Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Users' Information Security Awareness of Home Closed-Circuit Television Surveillance

Yazeed Alkhurayyif*
Department of Computer Science, College of Sciences and Humanities, Shaqra University, Saudi Arabia.

Received 21 Mar. 2023; Accepted 3 June 2023; Available Online 15 June 2023

Abstract

Closed-circuit television (CCTV) surveillance cameras are widely used in public and private areas around the world. It is primarily used for tracking individuals and preventing criminal activities. It is necessary to balance the benefits of video surveillance and the risks it poses to individuals' right to privacy. The existing studies raised privacy issues of installing CCTV in public places. However, there is a lack of studies investigating users' awareness of information security and privacy limitations in installing CCTV in private places. Thus, in this study, the author evaluated users' information security awareness of the value of CCTV and other forms of video surveillance. In-person interviews were conducted in Riyadh province, Kingdom of Saudi Arabia. A total of 77 individuals responded to the interview. A qualitative analysis was conducted to evaluate the participants' perception of CCTV usage. The outcome of the analysis revealed four themes: Privacy invasion, privacy awareness, dilemmas in implementing security, and preventive measures. The findings revealed that the participants required strict privacy policies for installing CCTV video monitoring systems in private areas. In addition, they understood that CCTV is effectively reducing the fear of crime. The research contributes to understanding users' general awareness of information security and offers the necessary steps to protect the user's privacy in a CCTV surveillance environment. In addition, a data-sharing framework is recommended to share the data in a secure environment. Furthermore, researchers can utilize the study findings in conducting further similar investigative studies.

I. Introduction

THE demand for infrastructure to safeguard against harm to persons or property has led to a rapid rise in video surveillance in the public and commercial sectors [1]–[3]. The widespread availability of low-cost communication infrastructure and the declining prices enable individuals or entities to install video surveillances [4]–[6]. Using video cameras to monitor public areas and secure private property has significantly reduced crime. Across the globe, governments employ closed-circuit television (CCTV) systems to monitor public spaces to reduce criminal activity [7]. Destruction and other forms of property damage can be uncovered and investigated with its assistance [8]. CCTV is widely deployed in the private sector to prevent criminal activity [9].

Keywords: Cybersecurity, Security Studies, Privacy Threats, CCTV, Information Security, Security Threats.

Production and hosting by NAUSS

* Corresponding Author: Yazeed Alkhurayyif
Email: yalkhurayyif@su.edu.sa

doi: 10.26735/VFKO2846

One of the significant attractions of video surveillance is its ability of distant monitoring [10]. As a result, law enforcement agencies may increase their coverage areas [11]. Video monitoring and rapid reaction can result in significant cost savings because hardware and communication infrastructure prices have decreased [12]. The same justifications apply to the private sector, where video surveillance systems have been rapidly adopted due to considerations such as reduced costs and the potential of outsourcing security services to other organizations [13]. Because of these tendencies, surveillance cameras can be found in many public and private establishments across many developed countries, including retail establishments, residential areas, streets, squares, parks, public transportation hubs, airports, and transportation hubs.

The Vision 2030 of the Kingdom of Saudi Arabia (KSA) focuses on data privacy and individuals' right to preserve their data [14]. In addition, one of its objectives is to balance activities related to monitoring and privacy. Data privacy policies protect individuals' privacy and integrity across trusted communication channels. Many Internet of Things (IoT) devices capture and analyze large amounts of individuals' sensitive data [1], [15]. Biometric access control is provided through fingerprint matching, voice identification, and facial recognition as part of a home security system [16]–[18]. A CCTV surveillance mechanism is vital to a Smart Home's security system for protecting the premises and avoiding unauthorized visitors. Moreover, this system can monitor the elderly, the young, and persons with disabilities [19], [20].

