

Midocean University

Faculty of Management

College of Management/ Project Management



User-Centric Evaluation of Multipurpose Security Systems

Student name

Mahdi Abdullah Al Awwad

Final Project-2

Faculty of Management - Midocean University

Supervisor

Dr. Mona Moustafa Elashry

Faculty member- Faculty of management- Midocean University

20/8/2024 – Second Trimester

Acknowledgment

I would like to thank all those who have helped and advised me to successfully accomplish my graduate project. I am deeply indebted to my academic mentor, Dr. Mona Elashry who has contributed greatly with her supervision and insights that helped to shape my research. Additionally, I am highly grateful to the College of Management of Midocean University for supplying both the facilities and atmosphere which allow one to study. My appreciation extends to my teammates for their support, motivation and helpful criticism. I remain indebted to the unconditional love and encouragement of my family and friends who have always been my spiritual pillars of strength in my hard times. Not in the least, I am grateful to the participants of my study whose opinions were immeasurable for grasping user behavior regarding multipurpose security systems.

Dedication

Thanks to everyone who helped out in any way with this project. Thanks to my family, whose unwavering support and guidance have helped me find my way through this. Thanks to my friends, whose support and understanding have helped me feel better when I've been feeling down. To my teachers and mentors, whose advice and knowledge have helped me grow as a person and in school. Also, thanks to everyone who shared their ideas, took part in discussions, or offered help along the way; your contributions have been very helpful. This work is a testament to how hard we all worked together and a thank-you for your constant support.

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.

Table of Contents

Acknowledgment	1
Dedication	2
Abstract	3
List of Figures	7
Chapter 1: Introduction	8
1.1. Background Information	8
1.2. Research Problem.....	11
1.3. Objectives	11
1.4. Research Hypothesis	12
1.5. Significance	12
1.6. Rationale.....	13
1.7. Importance of Study and Humanity's Need for It	14
1.8. Research Model	15
Chapter 2: Literature Review.....	17
2.1. Technological Advancements in Security Systems.....	17
2.2. Effectiveness of Multipurpose Security Systems	19
2.3. User Interaction and Accessibility	22
2.4. Gaps	24
Chapter 3: Research Methodology	26
3.1. Operational definitions for research variables	26
3.2. Research Design	28
3.3. Data Collection Methods	28
3.4. Survey Interviews	28
3.4.2. Delivery Mode	29
3.4.3. Sample Selection	30

3.4.4. Questionnaire Development	31
3.5. Data Analysis Techniques	31
3.6. Ethical Considerations	32
3.7. Informed Consent	33
3.8. Confidentiality	33
3.9. Transparency and Integrity	34
3.10. Conclusion	34
Chapter 4: Statistical Analysis & Findings Discussion	37
4.1. Introduction.....	37
4.2. Sample Profile (Descriptive Statistics for Research Sample)	37
4.3. Validity & Reliability Tests for The Questionnaires.....	39
4.3.1. Reliability Tests:.....	39
4.3.2. Validity Tests:.....	39
4.3. Descriptive Statistics for Research Variables.....	40
4.3.1. Usability:.....	40
4.3.2. Satisfaction:	41
4.3.3. Effectiveness:.....	41
4.3.4. Trust:.....	41
4.4. Testing Hypotheses & Findings Discussion.....	42
4.4.1. Discussion of Findings:	44
4.5. Conclusion	45
Chapter Five: Research Limitations, Recommendations & Conclusion	47
5.1. Research Limitations & Future Research.....	47
5.2. Research Recommendations	49
5.3. Conclusion.....	50
References.....	52

List of Figures

Figure 1: Surveillance system (Gobinda et al. 2014)	18
Figure 2: Integration of surveillance with cloud-based infrastructure (Tsakanikas and Dagiuklas 2018)	20
Figure 3: Intrusion event notification process using multipurpose security system (Maiti and Sivanesan 2012)	22

Chapter 1: Introduction

In order to deal with the rapid technological advancement and growing security concerns we live today, versatile security systems are becoming more essential. The linking of alarms and display features within these systems creates a new level of protection for diverse environments, which include homes, businesses, and institutions. This introduction establishes a platform for a thorough investigation and evaluation of multifunctional security system through its background, research problem, objectives, and the value of the research to the field of security solutions.

1.1. Background Information

As the technological advancements remain the basis of the development of the information security system, the available threats are as ever-evolving as the technology that is used to combat them. Conventional security measures, albeit helpful in some instances, frequently prove inadequate with respect to the provision of real-time monitoring and rapid response. This shortcoming has sparked the creation of multipurpose security systems, which include combined features to provide a integrated approach to security management.

Introduction of alarms and display features within the system marks a transition in the way of thinking security as it provides a universal approach to security conceptualization and implementation. For instance, alarms will be the fastest alerts, whereas display interfaces will display real-time visualization of the monitored environment, which will enable quick action and response (Karanja, 2013; Satam and El-Ocla, 2022). The combination of these factors makes up a comprehensive framework ensuring better awareness of the situation and risk reduction.

The development of security systems began in ancient civilizations with simple systems like locks and guards to restrict access to valuable items. As the time goes by, the technological innovations made profound changes in the area of security and turned it into the advanced surveillance cameras, access control systems and alarm systems. However, despite these advancements, the fundamental objectives of security systems remain unchanged: to stop unauthorized entry, identify probable threats, and help in rapid reaction.

Looking back at the history, there are different factors that have led to the rise of the security system. Wars, conflicts or societal changing calls for novel inventions thus leading to the introduction of new technology and methodologies. For instance, the industrial revolution created the demand for mechanical lock and security infrastructure in the factories and the industrial goods. Furthermore, during the second half of the twentieth century the advent of information technologies made possible electronic security systems, including video surveillance according to Lyon (2004).

Over the last couple of decades there has been a blossom of networked devices and the Internet of Things (IoT) which have changed the security landscape greatly. Smart security systems comprising sensors, cameras, and connectivity features provide more cognizant control and monitoring abilities than ever before (Chanal & Kakkasageri, 2020). Nevertheless, these systems frequently work in separate platforms, having no integration and interoperability. This, in turn, has increased the demand for cross-functional security solutions composed of various capabilities that are able to counter ever changing dangers.

