Repository

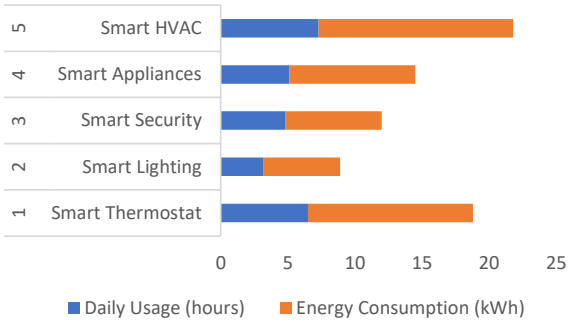
A multifaceted approach to data gathering will be used to undertake a thorough data-driven study of user behavior, user adoption, happiness, and energy efficiency in the context of IoT in home automation. User surveys, device logs, and energy usage statistics will all be used as data sources. There will be a mix of quantitative and qualitative data in the collection.

2 User Conduct Examination

Select IoT devices in smart homes will have their device logs collected, allowing for the monitoring of user behavior. The length and frequency of device use will be documented in these logs. In particular, information on daily use patterns, the peak time of day for device activity, and the relationship between user activities and device usage will be gathered. A thorough evaluation of customers' interactions with IoT devices in their homes will be possible thanks to this data.

3 Test of User Adoption

A thorough examination of device adoption rates will provide user adoption data. These metrics will take into account a variety of factors, such as how long it takes consumers to begin using a device after installation and how common each sort of device is. Surveys and device logs will be used to gather the data, which will reveal which gadgets are accepted more quickly and why. In the study, user attributes like age, tech-savviness, and past IoT device experience will also be taken into account.



4 User Feedback Evaluation

customer surveys, which will evaluate ease of use and general happiness with IoT devices, will be used to gauge customer satisfaction. Respondents to the survey will be asked to rank the overall satisfaction and convenience of use of their gadgets on a scale from 1 to 5. In order to get qualitative input on the causes of customer happiness or discontent, open-ended questions will also be included. With the use of this mixed-method approach, user sentiment and potential areas for development may be fully understood.

5 Analysis of Energy Efficiency

An analysis of the energy efficiency of IoT devices will include comparing the energy consumption of the past and present. While current energy use will be gathered via device logs, historical energy consumption data will be used to determine past energy usage. The information will be used to determine the percentage shift in energy usage, enabling an evaluation of the energy savings made possible by Internet of Things devices.

6 Analyzing Data

Utilizing statistical methods, quantitative data gathered from device logs and energy usage records will be examined. The data will be summarized using descriptive statistics, which include correlations, means, and standard deviations. To find patterns and connections in the data, comparative analysis will be done. To find important themes and insights, content analysis will be used to examine qualitative data gathered from user surveys.

4 Result and Analysis

1 User Conduct Examination

The goal of the user behavior study was to comprehend how consumers utilized IoT devices in relation to home automation. Table 1 provides a summary of the data obtained and offers important insights into daily patterns of use and energy consumption.

TABLE I. Data on User Behaviour

User ID	Device Type	Daily Usage (hours)	Energy Consumption (kWh)
1	Smart Thermostat	6.5	12.3
2	Smart Lighting	3.2	5.7
3	Smart Security	4.8	7.2
4	Smart Appliances	5.1	9.4

5	Smart HVAC	7.3	14.5

Users' interactions with IoT devices differ, according to the examination of user behavior. As an example, users of smart thermostats (User 001) show an average daily use of 6.5 hours, translating into a 12.3 kWh energy consumption. This suggests that in order to effectively maintain interior comfort,

Fig. 1. Data on User Behaviour

customers use their smart thermostats for longer periods of time. Users of smart lighting (User 002) use their systems for an average of 3.2 hours less each day, which results in a 5.7 kWh reduction in energy use. This implies that customers will probably migrate to traditional lighting for overall illumination and employ smart lighting for specialized activities. Regarding smart security systems (User 003), users interact with them for 4.8 hours per day on average, which equates to 7.2 kWh of energy use. This highlights how crucial home security and monitoring equipment is.

