

Midocean University



Faculty of Management

College of Management/ Project Management

User-Centric Evaluation of Multipurpose Security Systems

Student name

Mahdi Abdullah Alawwad

Graduation Project – 1

Faculty of Management - Midocean University

Supervisor

Dr. Mona Moustafa Elashry

Faculty member- Faculty of management- Midocean University

1st Semester- 2024

Abstract

The project investigated the topic of multipurpose IoT home security systems, determining users' level of satisfaction and experience. This study chiefly examined the degree to which these modern security solutions fit into the real-life needs and requirements of their users. It reflected the increasing demand for home security systems which, in addition to robust security options, users could easily access, understand and integrate with their daily lives, thus identifying a gap in existing literature and in market offerings.

The research problem mainly focused on the issue of whether the existing IoT-based security systems are able to meet user expectations in different aspects like usability, satisfaction and overall experience. With the fast-paced changes in technology in the security domain, there was a pressing need to make sure that these innovations translate into real benefits for users most importantly when it comes to improving the sense of security and ease of usage.

In an attempt to deal with this issue, the project applied a mixed methods approach, which combined the collection and analysis of both quantitative and qualitative data. Through surveys which were distributed to a wide range of users, the levels of their satisfaction with different aspects of security were quantified. Furthermore, semi-structured interviews with security experts, system developers, and users were carried out for a qualitative perspective on the actual deployment, effectiveness, and shortcomings of these systems.

The key takeaway from this thorough study proved that user-centered design plays a major role in the development of home security systems. It highlighted the fact that a high level of demand and acceptance is associated with this system, but also that there are many ways of improving user experience by making it more usable, personalized and easier to understand. Thus, the study possess significant implications for the design of future home security systems, prompting us to prioritise customised innovation for users.

Literature Review

The consequent development of multi-faceted security systems in the face of changing security needs has created a platform for tremendous academic and industrial-based research. This literature review covers security system technology advancements, their success in various circumstances, user interactions as well as the possibility of combining the systems with others in which we focus on the present state of affairs that need further investigation.

Technological Advancements in Security Systems

The diversity of security systems technology has been largely driven by the integration of digital technologies and IoT. Literature gives examples of numerous methods and technologies that are used for protecting organizations, industries and residential areas, showing the chronological flow of the developments.

The work of Karri and Lim (2005) utilized SMS-based alert system which made use of the internet for the fast and reliable notifications that goes beyond conventional text alerts. This is an early step of integrating digital technology in security systems for more effective communication.

Govinda, et al. (2014) investigated the design and process of the implementation of security alarm systems using GSM (Global System for Mobile Communications) technology, through the use of the Internet of Things (IoT) framework. They proposed an approach through motion detection through camera surveillance which sends notifications and alarms upon activation.



Figure 1: Surveillance system (Gobinda et al. 2014)

Anitha and Kalra (2016) took the matter to another level introducing IoT (Internet of Things) and the optical Morse code in the electronic lock system. Utilizing LEDs and a photoreceiver connected to the microprocessor, the system does lock monitoring and control remotely through cloud technology, which received the praise of good interface and cheapness.

Recently, Cavas and Ahmad (2019) addressed the issue of intrusion detection through LDR and laser ray sensors. These systems, which activate alarms and inform of light beam breakage via messages, can be considered as a revolutionary security system. On the other hand, there is a concern that intruders could intentionally do so in order to get around the rays by which this method is based, thereby showing the limitation of this approach.

As stated by Yadav et al. (2021) security system technologies have gradually turned into multipurpose systems incorporating alarms and display functionalities. This shift has been

powered by the integration of the Internet of Things (IoT), through which the approach to home security has developed and the real-time data exchange and remote control of the devices have been enabled. The review shows how some innovative technologies that have become available and cheap because of technology advancements have such as fiber sensors, accelerometers and global mobile communication systems. These innovations are primarily intended to provide residents with fast, convenient and secure access to their homes, thus improving both security and convenience.

This demonstrates that modern security system technologies are constantly evolving, from SMS alerts to advanced IoT solutions, this being an indication that technological innovation is ongoing in pursuit of improved security.

Effectiveness of Multipurpose Security Systems

The efficacy of multipurpose security systems remains a matter of intense investigation within security and surveillance technologies sector. The function of diverse surveillance components into a well-intended system based on active cooperation is the strongest point in improving security measures at different places.