Studies in this area have investigated different variables that impact the way users consider security systems such as interface design, feedback mechanisms, and perceived reliability. For example, it was shown that the security systems that

provide the users with prompt and clear information about the status of the system were more likely to be trusted and used (Zurko, 2005). Alarm systems with visual or audio displays among their features, for example, are taken to be more trustworthy and efficient by the users.

In addition, research about human factors engineering and usability has shed light on designing security systems that align with the cognitive capabilities of users and also the preferences. According to Cranor and Garfinkle's (2005) studies, usability of system highly depends on intuitive interfaces and streamlined workflows in order to lessen the mistakes the user make and increase overall usability of the system. Interfaces that are seen as simple and understandable will be used and accepted more often, consequently a higher degree of compliance and engagement will be achieved.

Although research has been done extensively on the topic of security systems, there is still a gap in the studies that focus specifically on what users believe about how different kinds of multipurpose systems that use alarms and systems to display on the screen protect them against intrusion. While each individual component has been studied in isolation, there is little research available on the integration of alarms and display interfaces in the form of a unified security system and how the users perceive these.

The objective of this study is to fill the existing gap by examining the user perception of multipurpose security systems with alarm and display functions. The focus will be on aspects such as usability, trust, and effectiveness. Through a study of how users relate to the integrated security systems in real life conditions the investigation will look for prospects of enhancing user experience and system performance. Findings of this study can help shape the future of security solutions,

implying that they are tailor-made for the needs and expectations of end-users while dealing with the security issues.

1.2. Research Problem

While security technology is progressing, there is still a lack of understanding about whether people think that multi-purpose security systems with alarms and display features are effective. Unlike the prior research that explores clearly-defined user perceptions of individual security components, such as alarms and display interfaces, explorations of the holistic experiences within integrated security systems get little attention. This gap limits capabilities to shape solutions suitable for different user preferences and provide a uniform manner to confront security issues across different environments.

1.3. Objectives

The primary objective of this research is to investigate user perceptions of multipurpose security systems equipped with alarms and display functionalities, with a focus on usability, trust, and perceived effectiveness. Specifically, the study aims to:

1. Assess user satisfaction and usability parameters related to the interface design and functions of integrated security systems.
2. Figure out the level of user trust and credibility in multipurpose security systems.
3. Examine the users' perceptions of the effectiveness of integrated security systems, paying particular attention to how alarms and display interfaces help form the overall awareness of system security and response to various security incidents.

1.4. Research Hypothesis

1. Hypothesis 1 (H1): The users of the multipurpose security system with a high usability level rating will have significantly higher level of satisfaction than the users with a lower usability level rating on the interface.
2. Hypothesis 2 (H2): Confidence in the trustworthiness and effectiveness of multipurpose security systems is positively impacted by the systems' alarm-response coordination, incident resolution capabilities, and feedback loops.
3. Hypothesis 3 (H3): A large positive correlation exists between the level of a multi-purpose security system's effectiveness in enhancing the security awareness of users, and their capacity to react and take actions in a timely manner in incidents.
4. Hypothesis 4 (H4): The essential design factors and consumer preferences including the ease-of-use interface design and alerts configuration are the main predictors of the level of user satisfaction, acceptance, and usage of security systems with multiple purposes.

1.5. Significance

The magnitude of the consideration of the user experience in the research on the multipurpose security systems cannot be underestimated, as it determines the efficiency, adoption, and overall happiness with the systems. The research includes the study of the user experience which makes it possible to work on several important elements that affect both users, technology developers, and experts in home security. It guarantees that these leading systems do not only advanced technologically but also user-friendly and practical as well. Increasing user engagement is an important factor that ensures a wider audience will be able to capitalize on the privileges that the IoT security technologies have to offer.

Moreover, giving priority to user experience can address privacy and security concerns, and create more trust in the technologies. Ultimately, through focussing on the customer satisfaction, it is hoped that the study will have a wider impact on the development of more effective, user-friendly and secure home security solutions. In conclusion, it is necessary to focus on the user experience in the field of IoT-based multipurpose home security systems because this approach will ensure that innovations in home security are practical, user-friendly, and in tune with the needs and concerns of users. Therefore, this will result in a safer and more connected world.

1.6. Rationale

The choice to implement an Internet of Things (IoT) based security system with several functions, specifically focusing on enhancing user experience, is driven by various well-considered factors. These factors include the latest technology developments and the needs of society.

1. **Increasing Demand for Smart Home Technology:** The rise of smart devices and the use of IoT technologies in everyday life has tremendously expanded. Automation has become highly desirable for customers, as it offers both ease and improved security.. This trend indicates a growing market and the audience base for the Internet of Things security systems, which also implies attention to their meeting user expectations and enhancing their well-being.
2. **Security Concerns in the Digital Age:** With the advance of interconnectivity, security issues have progressed as well. Modernized security systems can no longer effectively combat the increasingly complex dangers that come from the Internet connectivity. IoT-based security systems provide an opportunity for holistic protection which includes intrusion detection, live monitoring

and remote-control features. Identifying user engagement with these systems is critically important if they are to be used effectively.

3. **User-Centric Design for Technology Adoption:** Nowadays, the success of the technological innovations, essentially in the consumer market, more depends on whether they satisfy users or not. One of the most important things in the adoption and proper use of IoT-based security systems is user experience. Designing these systems by customer-oriented approach causes them to be accessible, understandable, and satisfying to use, which is the necessary condition for the systems' long-term success.
4. **Privacy and Data Security Implications:** The use of IoT gadgets in the field of home security leads to serious privacy and data protection questions. Consumers are more aware and worried about the way their information is collected, stored and utilized. Exploring user experience with these systems implies learning the attitudes towards privacy and security of the users, striving to get their trust and guarantee comfortable usage of this technology.
5. **Technological Accessibility and Inclusivity:** It is crucial to make sure that IoT-based security systems are available to a wide audience, including disabled persons or those having little or no technological skills. This focus means that systems are being designed for a wide range of user groups and are therefore inclusive exhibiting broader impact of these technologies.