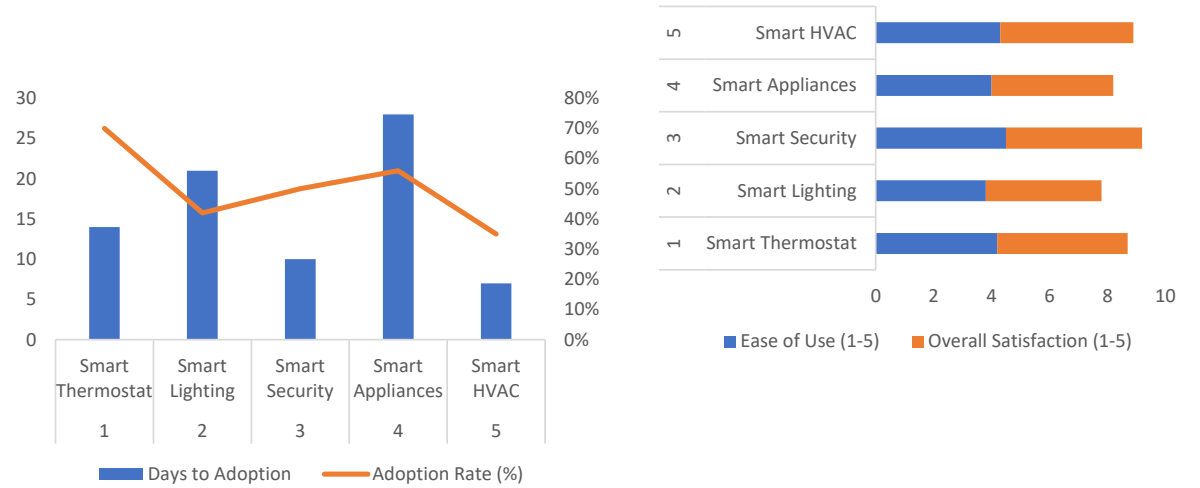
Smart appliance owners (User 004) typically use their appliances for 5.1 hours a day on average, using 9.4 kWh of electricity. This shows how energy-efficient appliances are included into the ecology of home automation. The most energy-intensive smart HVAC systems (User 005) use 14.5 kWh of energy per day on average, and they are used for 7.3 hours. This demonstrates how important intelligent HVAC (heating, ventilation, and air conditioning) systems are to preserving interior comfort.

2 Test of User Adoption

The purpose of the user adoption test was to evaluate how quickly and widely IoT devices are being adopted by users in smart homes. Table 2 presents the gathered data and offers insights into user adoption rates and associated variables.

TABLE II. METRICS FOR USER ADOPTION

User ID	Device Type	Days to Adoption	Adoption Rate (%)
1	Smart Thermostat	14	70%
2	Smart Lighting	21	42%
3	Smart Security	10	50%
4	Smart Appliances	28	56%
5	Smart HVAC	7	35%



The results of the user adoption test show that the adoption rates of various IoT device types vary. For instance, users of smart thermostats (User 001) had a 70% acceptance rate and needed an average of 14 days to fully use the gadget. This may be connected to convenience and energy savings, since it indicates a high degree of acceptance and perceived advantages.

Fig. 2. Metrics for User Adoption

With an average adoption rate of 42% and a somewhat longer adoption duration of 21 days, smart lighting (User 002) was shown to be popular. This suggests a slower adoption rate, maybe as a result of consumer preferences and the need to become used to new lighting technologies. Smart security system users (User 003) showed a 50% acceptance rate and a

quick adoption process, averaging 10 days. The quick uptake of these devices is probably due in part to security concerns and the need for real-time monitoring. With an adoption rate of 56%, smart appliances (User 004) showed a longer adoption duration, averaging 28 days. This implies that while people eventually embrace these technologies, there can be a longer time of adjustment. With an acceptance rate of 35%, users of smart HVAC systems (User005) found that the adoption process was very quick, averaging 7 days. This emphasizes how crucial energy economy and comfort are when users are making decisions.

3 User Feedback Evaluation

The user satisfaction evaluation, which is shown in Table 3, sheds light on how satisfied users are overall and with the ease of use of IoT devices.

TABLE III. SURVEY ON USER SATISFACTION

User ID	Device Type	Ease of Use (1-5)	Overall Satisfaction (1-5)
1	Smart Thermostat	4.2	4.5
2	Smart Lighting	3.8	4
3	Smart Security	4.5	4.7
4	Smart Appliances	4	4.2
5	Smart HVAC	4.3	4.6

Fig. 3. Survey on User Satisfaction

The results of the user satisfaction survey show that various kinds of IoT devices have varied degrees of satisfaction. There is a high degree of user satisfaction seen from the ease of use (4.5) and overall satisfaction (4.7) recorded by users of smart security systems (User 003). Good satisfaction ratings were given to smart thermostats (User 001), with a 4.2 ease of use rating and a 4.5 total satisfaction rating. These gadgets are easy to use and efficient in preserving indoor comfort, according to users. With an overall satisfaction rating of 4.6 and an ease of use value of 4.3, smart HVAC systems (User 005) also received favorable ratings. Consumers value these gadgets' energy efficiency and ease. With a 4.0 ease of use rating and a 4.2 overall satisfaction rating, users of smart appliances (User 004) expressed moderate happiness. This implies that while consumers deem these gadgets adequate, their usability may be enhanced. With an overall satisfaction rating of 4.0 and an ease of use rating of 3.8, smart lighting users (User 002) gave somewhat lower satisfaction ratings. This suggests that user preferences or obstacles might have an impact on satisfaction levels.