As per Tsakanikas and Dagiuklas (2018) modern video surveillance systems have made this evolution from the primitive state of video acquiring tools to the intelligent systems that can perform complex actions like object detection, tracking, recognition, and re-identification. Integration of cloud technologies as well as advanced algorithms for image enhancement makes these systems not only dynamic but also advanced.

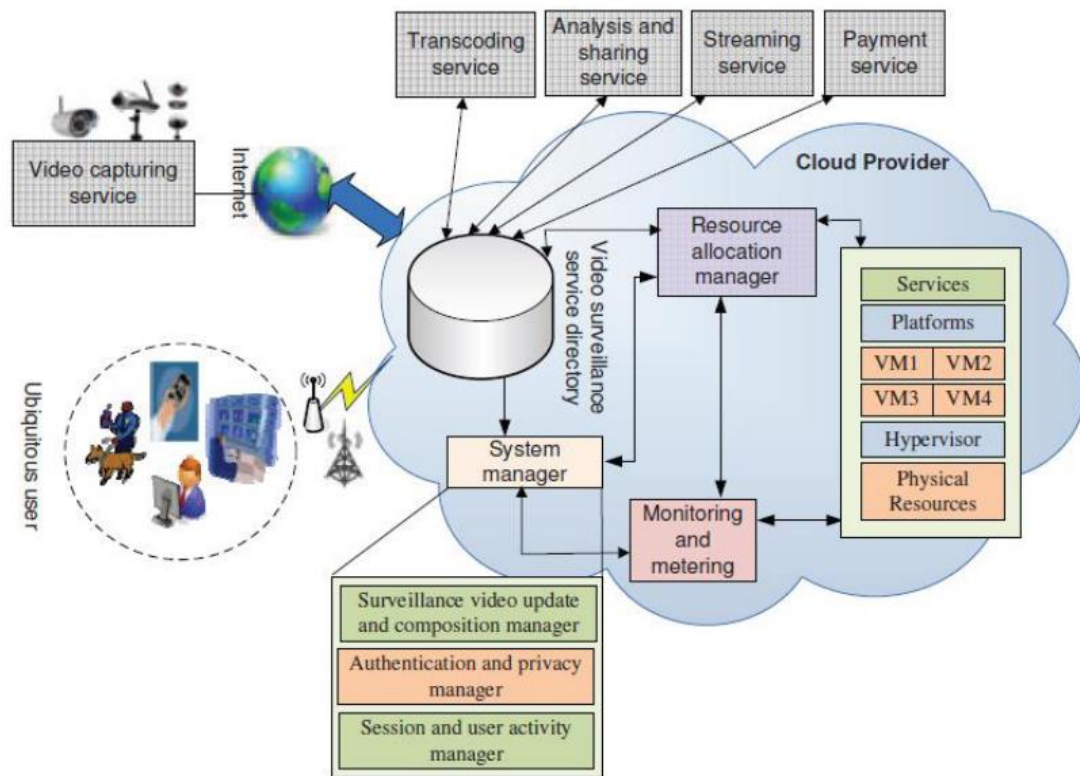


Figure 2: Integration of surveillance with cloud-based infrastructure (Tsakanikas and Dagiuklas 2018)

The move to the multifunction systems is a consequence of the failure of the single-function systems that lack a comprehensive security coverage. The merit of implementing alarms with visual displays is that they combine detection capability with identification or verification mechanisms. The alarm systems act as an immediate deterrent as well as a notification for any unauthorized activity, while the cameras allow you to monitor, identify and verify the nature of the threat in real time (Karanja, 2013; Sanjay Satam & El-Ocla, 2022). This double-pronged strategy promotes the overall security state by offering both preventive and inquisitive tools.

Notably, the use of artificial intelligence and machine learning algorithms in multipurpose security systems has resulted in a substantial improvement in their efficiency. These technologies have significantly improved their effectiveness through higher accuracy of threat detection, reduction of false alarms, and faster response times. Smart video analytics can

recognize between normal activity and suspected incidents, providing a more effective and focusing response of security (Tsakanikas & Dagiuklas, 2018).