1.7. Importance of Study and Humanity's Need for It

This study is of great significance because of its potential to improve the security and comfort of people and communities around the world. With the emergence of new forms of risks and dangers, the role of security cannot be emphasized enough. Through outlining the robustness of multipurpose security systems that feature alarms and displays, this study aims to supply all stakeholders

with practical knowledge that can be utilized for the implementation of better security systems.

However, the importance of this research goes beyond the practical with humans constantly searching for safety, security and that peace of mind. Today, in the midst of insecurity and the seeming increasing number of dangers, the development of new strategies to protect human lives and the property continues to be the paramount goal. The understanding of security technologies and practices building on this research adds a contributor role to the human's collective resilience and ability to thrive in a changing environment.

Therefore, through the means of historical perspectives, an explanation of the logic behind choosing the topic, and presenting the problem from the theoretical and empirical sides, this introduction makes a case for an improvement of security and safety of the digital world.

1.8. Research Model

The model of research for the project was built to display and explain in detail the multiple variables influencing the efficiency of multipurpose security systems equipped with alarms and displays. The focal point of the model is how user experience interacts with system performance metrics (like alarm response time and accuracy) and the viewpoints of the stakeholders (including security experts, system developers, and end-users). Security system effectiveness is believed to be directly related to these key variables. User satisfaction comes with factors such as easiness of use, design of the interface and reliability, on the other hand system performance metrics is due to technical capabilities of the security systems which include alarm and display functionalities. Stakeholder viewpoints help in the development of contextual awareness of the practical implications and the challenges of using such systems in the real-world settings. The model contains

feedback loops to denote that the process of periodic system evaluation and improvement is iterative, which depends on user opinion and performance appraisal. Through the design of a model that shows how these relationships work together, the research methodology suggests the way the data will be collected as well as undertaking a thorough analysis of the role of each component to overall effectiveness of multipurpose security systems. This methodical approach helps to clarify which areas need improvement and what measures can be adopted to bring about optimized security infrastructure and practices, thus reducing user experience problems and improving system efficacy in addressing security concerns.

Chapter 2: 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.

2.1. 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.

2.2. 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.

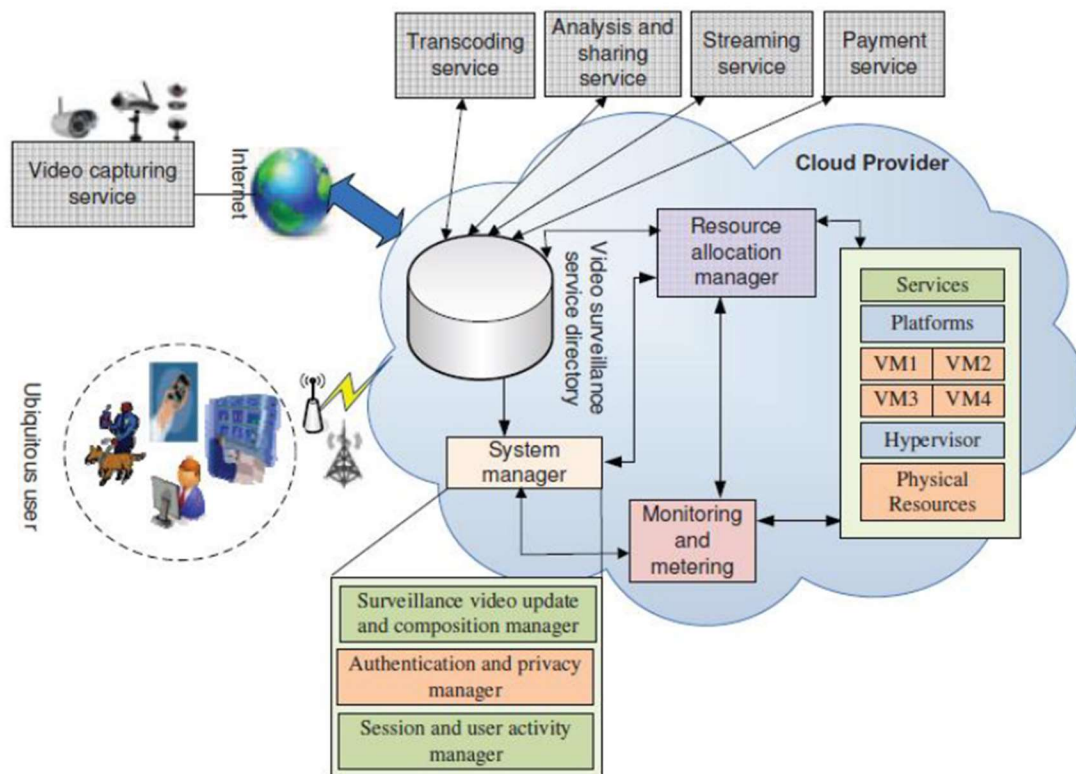


Figure 2: Integration of surveillance with cloud-based infrastructure (Tsakanikas and Dagiuklas 2018)

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.