Data and context-aware privacy are the two most common forms of vulnerability [17]. When transmitting sensitive information, data privacy should always be a top priority [21]. Adaptable services are in high demand due to the proliferation of context-aware applications [22]. Thus, companies are transitioning from making physical goods to offering services tailored to specific contexts. These services collect, structure, access, process, and distribute the user's confidential data [15], [23], [24]. Users are encouraged to provide their data to access the free services through a portal or product [25]–[27]. For instance, CCTV service providers may request users to share their data by offering false promises. Recently, public concerns and anxieties about privacy have increased due to unauthorized user data access [28], [29]. Therefore, it is essential to address trust and security concerns.

The exponential growth of internet-based home appliances enables individuals to store their data in a centralized or decentralized repository. CCTV is widely used in public and private premises. The users create profiles by providing their data in order to access the device. As a result, CCTV service providers may access the users' data without authorization. In KSA, the government introduced privacy policies to protect users' data. However, there is a demand for research studies to identify user perceptions of privacy invasions. This motivated the author to study the significance of data privacy awareness among individuals in KSA.

In this study, the author intended to investigate the user's perception of data breaches in CCTV surveillance activities. The citizens and residents of the KSA are the populations of this study. Qualitative analysis is employed to draw insight from the participants' responses. The contributions of the study are as follow:

1. Identification of the user's current knowledge of the privacy invasions in CCTV surveillance.
2. Extraction of key themes to support the government in improving the present data privacy policies.
3. Offering recommendations to protect users' privacy from unauthorized access.

The remaining part of the paper is organized as follow: Section II addresses the importance of privacy in handling CCTV data. Section III discusses the methodology of the study. The study findings are presented in section IV. Section V discusses the findings. Finally, section VI concludes the study with its limitations and future directions.

II. Related Works

Over the past few years, surveillance cameras have become increasingly ubiquitous in daily life [1], [8]. These are widely used in residences, apartments, organizations, government agencies,

TABLE I
Characteristics of Existing Literature

Authors	Methodology	Dataset	Features	Limitations
Mahmoud and Zohair [1]	Qualitative study	Six participants were included in the study	Participants discussed the limitations of data privacy in CCTV surveillance.	Limited number of population, Difficult to generalize the outcome
Birnhack and Perry-Hazan [2]	Qualitative study	The researchers recruited 83 students from different schools	Participants highlighted the significance of CCTV monitoring in the educational institutions	A broader overview of student perception in a diverse setting
Golda *et al.*, [5]	Qualitative study	216 participants were included in the study	The findings show that men had considerably lower confidence in the government to prevent privacy issues than women.	The sample was on average tech-savvy, and over 50% had an academic degree. Therefore, it may not reflect the total population.
Wang *et al.*, [4]	Qualitative study	Recruited participants' ages ranged between 18 and 62 years old.	Described the potential benefits of Drones and CCTV surveillance	Focused on lightweight Drone monitoring rather than CCTV monitoring
Fisher et al., [6]school security cameras have become one of the most common interventions for preventing and detecting school crime and violence. However, existing theoretical and empirical literature on the effects of school security cameras offer contrasting expectations. This study uses multiple waves of the nationally representative School Survey on Crime and Safety to create a two-wave longitudinal sample of schools (N = 850	Longitudinal study	850 participants were included from different schools	The outcome shows that there is no significant improvement in using CCTV	Focused on crime and safety. Compared the views of participants for generating the outcome
Birnstill *et al.*, [7]	Qualitative study	103 participants	Discussed the key mechanism for protecting the personal identities	Used different scenarios and proposed the protection mechanism
Tran *et al.*, [8]	Qualitative study	49 participants	The thematic analysis disclosed the significance of CCTV in enhancing overall school performance	46 individuals are excessively small for generalizing the results to the entire population.
Gupta *et al.*, [11]	Quantitative study	24 academic librarians	The outcome showed the importance of CCTV in controlling theft and criminal activities.	Focused on the CCTV applications in libraries
Yao *et al.*, [19]	Qualitative study	18 participants	The outcome provided the significance of users awareness of the internet based devices	The outcome is based on the specific scenarios
Yao et al., [31]	Qualitative study	25 participants	Discussed the importance of improving security standards in Smart home	Sample is small. Generalization is difficult

etc., [4]. This development has prompted experts to explore the benefits and limitations of CCTV surveillance.