Cloud integration is yet another dimension in the process of multipurpose security systems. Through the application of cloud computing, surveillance systems will be more scalable, data management and accessibility will be more efficient. Maiti and Sivanesan (2012) assert that home automation systems integration with security components is very essential, with digital cameras and sensors to monitor and alert homeowners when intrusion is attempted, reducing potential damage if burglary happens. This study highlights a cloud-linked and ad-hoc wireless home automation system that can be applied with a smart intrusion detection approach and thwarting of burglary cases. This algorithm described by the author includes the infrared cameras as well as the intelligent nodes which can detect intrusion and reports to location aware cloud service. If some activity is suspicious like some entry, the system would send you an SMS message and put into a position to identify the problem through any internet-connected device by accessing a website designed and developed by the cloud service provider. The system in addition strengthens the residents with their ability to secretly inform their neighbors via the same home automation system, turn on alarm sounds, or even contact the police directly. Hence, this study proves that cloud technology is one of the most vital tools to boost the efficiency of home automation systems to resist and defeat burglary attempts.

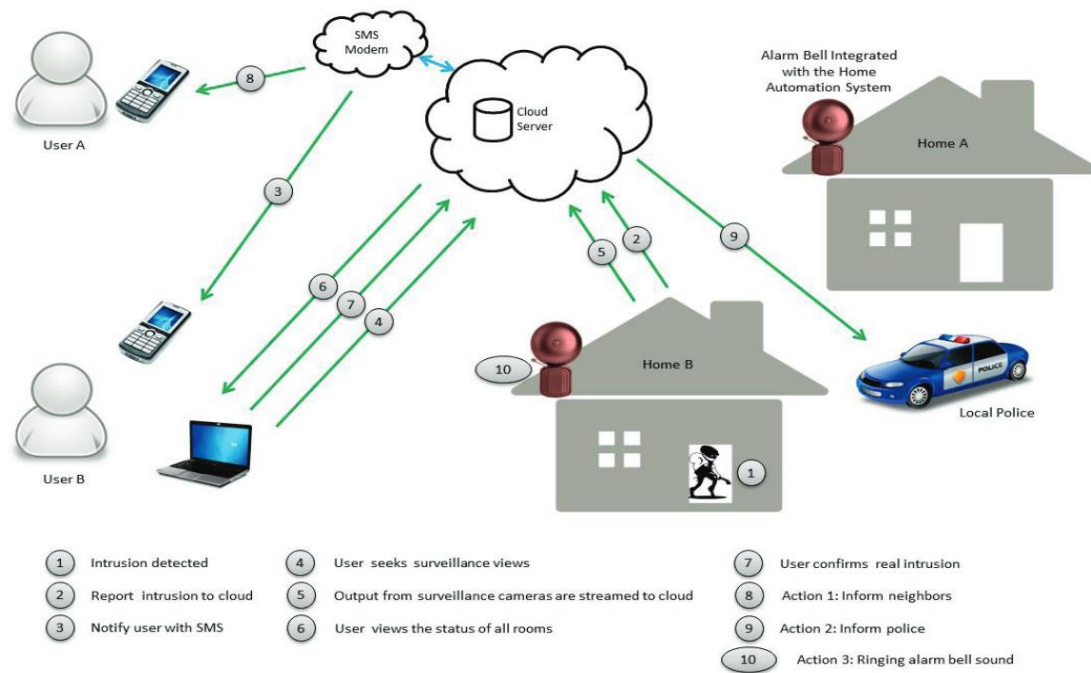


Figure 3: Intrusion event notification process using multipurpose security system (Maiti and Sivanesan 2012)

Therefore, this demonstrates the market's shift towards integrated security systems that are both audible and visual, employing technological innovations to maximize security. These systems provide a multi-dimensional approach to security, taking both the immediacy and the investigation into consideration. The future innovations especially in the domains of artificial intelligence, cloud computing, and data analytics are going to contribute to the improvement and effectiveness of multipurposed security systems.

User Interaction and Accessibility

The incorporation of multifunctional security systems had witnessed a tremendous advance in usability and accessibility. This approach, leveraging IoT-based devices, constitutes a fundamentally new method of security implementation and management for different types of domains, such as residential and commercial.

One of the key elements of the systems is the importance of easy-to-use interfaces that allow users to monitor, control and communicate with the security system. For instance, the mentioned work of Alsufyani et al. (2023) propose several applications in security systems that

are based on IoT. They point at web pages as a way of controlling security components, such as cameras, alarms, and door locks, remotely. This approach yields a combination of simple user experiences and excellent security measures accessibility, making it feasible for homeowners to manage their security systems all around the universe through internet connectivity.