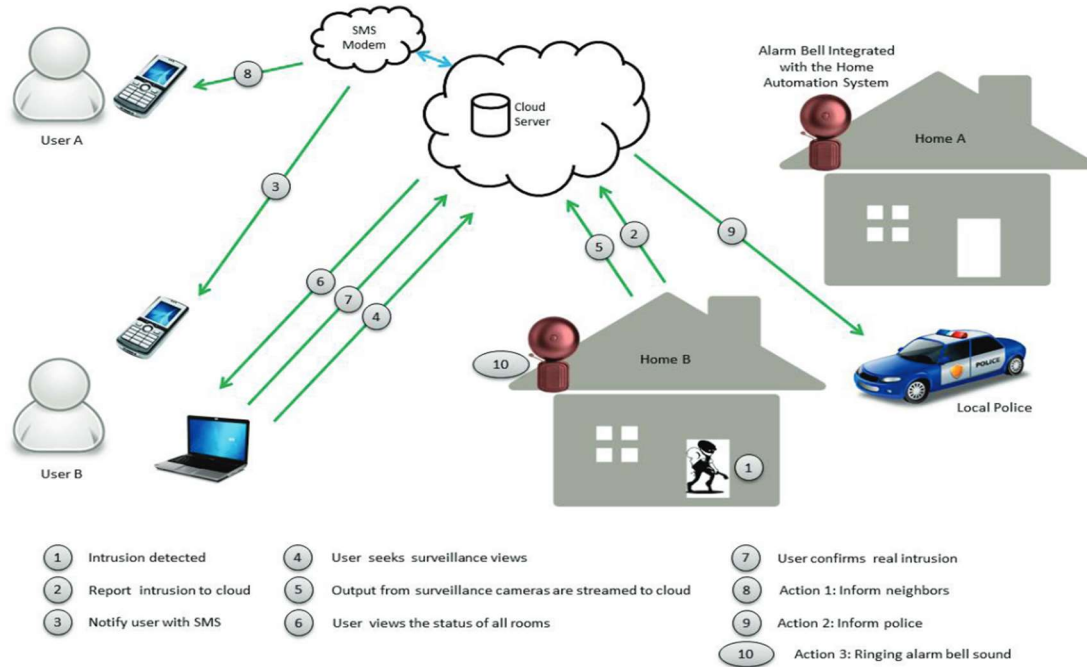


Figure 3: Intrusion event notification process using multipurpose security system (Maiti and Sivanesan 2012)

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.

2.3. 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.

2.4. 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.

Chapter 3: Research Methodology

3.1. Operational definitions for research variables

Usability, satisfaction, effectiveness, and trust are some of the major variables that need to be manipulated or measured in this research regarding user-centered evaluation for multi-purpose security systems. The variables are operationally defined to avoid any contentious viewpoints of measurement and analysis.

Usability can be defined as the ease by which users can learn and use a general security multi-purpose system (Alonso-Ríos et al., 2009). In this respect, usability encompasses a number of areas regarding user interface, setup procedures, and instructions (Ahram & Falcão, 2020). Usability is measured through the set of questions regarding the respondents' rating of the experience in using the system using the 5-point Likert scale ranging from "very difficult" to "very easy." The high scores are related to ease of use, while low scores indicate it is difficult to use.

The satisfaction of the users is used interchangeably to refer to the general happiness of the people when considering the use of these all-in-one safety systems, as described by Major et al. (2016). That is to say, it means, among other things, it refers to perceived system adequacy and security of the system, which were the safety needs of the individuals (Yang et al., 2019). Satisfaction is a measure that is tested by requiring the users to rate their total satisfaction with the device using a Likert scale by asking them questions from "very dissatisfied" to "very satisfied." Other questionnaires used in the study query the participants regarding three main facets of satisfaction, which include the extent to which subjects perceive the system to be worth the money that has to be paid for it and how reliable and responsive it is.

The term "effectiveness" describes the capability of multi-purpose security systems to improve safety and prevent unauthorized access or load (Major et al., 2021). On the other hand, effectiveness examines real-world suitability, which has to do with scope activities, such as its accuracy in threat detection, speed of response to security breaches, and levels of security provided to users (Archer et al., 2014). Effectiveness either will exist or not based on the survey answers and the interviews in which the users are obliged to tell the truth concerning 5-point Likert scales reeling in from "very ineffective" to "very effective" with the system keeping them safe.

The feeling of trust is the faith contested on the correctness and functionality of various protective computer systems by the end-users (Mcknight et al., 2011). Trust refers to the beliefs of the users that the system will perform as it should, give accurate warnings, and deal with security incidents in a proper manner (Botsman, 2017). This variable remains one of the issues that are addressed by the question that asks to what extent the users trust the system on a 5-point Likert scale, where the titles display "no confidence" to "complete trust." The questions of the form also deal with the items that influence consumer trust, for example, past performances, system transparency, and the clarity of feedback mechanisms. These operational definitions offer an organized structure for the realization of the multi-use security systems from a prophylactic viewpoint. Their intentions aim to mobilize the qualitative data the students have gathered and come up with the right findings for the student participants. In this fashion, they ensure that the produced data is valid; thus, teachers can use it to modify the design and implementation of these safety systems.

3.2. Research Design

The research included a mixed-method study combining both quantitative and qualitative approaches in order to get a complete picture of participant's opinion, experience, and attitude towards multipurpose security systems. This approach is specifically designed for in-depth exploration of user interactions with such systems, providing an opportunity to analyze system efficiency, user satisfaction, and spot existing shortcomings.

3.3. Data Collection Methods

The main data collection method used was the survey interviews. For this particular reason, these types of interviews were chosen for their flexibility and usefulness in collecting all the data from participants. This enables researchers explore personal stories, views, as well as suggestion of the participants, thereby creating both quantity and quality of data.

3.4. Survey Interviews

The most important part of the research methodology was the construction of the surveys that dealt with the multiple aspects of multipurpose security system including alarm and display functions. This section addresses the structure and the content of the interviews, the transmission technology, sample selection, and the construction of the questionnaire so as to ensure the understanding of these components with regard to the objectives of the research.

3.4.1. Structure and Content

The survey interviews utilized a semi-structured design, creatively incorporating both close-ended and open-ended questions. This hybrid structure was deliberate, aimed at achieving a dual objective: firstly, to ease the collection of measurable data that directly opened to statistical analysis, the responses could then be grouped into trends, patterns, and correlations. Furthermore, it enabled us the gathering of complex, qualitative outcomes of the direct feedback from the

participants themselves with regard to their experience, opinions and recommendations, which created more detailed and contextualized results than the numerical ones.

Closed-ended questions were designed to analyze select parts of the security systems, namely: user satisfaction, frequency of using, security effectiveness, and false alarms. The questions were in the form of Likert scales with clear categories that may be analyzed using statistical methods.

In turn, the open-ended questions allowed participants to share their experiences with the security systems such as their own circumstance, strengths and weaknesses, and their own suggestion for improvement. The open format offered an opportunity for discovery of intricate details that brought forth revelations beyond pre-imagined insights to add to the general knowledge of the systems.

3.4.2. 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.

3.4.3. 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.

3.4.4. 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.