Lack of awareness tends to cause users to disclose crucial data to external parties [2]. This data can be used to deceive, steal, and discriminate against users. Modern techniques can create a user profile on social media platforms using the user's crucial data. Moreover, a few organizations may exploit the customer's data in today's data-driven environment. Many security recommendations have been offered to clarify fundamental safety requirements and streamline data privacy activities [11]. These requirements include ensuring the CCTV data storage application is always up-to-date and requiring the CCTV vendors to provide a list of authorized service providers. However, such recommendations only address the minimum security demands. Hackers can employ ever-more-complicated and original methods to breach the devices' defenses [10]. Thus, users should use equipment with robust encryption, do regular maintenance, and adhere to a stringent procurement procedure when purchasing [11]. Users may install susceptible devices due to lack of expertise, poor operational testing, lack of autonomous asset management, and limited network monitoring abilities [15]-[17].

Table I should be after this part outlines characteristics of the existing literature. The literature discussed some case studies demonstrating the efficacy of CCTV systems as a vital safety and security measure. Mahmoud and Zohair [1] probed the perceptions of citizens and residents of the United Arab Emirates of using CCTV cameras. Birnhack and Perry-Hazan [2] discussed the potential benefits of CCTV in educational insititutions. They analyzed students' perception of video montioring devices in the schools. Golda *et al.*, [5] conducted a study evaluating the applications of smart video surveillance systems. Wang *et al.*, [4] discussed the benefits of CCTV surveillance in educational institutions. They expressed that surveillance cameras were crucial in preventing terrorist acts committed by individuals across the globe.

Furthermore, Fisher *et al.* [6] investigated the role of CCTV surveillance in controlling criminal activities in schools. Birnstill *et al.* [7] studied the applications of anonymization techniques for smart video surveillance. Recently, Tran *et al.* [8] have evaluated stakeholders' attitude towards installing CCTV cameras. They discussed the significance of CCTV in public places. Similarly, Gupta et al. [11] discussed the role of CCTV in mitigating theft and criminal activities in libraries. Yao et al. [19] proposed a co-design study for developing a privacy mechanisms for smart homes.

Numerous incidents of online privacy violations due to the leakage of personal information of social media users have occurred in recent years. However, users appear to be losing out on privacy protection, leading to more privacy invasions. The existing studies [10]-[17] discussed the impact of privacy invasions in internet-based devices. There is a knowledge gap in the current literature. There is a lack of studies investigating the impact of previous encounters with privacy violations in maintaining CCTV surveillance environments in private residences. In addition, few studies [18]-[24] addressed the significance of protecting data from unauthorized users.

III. Research Methodology

The interview approach elicited a range of notions pertinent to the study's objective. According to the study [1], this method allows a detailed evaluation of the participants' perception of data privacy invasions. An ethical application document was submitted to the research ethics committee at the Shaqra University to investigate and resolve any ethical issues regarding human rights violations and safeguard the privacy and anonymity of the participants (the ERC approval number: ERC_SU_20230010).

A. Research Questions

The following research questions were addressed:

- How do the participants perceive privacy invasion in a CCTV environment?
- What are the participants' experiences with privacy invasion in private and public spaces?
- How can one prevent intrusions into their personal space?

B. Data Collection

This research examined public perceptions regarding CCTV systems' capabilities to address security and privacy concerns. Initially, the author requested his colleague for recruiting the participants by using a snowball-sampling approach. After obtaining the participants' consent, the author conducted the interview on seventy-seven participants. An expert at information security and data privacy from the Department of Cybersecurity, Shaqra University, was requested to validate the views of the participants recruited randomly from various locations in Riyadh. The expert is a well-known panelist at conferences in the KSA on Information Security and Data Privacy. He is a security analyst at one of the country's most prominent institutions.