Moreover, adaptability and scalability of those systems also influence the accessibility. The IoT technology can very easily add or remove new sensors and devices into the security system without any extensive overhauls and hence accommodating dynamic nature of the security requirements over time. The possible integration of smart devices into existing home or commercial networks via standard communication protocols and networks such as Wi-Fi eliminates the need for complex installation and upkeep processes (Alsufyani et al. 2023).

However, the integration of advanced authentication and authorization methods by these systems have solved the issues of security and privacy efficiently. According to Bowers (2013), the introduction of fingerprinting technology onto multipurpose security systems leads to customized access controls. By implementing this, it is guaranteed that system integrations or modifications are solely done by authorized personnel. These measures not only give the system a stronger security framework but also assure users about their data protection and the management of the security parameters.

Thus, the development of multipurpose security systems into complex, IoT-based solutions enhanced interaction and availability of end users. Through user interface design, scalability solutions and advanced authentication tools the systems provide an easy and secure way of managing security programs. Furthermore, with the progress of technology, user interaction and system accessibility are expected to be developed even further, resulting in more advanced security measures becoming available to a wider audience.

Gaps

The most important gap found in the literature about multipurpose security systems was the absence of holistic studies on their effectiveness and user satisfaction. There is a lack of research in the area of security system technologies that explores users' perceptions of the systems' effectiveness and satisfaction. The comprehension of user satisfaction is essential as it

affects directly the tendency of people to accept and continue using the systems. If users find the system too difficult to learn, with poor navigation, or the system is unreliable, they will have dissatisfaction; hence, they might end up disengaging, or even abandoning the system, which compromises their security in the end. Additionally, monitoring of user satisfaction will allow one to have an overview of the areas, where the multipurpose security systems need to be improved. It is also worth noting that feedback from users on the interface can help enhance usability by adjusting the design so that it is accessible to more individuals, such as those with less technological awareness or disabilities. Therefore, this study was conducted to resolve this insufficiency in the research field.

Overall, current research so far has provided an adequate base for the comprehension of multipurpose security systems that include alarms and displays. Consequently, it exposes what needs to be achieved and calls for sustained research efforts in the domains of system effectiveness, user interaction, integration capabilities, and security technologies adjustment to the next wave of threats. This literature review provides groundwork for the current research project which shall attempt correcting the shortcomings, offering new insights into development and implementation of such security systems.

Delivery Mode

As the location and preference of the target population were heterogeneous, the survey interview was conducted remotely over Zoom. Through this method, participants were able to contribute to the research regardless of their location and time, minimizing transportation time and scheduling conflicts. Furthermore, online delivery permitted the set-up of a diverse participant pool, including people from different locations, vocations, and societal groups, thereby contributing to increase the dataset with multiple perspectives on the security systems under evaluation (Oates et al. 2022).

Initially, potential participants were recruited through email or social media, and given brief information about the research, its objectives, and what they would be required to do. The ones who agreed to take part were followed up by a mail, and the mail contained a digital

consent form and detailed information about how to access the survey or interview platform. As for the quantitative surveys, the participants were sent a link to the survey, which was hosted on user-friendly platforms such as Google Forms or SurveyMonkey and included information about the survey completion deadlines and tips how to manage the surveys. Qualitative interview participants were provided with an online scheduling tool, where they were asked to schedule their sessions and provided with the Zoom meeting link and instructions on joining the interview. Live interviews were carried out in strict adherence to the schedule. Researchers ensured a setting conducive for open discussions, guided by a semi-structured format, while also allowing participants to express themselves creatively.

Immediately after the interview, the participants of the study were sent courtesy email recipients who expressed their respect for their contribution to the research and reiterated their rights, namely the data withdrawal possibilities. The process of security and privacy of data was essential, and all digital platforms complied with data protection regulations, thus keeping personal information as well as responses secure and strictly accessible only by the research team. Consequently, the research team was able to maintain the integrity of the study while creating a participant-friendly engagement process.

Sample Selection

The survey sought to involve a purposively chosen sample of present users of multi-purpose security systems, security experts, and employees of companies that manufacture or sell these systems. This directional or strategic sampling technique was purposely and specifically focused on identifying people who had particular experiences, knowledge or insights that were crucial to have an in-depth understanding of the security systems' efficiency. A sample population size of 50 participants was selected. The aim was to guarantee that the sample included a wide range of viewpoints, by including participants from diverse demographic backgrounds, different types of experience, and professional milieu. Such diversity has been significant in obtaining a multifaceted perception of the system's functioning, as well as users' acceptance by different groups.