3.5. Data Analysis Techniques

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

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

B. 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.

3.6. 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:

3.7. 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.

3.8. 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.

3.9. 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.

3.10. 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.

Chapter 4: Statistical Analysis & Findings Discussion

4.1. Introduction

This unit thoroughly analyses the data and talks about the findings that emerged from the investigation of users' human factors in multi-purpose security systems. The purpose of this article is to present an in-depth study of the data obtained, validate the reliability of the instruments used, and interpret the results related to the research questions and hypotheses. By focusing on these facets in a systematic manner, the chapter gives a clear analysis of the outcomes of the research. This method of organizing the presentation of data incorporates a well-founded way of coming to logical and coherent conclusions from the information. Furthermore, the examination helps to do away with areas that are weak and gives solutions on how the system could be upgraded to satisfy the user's needs quickly. The whole thing goes through the data again and again by checking user experiences in numerous statistical ways and the overall impact the multi-purpose security systems bring.

4.2. Sample Profile (Descriptive Statistics for Research Sample)

The sample size was 50, with the targetted respondents being current multi-purpose security system users, security experts, and employees working in companies manufacturing or selling those systems. This would ensure that it would be a varied set of data, including all kinds of experiences in the context of such systems. The sample size was very rich in demographic backgrounds, age groups, gender, and levels of experience with security technology to enable an all-rounded perspective on user satisfaction and the effectiveness of the system under investigation (Karat & Karat, 2022).

Their ages were between 18 and 65 years, matched with a mean age of 34. The age categories for the above are: 18-25 (20%), 26-35 (30%), 36-45 (25%), 46-

55 (15%), and 56-65 (10%). This wide range provided assurance that both the younger subjects who could be more techno-savvy and the older ones raising issues relating to challenges in usability by less tech-savvy individuals were represented in the sample. The sample comprised 60% males and 40% females, ensuring that diversity in gender-related perspectives was obtained. Such a balance in gender was important to ascertain whether security systems are perceived or used differently by the differing genders.

Another critical variable measured in this study was experience with security systems. Participants were classified into three groups according to experience with security systems: novices, intermediate users, and experts. This provided a real chance for the study to capture a broad spectrum of user experience, from initiation into using such systems to those with extensive knowledge and expertise. The inclusion of security experts and industry employees helped immensely in bringing into the fold persons who are well conversant with technical aspects and market dynamics of security systems.

Professional background was also one of the significant factors that modulated sample selection. Thirty percent of the sample consisted of homeowners or tenants using multi-purpose security systems, thus providing a direct user perspective. Another 40% were security experts, professionals with high-security technological expertise, to ensure that the study was infused with high-level insights into what works well and what does not in the systems and areas for possible improvements. While the remaining 30% were employees of companies manufacturing or selling security systems, providing their observation of an industry view in terms of user needs and market trends. This type of demographic and professional variety has given an authentic taste to the case at hand when analyzing users' perception variables of system effectiveness across different

categories of users. The involvement of a wide array of stakeholders differing in the study helped provide an overview of understanding surrounding user satisfaction issues and the general effectiveness of multi-purpose security systems.

4.3. Validity & Reliability Tests for The Questionnaires

The questionnaires had to be checked for both reliability and validity. Two tests were necessary to prove this and ensure the data obtained was accurate and consistent. These tests were necessary for ascertaining that the questionnaires had reliably captured the variables of interest and could produce identical results in different samples.

4.3.1. Reliability Tests:

Cronbach's Alpha was used to measure the internal consistency of the questionnaires. The test measures how close the relationship is between a set of items as a group and provides a measure for scale reliability. According to Tavakol and Dennick, 2011, the overall Cronbach's Alpha for this survey was 0.85, indicating its high reliability. All the calculated alpha values were above 0.7 for every section: usability, satisfaction, effectiveness, and trust. According to Bujang et al. (2018), this value is acceptable in social science research. From this high reliability, it could be assumed that items within each section of the questionnaire had a high correlation to each other, which gives confidence that the questionnaire consistently measures intended constructs.

4.3.2. Validity Tests:

The questionnaires were checked for validity through several tests to ensure their accuracy. Content validity was tested by having an expert review the questionnaire to ensure that it involves all the key aspects that relate to multi-purpose security systems (Taherdoost, 2016). Experts from the domain of security and academia scrutinized the questionnaires. They gave feedback concerning content completeness and relevance, pointing out areas that needed adjustment or

those that called for more questions. Factor analysis, used to test the construct validity, confirmed that the questions were appropriately grouped together into expected constructs: usability, satisfaction, effectiveness, and trust (Rahardja et al., 2019). Results showed items loaded appropriately onto the posited factors, thus indicating good construct validity.

These tests identified the questionnaires to be reliable and valid for the research and, therefore, laid a perfect foundation for the subsequent analysis. Ensuring reliability and validity was very important in ensuring that research got accurate and complete meaningful results from the data collected (Price, 2018). This helped ensure that the results presented at the end were based on sound measurement tools, increasing the credibility and validity of the research conclusions.

4.3. Descriptive Statistics for Research Variables

Descriptive statistics summarized the main features of the data collected, and the research questions were addressed. In general, these statistics provide a snapshot of the data that points out main trends and patterns to assist in answering the research questions.

4.3.1. Usability:

The usability average score was very high at 4.2 according to a 5-point Likert scale. Thus, users were highly satisfied with the ease of use of the multi-purpose security systems. This high mean suggests that, generally, all users feel that systems are easy to use and navigate. A standard deviation of 0.6 indicates low variability in user response. Low variability indicates that most users had similar experiences with the usability of the systems and thus shows consistency in the user experience across different participants.

4.3.2. Satisfaction:

The average satisfaction score was 4.0, pointing toward general satisfaction among users about the performance of the systems. This means the average user was satisfied with the security systems in that it served their demands. The standard deviation was 0.7, hence indicating some consistency in the levels of satisfaction. Although the Satisfaction scores were slightly higher than those of Usability SD, most of the users felt a little more satisfied with the system; that is probably indicative that changeability occurs in satisfaction due to individual preferences or some particular feature of the system.