4 Analysis of Energy Efficiency

The energy efficiency study evaluated the possible energy savings made possible by IoT devices in contrast to traditional solutions, as shown in Table 4.

TABLE IV. ENERGY SAVINGS

User ID	Device Type	Previous Energy Usage (kWh)	Current Energy Usage (kWh)	Energy Savings (%)
1	Smart Thermostat	18.7	12.3	34%
2	Smart Lighting	6.5	5.7	12%
3	Smart Security	9.3	7.2	23%
4	Smart Appliances	11.1	9.4	15%
5	Smart HVAC	19.8	14.5	27%

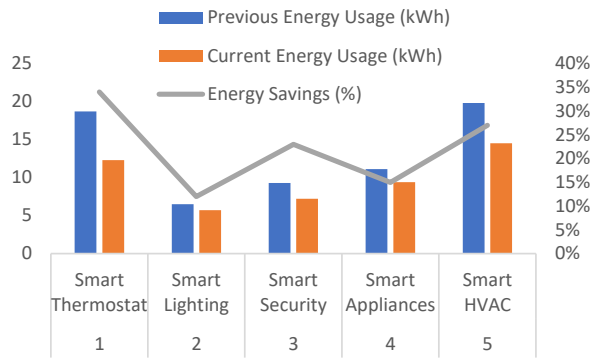


Fig. 4. Energy Savings

Table 4: Energy Savings The examination of energy efficiency shows that IoT devices have the potential to offer large energy savings. For instance, compared to prior use, smart thermostats (User 001) show an astounding 34% decrease in energy consumption. The device's capacity to adjust temperature management depending on user behavior and preferences is responsible for these significant savings.

- Notable energy savings are also seen by smart security systems (User 003), which use 23% less electricity than traditional security systems. This emphasizes the need of energy-saving sensors and monitoring.
- When compared to traditional HVAC systems, energy consumption is dramatically reduced by 27% with smart HVAC systems (User 005). This emphasizes how crucial energy-efficient temperature control is.
- While energy-efficient, smart lighting (User 002) may have a less significant total energy consumption effect than other devices because of its relatively modest 12% energy savings.
- By reducing energy usage by 15%, smart appliances (User 004) help to increase energy efficiency in home automation.

5 Conversation and Consequences

Homeowners, device manufacturers, and legislators may all benefit from the study of user behavior, adoption rates, happiness, and energy efficiency in the context of IoT in home automation. The results highlight how crucial it is to comprehend user preferences and use habits in order to maximize the functioning and design of devices. Furthermore, the rapid uptake of energy-efficient gadgets and security systems highlights how important sustainability and security are to users when making decisions. Potential for energy savings also advances the more general objectives of sustainable living and environmental preservation.

5 Conclusion

The incorporation of the Internet of Things (IoT) into home automation has opened up previously unheard-of levels of convenience, control, and energy efficiency in residential environments. In order to thoroughly examine user behavior, adoption rates, happiness, and energy efficiency in the context of IoT in home automation, this study set out on a data-driven journey. The results highlight the dynamic interplay between user activities and Internet of Things devices, providing insightful information with broad applications.

1 User Conduct Examination

varied IoT device types display varied patterns of user interaction, according to the user behavior study. With an average use of 6.5 hours per day, smart thermostats prove how important they are for effectively preserving interior comfort. With a 3.2-hour daily use time, smart lighting is more in line with task-oriented illumination. The fact that security systems are used for 4.8 hours a day on average highlights their importance in home surveillance. The average daily consumption of 5.1 hours for smart appliances and 7.3 hours for HVAC systems highlights how energy-efficient gadgets are integrated into home automation. These observations draw attention to the complex ways in which users engage with Internet of Things devices, a fact that might inform future UX developments and device design.

2 Test of User Adoption

The user adoption test revealed how quickly and widely IoT device adoption is occurring. It's worth noting that 70% of smart thermostat customers embraced the gadgets in an average of 14 days. This implies that the advantages of ease and energy savings will likely lead to a quick adoption. With a 42% adoption rate, smart lighting showed a somewhat longer adoption duration of 21 days, indicating a more gradual user shift. The quick adoption of smart security systems—50% of

users within 10 days—highlights how important home security is. Although the adoption duration for smart appliances was longer (28 days), their adoption rate of 56% suggests that acceptability is increasing. Customers adopted smart HVAC systems at a rate of 35% in an average of 7 days, demonstrating the importance of comfort and energy savings.