Questionnaire Development

While it was a very meticulous process, the designing of the questionnaire was based on an in-depth review of the pertinent literature and consultations with security system experts. Thus, this preparatory work was essential for achieving a balance between the completeness of a questionnaire and its objectives.

The questionnaire has covered different aspects of the security systems, including their usability, user satisfaction, reliability, and the impacts of alarm and display features on security outcomes in general.

In designing the questionnaire special importance was given to understanding questions correctly and to avoid ambiguity, leading questions, and any bias that can affect the responses. The goal was to inspire truthful, genuine responses that accurately represented the participants' thoughts and feelings.

Data Analysis Techniques

The study employed both quantitative and qualitative data analysis techniques to interpret the survey interview results comprehensively.

Quantitative Analysis: Descriptive statistics were used to analyze closed-ended questions, providing insights into trends, patterns, and general attitudes towards the security systems.

Qualitative Analysis: Questionnaire was analysed by using thematic analysis for the open-ended questions. This qualitative approach was simply indispensable in the reduction of rich tapestry of narratives from the participants into themes and subtopics that eloquently captured their sentiments and perceptions. The process included several main steps:

1. **Initial Coding:** Responses were scrutinized carefully, and segments of text, which carried concepts conveying the idea of user experience, effectiveness, and possible improvements of the system, were assigned codes.

2. Theme Development: Codes were brought under potential themes that encapsulated the participants' narratives. The recurring process encompassed merging, subdividing, or redefining of initial codes and themes in a way that was closer to the data.
3. Refinement and Naming: Themes were crafted and evaluated to make sure that they fit a uniform scheme and mirror the dataset truthfully. Every theme was assigned a vivid title that highlighted the central idea it expressed.

The objective of thematic analysis was to unveil deeper level understanding of users' interactions with security systems, their effectiveness in real world and how they can become more useful by adding some advantages. This qualitative exploration was really necessary to understand the subjective features of using security systems. This holistic data analysis strategy enabled the study to not only track broad user experiences and attitudes but also get into the depth of personal narratives, thus giving us a solid base for the evidence-based advice for system improvement and future study directions.

Ethical Considerations

Ethics were key concerns in carrying out research, more so when humans were the participants, as it is the case with survey interviews to assess the effectiveness of multipurpose security systems with both alarm and display features. Ethical conduct safeguarded the rights of participants, the validity of the research and the reliability of its outcome. The following explores these in further detail:

Informed Consent

Informed consent is the cornerstone of every ethical study. Participants received information on the study's purpose, the procedures, the types of questions asked and any potential risks or fear of discomfort that they might experience. This technique would guarantee that the subjects know what they are agreeing to and made a conscious choice to participate.

1. Clarity and Comprehensiveness: Information was presented in a way that made it simple to understand and help the participants come up with effective actions that could help in addressing the issue.

2. **Voluntary Participation:** The primary purpose was clarifying the stand that the participants could refuse or withdraw from the study at any time, and it would not affect interpretation of the results.

Confidentiality

Preserving the anonymity of the data of the participants was essential for the developing of trust and ethics. This part was dedicated to protecting personal data and responses during and after the research process.

1. **Anonymization of Data:** In order to maintain anonymity of the participants the original data was partially encrypted and identifiers were removed from the dataset.
2. **Secure Data Storage:** Digital recordings, transcripts, and consent forms were collected and were protected from unauthorized access.
3. **Usage of Data:** Participants' information was used only for the research purposes. Beyond the use of the data provided during the research, we acquired an additional consent from the participants for any possible secondary use of the data.

Transparency and Integrity

Ensuring that transparency and integrity throughout the research process was imperative for the credibility of the study and its results. In pursuit of this commitment, the research study was designed, conducted, and documented accordingly.

1. **Clear Methodologies:** The research methodology was completely described, including data collection and analytic techniques, in any papers or presentations that were published, which allowed for scrutiny and replication by other researchers.
2. **Acknowledgment of Limitations:** In the research, the limits or the possible biases in the design or implementation of the study were openly admitted which gave a balanced and transparent outlook of the findings.
3. **Disclosure of Conflicts of Interest:** The potential conflicts of interest that could impact the research outcomes were declared from the beginning. That was by highlighting their

financial interests, affiliations or personal beliefs which would impact the research in question.