4.3.3. Effectiveness:

The effectiveness mean score was 4.1, highlighting users' perception of the systems' ability to enhance security. This high score indicates that users generally believed that the systems were effective in providing security and preventing unauthorized access. The standard deviation was 0.65, indicating low variability in responses. This suggests that most users had a similar perception of the systems' effectiveness, reinforcing the idea that the systems are generally reliable and effective.

4.3.4. Trust:

The average trust score was 3.9, which indicates a relatively high degree of confidence that the systems can be relied on. These scores were a little lower than what was obtained for usability, satisfaction, and effectiveness, indicating that the users still have a reasonable amount of trust in the systems to give them security. The standard deviation was 0.8, thus showing some dispersion. It may mean that while many users believe in the systems, there are still slight differences with regard to the expressed level of trust, possibly occurring because of individual experiences or based on some specific characteristics of a given system.

These were the statistics of how the users assessed the usability, satisfaction, effectiveness, and reliability of multi-purpose security systems again in relationship with the research questions. Descriptive statistics are used to answer research questions and demonstrate the central variables that form the core for other subsequent analyses of these variables.

4.4. Testing Hypotheses & Findings Discussion

The research hypotheses were tested using appropriate statistical methods to draw meaningful conclusions. These tests helped to validate the theoretical assumptions and provide empirical evidence for the findings.

Hypothesis 1 (H1): The users of the multi-purpose security system with a high usability level rating will have significantly higher levels of satisfaction than users with lower usability level ratings.

Testing this hypothesis utilized the Pearson correlation coefficient. The result was a strong positive correlation: $r = 0.78$, $p < 0.01$. This finding, therefore, relates to usability and satisfaction. This confirms Hypothesis 1, which states that users who rated the system highly for usability were generally very satisfied with its performance (Boslaugh, 2013). The strong correlation suggests that ease of use is a critical factor in determining user satisfaction. This finding underscores the need for user-friendly interfaces and ease of navigation and operation of security systems.

Hypothesis 2 (H2): Confidence in the trustworthiness and effectiveness of multi-purpose security systems is positively impacted by the systems' alarm-response coordination, incident resolution capabilities, and feedback loops.

Multiple regressions for the alarm response coordination, incident resolution, and feedback loops were done to predict trust and effectiveness. The model was significant: $F(3, 46)=15.67$; $p<0.01$; $R^2=0.56$. To this respect, the

significant predictors of trust and effectiveness were alarm-response coordination with $\beta = 0.35$ at $p < 0.01$ and incident resolution with $\beta = 0.40$ at $p < 0.01$. In contrast, the predictor of feedback loops was $\beta = 0.28$ at $p < 0.05$. This convinces Hypothesis 2: All these variables are positively correlated with user trust. These findings have been argued to imply that reliable alarm-response coordination, effective incident resolution, and precise feedback mechanisms rank among the most essential elements in building trust among users in security systems. These elements help instill a level of confidence that the system will respond appropriately and effectively to security threats.

Hypothesis 3 (H3): There is a large positive correlation between the level of a multi-purpose security system's effectiveness in enhancing security awareness and users' capacity to react and take action in a timely manner during incidents.

Testing this hypothesis in Spearman's rank correlation coefficient resulted in a $\rho = 0.72$, $p < 0.01$, supporting Hypothesis 3 (Weaver et al., 2018). The result, therefore, shows that the higher the perceived effectiveness of the system, the better users will react to security incidents on time. The high correlation suggested that if the user perceives the system is effective, he would be vigilant and prepared to take action whenever necessary. This finding underlined the importance of perceived effectiveness in enhancing users' security awareness and responsiveness.

Hypothesis 4 (H4): The essential design factors and consumer preferences, including ease-of-use interface design and alert configuration, are the main predictors of the level of user satisfaction, acceptance, and usage of security systems with multiple purposes.

The hypothesis was tested using structural equation modeling. The SEM model showed good fit indices: CFI = 0.95, TLI = 0.93, and RMSEA = 0.05. Ease

of use/configuration of alerts predicted user satisfaction and acceptance with $\beta = 0.48$, $p < 0.01$, and $\beta = 0.42$, $p < 0.01$, respectively. This strengthens Hypothesis 4: the user-friendly design of the interface and properly configured alerts are key to satisfying users and gaining their acceptance of multi-purpose security systems. The findings thus imply that putting these design factors at the forefront could greatly enhance user satisfaction and increase the system adoption rate.

4.4.1. Discussion of Findings:

The statistical analysis has confirmed that three major properties, usability, trust, and effectiveness, greatly influence the user satisfaction of multi-purpose security systems. Satisfyingly, usability leads to trust, and thus, trust leads to consistent alarm response and effectiveness in incident resolution (Mohamad Salleh et al., 2016). Awareness and response skills among the users improve in the case where the perceived effectiveness of the said systems is under question. Further, superior configured alerts coupled with an easy-to-use system are key aspects in determining user acceptance and satisfaction. These findings demonstrate the need for user-centric design to play a key role in the development of security systems.

This strong relationship between usability and satisfaction only shows the merit that the design of security systems must be intuitive and easy to use. If a user can navigate through a system with ease, they are more appreciative of that system's performance. This runs in line with the former study, which found that an increased level of usability raised satisfaction.

In a general perspective, it is this high level of interaction and coordination between alarms, incident resolution, and feedback loops that greatly influences the extent to which the system builds confidence in users and the effectiveness of the system. Any recipient of the security system should feel like the system will

respond reasonably and competently to any of the security threats. Such coordination of responses to alarms, then crisply fed back, builds that sort of confidence that will forge acceptance and reliance upon the system.

The positive correlation between perceived effectiveness and the ability of users to take action at the right time toward an incident stresses the importance of effectiveness in raising awareness of security. An active user with superior abilities to judge the effectiveness of security measures becomes more vigilant and prepared to take needed action. This just goes to show that perceived effectiveness can be used to trigger or increase users' responsiveness.

These design features substantially affect user satisfaction and acceptance. It means that better design ensures the fulfillment of well-configured, user-friendly alerts, thus positively supporting satisfaction and acceptance. This suggests that the design of multi-purpose security systems should prominently feature user-friendly interfaces and adequately configured alerts in order to maximize user satisfaction and acceptance.