C. Pilot Study

The author developed a set of questions to receive elicit participants' responses to share regarding the features and limitations of CCTV surveillance. The research procedure and interview questions were modified after conducting two sessions with nine individuals and receiving some insights from them. First, the author asked participants to consider CCTV surveillance from their viewpoint. It was evident from the pilot study that the participants were likely to perceive issues from the government's point of view. Therefore, a question about the last time the CCTV service team visited them was added. Second, the preliminary procedure posed questions to the participants on their overall impressions and concerns regarding the technologies used in the smart home. However, the author discovered in the pilot research that participants were more concerned with the drawbacks of CCTV services' data privacy regulations. Finally, the author interviewed the individuals to find out what they thought that would make their data more secure. As a result, he included a short introductory session in which participants were shown a few examples of data-sharing regulations.

D. Data Analysis

The interviews' primary goal was to collect information about the features and qualities of CCTV systems that the public needs to co-exist with them. The participants were interviewed using a semi-structured interview. It gives the participants greater freedom of expression and allows them to share their perceptions. Several elements were investigated to determine the features and limitations of CCTV surveillance systems. These included the locations and methods of installing cameras, security problems addressed by cameras, privacy threats, and strategies for mitigating threats.

There is a knowledge gap in identifying the data privacy invasions in the CCTV environment and it can be bridged by providing concrete instances of disparities and clarity on trust in data security policies using intelligent technologies [3]-[7]. Thus, the descriptive analytic approach was employed to provide qualitative findings. The author conducted the interview in which participants shared their opinions on CCTV data privacy invasions. He requested the participants to share their experiences with the CCTV providers and technicians who monitor the recorded videos and images. Interviewees were encouraged to share their past experiences related to CCTV surveillances.

The population of Riyadh province was divided into a sample of 77 individuals, and each of the corresponding critical individuals was interviewed two times. There were 77 individuals, 36 females and 41 males whose ages ranged between 21 and 65+. Of the 77 individuals, 45 were citizens, and 32 were residents.

Only persons with five years of experience with IT gadgets and CCTV applications were recruited as participants in the study. The selected participants were more likely to provide unique insights into the social context of the CCTV either because of their unique CCTV installations or their relationships with other participants (neighbors, family, and friends). The interviews were conducted online, using Zoom and Skype, and lasted one hour.

The descriptive-analytic approach involving an iterative theory and data process was utilized [1]. The statistical analysis is presented in Appendix. The author followed the thematic analysis approach for extracting the data insight. Data pre-processing was conducted to establish commonalities in the research information. Various CCTV configurations, participant concerns, and utilization standards were compared. Using this framework as an analytic toolkit, the responses unique to privacy and risk were systematically analyzed. This assessment approach allowed the researcher to understand the study participants' perceptions. The study participants asserted a combination of principles related to the CCTV surveillance environment. To avoid revealing personal information, quotes from participants were de-identified. The stories presented served as illustrative instances. As a result, the outcome of this study may be applied to other contexts.

IV. Results

The thematic analysis generated four themes: a perspective on privacy invasion, privacy awareness, dilemmas in implementing security, and preventive measures. Table II presents some critical questions used in the study in order to extract central themes.

The first three topics outline the participants' perception of the current CCTV data privacy standards. Lastly, the fourth topic presents the preventive measures to strengthen data protection techniques. Fig. 1 depicts the themes extracted from the responses.

TABLE II
Questions for Extracting Themes

Questions
Are you aware of the risks in handling CCTV video / audio / images?
Are you aware of the current data privacy policies in the Kingdom of Saudi Arabia?
Does your CCTV provider comply with the Global Records Retention Schedule with regard to Saudi Arabia data privacy policies?
Do you routinely access / review / monitor your CCTV data or application to determine whether the data collected, stored, or processed is necessary to meet the stated business objectives?
What are the security vital roles provided by CCTV systems?
Are you satisfied with the CCTV security roles implemented by the CCTV providers?
What are the privacy concerns caused by the existence of CCTV?