These ethical practices not only secured participants but also increased the quality and trustworthiness of the research findings, bringing useful intelligence to the effectiveness of multipurpose security systems with alarm and display features.

Conclusion

On the whole, this project has made a complete examination of the user efficiency and satisfaction of the multipurpose security systems. Through a mixed-methods approach that combines both quantitative surveys and qualitative interviews, this research work has therefore attempted to go a step further, by providing a comprehensive look at the various aspects of these security systems. However, the effects of this project go far beyond the simple assessment of existing security systems. Furthermore, the importance of continuous improving is highlighted by the fact that systematic monitoring, evaluation, and adaptation to security infrastructure and practices are the key to success on a long-term basis. Thus, the study's implications are extensive, indicating that the future of multipurpose security may be found in the smooth assimilation of technology with consumer requirements. It is recommended that producers and developers give careful consideration to the user experience while designing their goods, so that these systems are not only highly technologically sophisticated but also easily navigable and easy to use.

As far as additional research, some avenues can be considered for extensive evaluation. Further research could be directed toward the carrying out of longitudinal evaluations to evaluate on the long-term effectiveness and sustainability of multipurpose security systems. Moreover, comparative research on different types of security systems or on the successful implementation of certain security features and technologies within multipurpose systems may be useful. Deeper insights may be obtained by looking into long-term user satisfaction and how ongoing technical

improvements affect system usage. Furthermore, investigating how to incorporate cutting-edge technology like machine learning and artificial intelligence into these systems may open up new avenues for improving security.

In general, this project reflected the efficacy of multipurpose security systems with alarms and displays, which indicated the beneficial points for the stakeholders which are involved in the security infrastructure and practice. Through the integration of empirical materials, stakeholder viewpoints, and theoretical frameworks, this research generates knowledge and serves as a foundation for further studies.

References

- Alsufyani, A., Rana, O., & Perera, C. (2023). *Knowledge-based cyber physical security at smart home: a review*. Cardiff University, UK
- Anitha, A., & Kalra, S. (2016). A Cyber defence using artificial home automation system using IoT. *International Journal of Pharmacy and Technology*, 8, 25358-64.
- Bowers, D. M. (2013). *Access control and personal identification systems*. Butterworth-Heinemann.
- Çavaş, M., & Ahmad, M. B. (2019). 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.
- Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: a survey. *Wireless Personal Communications*, 115(2), 1667-1693.
- Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc."

- Govinda, K., Prasad, S. K., & Susheel, S. R. (2014). Intrusion detection system for smart home using laser rays. *International journal for scientific research & Development*, 2(3), 176-178.
- Karanja, M. K. (2013). *Mobile Video streaming Surveillance System With SMS Alert* (Doctoral dissertation, University of Nairobi).
- Karri, V., & Lim, J. D. (2005, November). Method and Device to Communicate via SMS after a Security Intrusion. In *1st international conference on sensing technology, Palmerston North, New Zealand* (pp. 21-23).
- Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology*, 19(2), 135-149.
- Maiti, A., & Sivanesan, S. (2012, April). Cloud controlled intrusion detection and burglary prevention stratagems in home automation systems. In *2012 2nd Baltic Congress on Future Internet Communications* (pp. 182-186). IEEE.
- Oates, M., Crichton, K., Cranor, L., Budwig, S., Weston, E. J., Bernagozzi, B. M., & Pagaduan, J. (2022). Audio, video, chat, email, or survey: How much does online interview mode matter? *PloS one*, 17(2), e0263876.
- Sanjay Satam, S., & El-Ocla, H. (2022). Home security system using wireless sensors network. *Wireless Personal Communications*, 125(2), 1185-1201.
- Tsakanikas, V., & Dagiuklas, T. (2018). Video surveillance systems-current status and future trends. *Computers & Electrical Engineering*, 70, 736-753.
- Yadav, A., Thaker, N., Makwana, D., Waingankar, N., & Upadhyay, P. (2021, May). Intruder Detection System: A Literature Review. In *Proceedings of the 4th International Conference on Advances in Science & Technology (ICAST2021)*.
- Zurko, M. E. (2005, December). User-centered security: Stepping up to the grand challenge. In *21st Annual Computer Security Applications Conference (ACSAC'05)* (pp. 14-pp). IEEE.