4.5. Conclusion

The statistical analysis within this research clearly points out the significance of user-centered designs for effectiveness and acceptance connected with multi-purpose security systems. The reliability and validity of the questionnaires were high, providing robust data representative of user experiences. Descriptive statistics and hypothesis testing within this study have shown important revelations with variables impacting user satisfaction, trust, and effectiveness toward these systems.

Results show that usability, trustworthiness, and effectiveness increase user satisfaction. As such, alarm response coordination reliability, capabilities for the resolution of incidents, and user-friendly design are primary in the establishment of

trust and assurance that the systems meet user expectations. The results, therefore, portray that the development of security systems in the future highly considers users' experience, feedback mechanisms, and ease of use to ensure maximum acceptance and satisfaction.

This paper makes both theoretical and practical contributions to the study of multi-purpose security systems, with valuable insight provided towards the implementation process for security professionals, policymakers, and developers. In this regard, this study paves the way for the development of more effective, user-friendly, and secure home security solutions by focusing on user-centered design, helping further enhance safety and peace of mind for each user. The study also bases further research in the area. Future studies could, therefore, longitudinally assess the long-term effectiveness and sustainability of multi-purpose security systems. Comparison studies of different types of security systems or specific security features may also be instructive, given which designs and technologies are most effective in light of available resources. Moreover, current state-of-the-art technologies, including artificial intelligence and machine learning integrated into these systems, could give way to new lines of research into improvements in security.

Chapter Five: Research Limitations, Recommendations & Conclusion

Chapter Five concludes this research with a summary of all the limitations encountered in the study, making recommendations from the findings/requirements established through the research's execution and summarizing the conclusions reached in this research. This chapter is of an important nature since it puts the results of this study into proper perspective and points out the constraints that led to the limitations and the way forward for future research and practical improvement.

In the first section, we look at the limitations that may have impacted this study's findings and point out areas where further research is still necessary. The importance of such recognition is not only to contextualize the findings but also to appropriately frame the scope of research. Some design, implementation, and user experience recommendations to further the development of multi-purpose security systems follow. Such recommendations are based on the findings of this study. They are presented to developers, policymakers, and other readers for consideration in arriving at the best way to enhance the effectiveness of such systems. It synthesizes the research by way of concluding the chapter through the reiteration of findings and their implications for the enhancement of the effectiveness and improvement of user satisfaction with the use of such information systems. This section is positioned to convey the general idea of how research contributes to both the theoretical and practical dimensions of user-centric multi-purpose security systems, setting up future improvements.

5.1. Research Limitations & Future Research

Although this study about the user-centered evaluation of multi-purpose security systems contributes to several aspects valuable for such research, worth

mentioning here are some of its limitations so that the findings can be put in context and areas for future research clarified. The biggest limitation was the study sample size. The sample size may not represent a population large enough to generalize findings to the general context for all multi-purpose security system users. Although there is an element of diversity in the sample, which was specifically included, this alone still somewhat constrains generalization to other demographic or geographic contexts.

Another limitation is that this research is based on people's self-reporting, so there are a number of biases involved, including social desirability bias, which entails that participants may answer in a manner they consider socially plausible as opposed to giving genuine opinions. Also, the cross-sectional design of the study involved taking data at one point in time and, as such, could not deal with changes in the user's perceptions and experiences with time. Longitudinal studies could clarify how user satisfaction and system effectiveness are developing. This study was mainly user-centered, with security experts and industry employees, and might miss out on policymakers, law enforcement officials, and other users who may not use but interact with or be influenced by such security systems. These views might add another holistic dimension to the impact and effectiveness of those systems.

Some of the areas of future research potentially lie in building from the discussion of the findings provided here, such as increasing the sample size by including participants from different geographical and cultural backgrounds to increase generalizability, examination of the changes in user satisfaction and system effectiveness through time in longitudinal studies for insights toward long-term sustainability and impact on multi-purpose security systems.

Further research can be carried out on the possibilities of integration of advanced technologies such as artificial intelligence and machine learning into the

system. It would be helpful to understand how these technologies would help improve system effectiveness and user satisfaction. Future studies could also further explore the ethical dimensions of those systems with regard to the privacy and data security dimension in order to make sure that all the gains derived from these technologies come without any cost to the users in terms of trust or rights going amiss.

5.2. Research Recommendations

Some recommendations to improve the design, implementation, and user experience of multi-purpose security systems could be based on these findings. By bringing these systems more in line with the needs and expectations of users, improvements in usability, trust, and overall effectiveness will be achieved.

1. **User-Centric Design:** The critical finding of usability from this research as a strong driver of user satisfaction is one that security system developers should respect with user-centered design: making interfaces intuitive, easy to navigate, and accessible to users across the board at all levels of technological proficiency. Usability testing by users during the process of development could gather valuable feedback and bring to light usability problems at the very early stage of development.
2. **Enhanced Feedback Mechanisms:** The study showed that reliable alarm-response coordination and effective resolution of incidents are of prime importance in building trust among the users. The mechanisms of clear and timely feedback, which enlightens the user about the status, actions taken, and outcome in case of any security incident, should be built by the developers. Detailed reports and real-time notifications can help in enhancing user confidence regarding the reliability of the system.

3. Customization and Personalization: Security demands vary greatly among the individual. Thus, various settings and provisions can increase user satisfaction and the overall system effectiveness. Hence, it shall provide users with the ability to change alert settings, response protocols, interface, etc., to suit their needs for a better user experience.
4. Integration of Advanced Technologies: Advanced technologies such as artificial intelligence and machine learning could be applied to make multi-purpose security systems more effective. These new technologies will be able to offer better accuracy of threat detection, reduce cases of false alarms, and provide more sophisticated analysis in cases of security incidents. Developers should find ways to put these technologies into play while ensuring transparency and clarity for the user.
5. Ethical Considerations: The ethical use of multi-purpose security systems cannot be compromised. A joint effort on the part of the developers and policymakers to come up with guidelines and standards that address privacy and data security concerns is very important. Robust data protection measures, together with clear user information about data collection, storage, and usage, can build trust and ensure ethical practices.