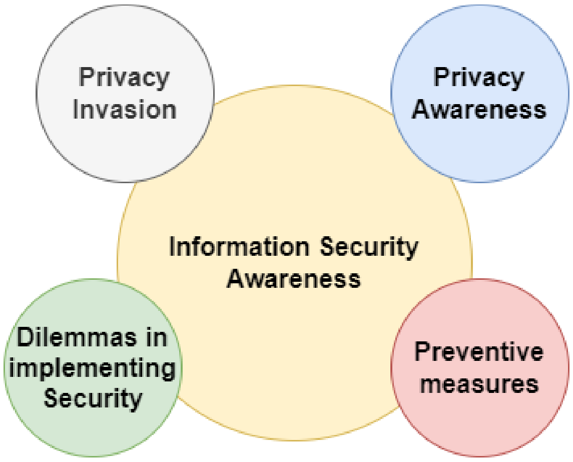
Privacy Invasion
Privacy Awareness
Information Security Awareness
Dilemmas in implementing Security
Preventive measures

Fig. 1. Information Security Themes.

The public and private domains shared these commonalities. The themes are composed of several sub-themes. It is evident that there might be some overlap between these topics and the underlying dimensions. The verbatim of the participants has been recorded under the respective sub-themes. Table III outlines the extracted themes and sub-themes.

A. Perspective on privacy invasion

This topic reflected the participants' attitudes and opinions about strangers invading their personal space in public and private spaces. Participants generally agreed that respecting people's personal space in public is necessary. When people's personal space is invaded, they feel uneasy and upset. The participants expressed resentment at being recorded by friends and strangers without their knowledge or consent. All

TABLE III
Themes and Subthemes

Themes	Subthemes
Privacy Invasion	Data disclosures, Targeted advertisements, Identity theft, Personal abuse
Privacy Awareness	Privacy expectations, Content information norms, Legal and political issues, Consent to access data
Dilemmas in implementing security	Location information, Unwanted messages, financial data exposure, Exposure of personal contacts
Preventive measures	Strong passwords, Diligence in monitoring, Two-factor authentication, Disable data tracking facility

participants agreed that CCTV owners should follow data privacy in disclosing the footage on social media platforms or sharing it with external parties. When someone violates privacy, there should be strict and well-defined consequences. They expressed the possibility of misusing the recorded videos by strangers. The following verbatim reflects users' attitude towards the CCTV cameras.

> "We have to learn the consequences of purchasing an internet-based video monitoring system. Since there have been so many tales of things seeping through and whatnot recently, contrarily, secrecy is highly valued. "

> "It's more difficult, in my opinion, to have faith in the CCTV maintenance team. I advised my family not to provide the strangers any personal details."

Privacy is a concept that has undergone dynamic definitional shifts over the centuries. The nature of privacy issues may not always fit well inside existing privacy frameworks. It might include challenges associated with data collection, data processing, and disclosure of crucial data. Extraction, observation, and incursion are all possible forms of invasion. In order to present a compelling data privacy policy, multiple forms of data invasions need to be addressed.

B. Privacy Awareness

An individual's level of privacy awareness is based on his/her knowledge about the consequences of sharing data with external parties. In addition, the nature of data plays a significant role in data-sharing policies. The findings revealed that the participants had serious concerns about privacy in public settings. In contrast, the participants who were unaware of the data privacy shared their details with unauthorized persons. One of the participants shared the following opinion.

> "The maintenance team knows our CCTV application credentials. They never allow us to change the password."

Another participant stated:

> "I asked the maintenance team to ask us to access the CCTV footage. I will not allow them to copy any files from the hard disk."