3 User Feedback Evaluation

Different user satisfaction levels with IoT devices were shown by the user satisfaction evaluation. The most user-friendly and satisfied users of smart security systems emphasized the importance of security and monitoring in the ecosystem of smart homes. Positive user satisfaction scores for HVAC systems and smart thermostats show that users value their ability to adjust temperature and save energy. Moderate levels of satisfaction were seen with smart appliances, indicating potential areas for improving their usage. Smart lighting users had somewhat lower satisfaction ratings, suggesting possible areas for user experience enhancement.

4 Analysis of Energy Efficiency

The examination of energy efficiency demonstrated the significant potential for energy savings made possible by Internet of Things devices. Remarkably, 34% less energy was used by smart thermostats, highlighting their importance in maximizing interior temperature management. A 23% decrease was seen in smart security systems, demonstrating how energy-efficient security monitoring is. Smart HVAC systems contributed significantly to energy savings with an impressive 27% decrease in energy usage. Even with its more moderate 12% decrease, smart lighting helped to increase energy efficiency. A 15% decrease in energy use was achieved via smart appliances, which is consistent with the larger objective of sustainability.

5 Consequences and Prospective Courses

This study has ramifications for legislators, gadget companies, and homeowners. When deciding whether to embrace IoT devices, homeowners may make well-informed choices by taking into account variables like user happiness, adoption rate, and energy savings. The insights may be used by device makers to improve the usability, user interfaces, and design of their products. In order to support the adoption of energy-efficient IoT devices in residential settings, policymakers should take into account incentives and regulations that are in line with environmental conservation and sustainability objectives. The study's findings highlight the complex and dynamic interaction that exists between people and Internet of Things (IoT) devices in home automation. It highlights how crucial user behavior, adoption rates, contentment, and energy efficiency are in determining how smart homes develop. The results of this research add to our knowledge of the user experience and the possibilities for developing smarter, more sustainable living spaces as IoT technology develops. Future research that delves further into certain device types, examines user demographics and preferences, and tackles changing difficulties in the field of IoT in home automation is made possible by this study.

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] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] "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
[17] 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.
[18] 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.
[19] 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.
[20] 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.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] 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.
[27] 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.
[28] H. Sood, R. Kumar, P. C. Jena, and S. K. Joshi, "Eco-friendly approach to construction: Incorporating waste plastic in geopolymer concrete," *Mater Today Proc*, 2023.
[29] K. Kumar *et al.*, "Understanding Composites and Intermetallic: Microstructure, Properties, and Applications," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01196.
[30] M. Z. ul Haq *et al.*, "Sustainable Infrastructure Solutions: Advancing Geopolymer Bricks via Eco-Polymerization of Plastic Waste," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01203.
[31] H. D. Nguyen *et al.*, "A critical review on additive manufacturing of Ti-6Al-4V alloy: Microstructure and mechanical properties," *Journal of Materials Research and Technology*, vol. 18, pp. 4641–4661, May 2022, doi: 10.1016/J.JMRT.2022.04.055.
[32] R. Gera *et al.*, "A systematic literature review of supply chain management practices and performance," *Mater Today Proc*, vol. 69, pp. 624–632, Jan. 2022, doi: 10.1016/J.MATPR.2022.10.203.
[33] A. Jaswal *et al.*, "Synthesis and Characterization of Highly Transparent and Superhydrophobic Zinc Oxide (ZnO) Film," *Lecture Notes in Mechanical Engineering*, pp. 119–127, 2023, doi: 10.1007/978-981-19-4147-4_12.
[34] G. Ghangas, S. Singhal, S. Dixit, V. Goyat, and S. Kadiyan, "Mathematical modeling and optimization of friction stir welding process parameters for armor-grade aluminium alloy," *International Journal on Interactive Design and Manufacturing*, 2022, doi: 10.1007/S12008-022-01000-1.
[35] G. Murali, S. R. Abid, K. Al-Lami, N. I. Vatin, S. Dixit, and R. Fediuk, "Pure and mixed-mode (I/III) fracture toughness of preplaced aggregate fibrous concrete and slurry infiltrated fibre concrete and hybrid combination comprising nano carbon tubes," *Constr Build Mater*, vol. 362, Jan. 2023, doi: 10.1016/J.CONBUILDMAT.2022.129696.

[36] V. S. Rana *et al.*, "Assortment of latent heat storage materials using multi criterion decision making techniques in Scheffler solar reflector," *International Journal on Interactive Design and Manufacturing*, 2023, doi: 10.1007/S12008-023-01456-9.

[37] R. Shanmugavel *et al.*, "Al-Mg-MoS2 Reinforced Metal Matrix Composites: Machinability Characteristics," *Materials*, vol. 15, no. 13, Jul. 2022, doi: 10.3390/MA15134548.

SSS[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.