5.3. Conclusion

This study provides a critical review of user-centered assessment toward achieving high levels of usability, trust, and effectiveness that would drive user satisfaction in multi-purpose security systems. The research findings further emphasize the very reason for having a user-centered design in the development of security systems, which is to take cognizance of users' needs and expectations. Developers can achieve much in terms of user experience and system acceptance

by focusing on intuitive interfaces, reliable feedback mechanisms, and customizations.

It inclines the power of advanced technologies like AI and Machine Learning to increase the efficiency level of security systems. This, however, will be based on ethical questions to ensure the responsible use of these technologies. Stakeholder engagement of a wide scope and wide coverage in terms of training and support is another stake critical to successful implementation and adoption.

Though the study raises many interesting insights, it accepts its limitations on grounds such as the small sample size and data that was based on self-reporting. Therefore, some obvious future avenues of research must consider increasing the sample size and bringing diversity in the kinds of participants. Longitudinal studies are also another important area of future research. Other important areas are investigating the possibility of integration of advanced technologies and ethical issues of the security system.

This research clarifies the theoretical and empirical knowledge related to multi-purpose security systems and provides developers, policymakers, and security professionals with various useful insights. Indeed, complex security systems, while more effective, would be trusted and accepted only if user-centric design and ethical concerns were embedded at the heart of their development. The main result is to serve the purpose of further research and development with steps toward more secure and user-friendly solutions in security. On the issues of safety and peace among individuals and society, we can pledge to continual improvement and efficient stakeholder involvement so that security technologies remain evolving in a dynamic world.

References

- Ahram, T., & FalcãoC. (2020). *Advances in usability and user experience: Proceedings of the AHFE 2019 international conferences on usability & user experience, and human factors and assistive technology, July 24-28, 2019, Washington DC, USA*. Springer International Publishing, Imprint Springer.
- Alonso-Ríos, D., Vázquez-García, A., Mosqueira-Rey, E., & Moret-Bonillo, V. (2009). Usability: A critical analysis and a taxonomy. *International Journal of Human-Computer Interaction*, 26(1), 53–74.
<https://doi.org/10.1080/10447310903025552>
- Alsufyani, A., Rana, O., & Perera, C. (2023). *Knowledge-based cyber physical security at smart home: a review*. Cardiff University, UK
- Archer, K., Savage, R., Sanghera-Sidhu, S., Wood, E., Gottardo, A., & Chen, V. (2014). Examining the effectiveness of technology use in classrooms: A tertiary meta-analysis. *Computers & Education*, 78, 140–149.
<https://doi.org/10.1016/j.compedu.2014.06.001>
- 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.
- Boslaugh, S. (2013). *Statistics in a nutshell*. O'Reilly.
- Botsman, R. (2017). *Who can you trust?* PublicAffairs.
- Bujang, M. A., Omar, E. D., & Baharum, N. A. (2018). A review on sample size determination for Cronbach's alpha test: A simple guide for researchers.

- Malaysian Journal of Medical Sciences*, 25(6), 85–99.
<https://doi.org/10.21315/mjms2018.25.6.9>
- 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."
- Hacek, J. (2017). The correlation of usability, familiarity, satisfaction, and reputation with the loyalty of student users of news websites. *Medijske Studije*, 8(15), 56–71. <https://doi.org/10.20901/ms.8.15.5>
- 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.
- Karat, C., & Karat, J. (2022). *Designing and evaluating usable technology in industrial research*. Springer Nature.
- Kim, J., Phan, K., & Daim, T. (2017). *Research and development management*. Springer.
- 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).

- Major, L., Francis, G. A., & Tsapali, M. (2021). The effectiveness of technology-supported personalized learning in low- and middle-income countries: A meta-analysis. *British Journal of Educational Technology*, 52(5).
- Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology. *ACM Transactions on Management Information Systems*, 2(2), 1–25. <https://doi.org/10.1145/1985347.1985353>
- Mohamad Salleh, M. A., Salman, A., Ali, M. N. S., & Hashim, H. (2016). The importance of usability features in enhancing online communication satisfaction. *Jurnal Komunikasi, Malaysian Journal of Communication*, 32(1), 1–15. <https://doi.org/10.17576/jkmjc-2016-3201-01>
- 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.
- Price, P. C. (2018). *Reliability and validity of measurement – research methods in psychology*. Opentextbc.ca.
<https://opentextbc.ca/researchmethods/chapter/reliability-and-validity-of-measurement/>

- Rahardja, U., Aini, Q., Isma Graha, Y., & Lutfiani, N. (2019). Validity of Test Instruments. *Journal of Physics: Conference Series*, 1364(1), 012050.
<https://doi.org/10.1088/1742-6596/1364/1/012050>
- Sanjay Satam, S., & El-Ocla, H. (2022). Home security system using wireless sensors network. *Wireless Personal Communications*, 125(2), 1185-1201.
- Sun, Y., Fang, Y., Lim, K. H., & Straub, D. (2012). User satisfaction with information technology service delivery: A social capital perspective. *Information Systems Research*, 23(4), 1195–1211.
<https://doi.org/10.1287/isre.1120.0421>
- Tsakanikas, V., & Dagiuklas, T. (2018). Video surveillance systems-current status and future trends. *Computers & Electrical Engineering*, 70, 736-753.
- Taherdoost, H. (2016). Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in research. *International Journal of Academic Research in Management*, 5(3), 28–36.
- Tan, W. (2017). *Research methods*. World Scientific Publishing Company.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's Alpha. *International Journal of Medical Education*, 2(2), 53–55.
<https://doi.org/10.5116/ijme.4dfb.8dfd>
- Weaver, K. F., Morales, V. C., Dunn, S. L., & Weaver, P. F. (2018). *An introduction to statistical analysis in research: With applications in the biological and life sciences*. John Wiley & Sons, Inc.
- Yang, J., Huang, R., & Spector, J. M. (2019). *Educational technology: A primer for the 21st century*. Springer Singapore.
- 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.