These results showed that users' awareness reduces unauthorized data access and safeguards individuals' privacy. The participants were familiar with the privacy of conduct, activity, and communication. They were aware of the consequences that might result from privacy breaches of various types (technical and non-technical). However, few participants not aware of the newer technologies based on IoT. The introduction of IoT devices leads to the development of smart home techniques. Thus, addressing the data breaches in the CCTV surveillance environment can support the policymakers to focus on developing a practical data-sharing framework for KSA. To what extent this awareness existed could not be seen. Moreover, there was an inverse relationship between the degree to which users felt their privacy was invaded and their plans to keep using the service. Participants' perceptions were found to be influential in shaping their behavior.

C. Dilemmas in Implementing Security

Participants were unsure whether technology such as Amazon Echo, CCTV surveillance, and face recognition AI were helpful or intrusive. The trustworthiness of these applications was questioned. Emerging technologies have brought positive and negative consequences, leading to many new dilemmas and perplexities. Due to their limited technology skills, the participants displayed reluctance to implement the recent security measures. In addition, misleading information in social media influenced the participants. The participants with technical skills positively implemented security using newer technologies. The following verbatim shows the importance of strict data access policies for CCTV maintenance.

> "I am afraid the CCTV providers may access the data using the hidden app."

> "The advanced hacking technologies and Dark net may use the recorded videos and images."

Some participants pointed out that people in the modern period are hyper-vigilant because of the different technologies available to them. Participants were concerned about the videos and images captured using CCTV devices. Participants expressed rising apprehension about the usage and effects of CCTV and other types of surveillance. Even though they were aware of the benefits and risks of artificial intelligence models, they might have experienced technology anxiety due to their inability to avoid or control potential technical harms. They stated that they had learned more about privacy-related issues by reading news articles and using social media. They called for a public awareness program to educate the citizens and residents about data breaches in public and private spaces. This encourages individuals to avoid sharing information in public or online forums.

The author discovered that few participants were not sharing their details in public spaces. In addition, they had their protocol to safeguard their information. Participants reported avoiding public areas to conduct financial transactions or use programs requiring credentials. Thus, participants were using their mobile devices to make fewer purchases in public.

D. Preventive Measures

The responses to queries related to the preventive measures revealed noteworthy differences in the participants' perceptions. There was a consensus among the participants on the need for face-hiding mechanisms while broadcasting the CCTV footage to unauthorized users. In public places, there should be a notification to individuals about the presence of cameras, the need for strict policies, laws, and regulations against violators.

There is also conclusive evidence that the participants appreciated the presence of laws to safeguard their privacy. The expert made some suggestions, such as restricting internet access to surveillance devices and using AI solutions to make monitoring more efficient and focusing on specific instances rather than disclosing the entire data. It is also possible to use motion or zooming auto-triggered capabilities so that the camera only turns on to record when it detects suspicious faces or movements.

The Saudi Arabia government initiated strict regulations for using CCTV in public and private spaces. Institutions of higher education, public and private healthcare facilities, public transportation, and government offices are among the places that must now have security cameras installed. Cameras are also forbidden in areas where people change clothes, beauty parlors, and women's clubs. Fines for infractions range from SR5,000 for failing to record and maintain footage to SR10,000 for installing cameras in restricted places and SR20,000 for transmitting or destroying footage or camera systems [14]. Any person who helps prosecute lawbreakers will get 10% of the corresponding fine as an incentive [13].

The resolution No. 98 was issued on 7/2/1443H and was approved by Royal Decree M/19 dated 9/2/1443H (16 September 2021), (14 September 2021) for protecting the individual's data [12]. The Personal Data Protection Law (PDPL) is Saudi Arabia's primary privacy law. Beginning on March 23, 2022, PDPL would be fully enforced, with an additional year provided for compliance. The effective date is subject to the publication of different implementing rules [12], [13]. The topic of data protection is addressed in a wide variety of additional obligatory papers and sector-specific regulations. The National Data Management Office has produced the National Data Governance Interim Regulations of 2020 (National Data Regulations), primarily concerned with governmental data [13]. However, the National Data Regulations state that any entity in the KSA that processes personal data in whole or in part, as well as any entity outside the KSA that processes personal data related to individuals residing in the KSA, must comply with Part 5 of the regulations, which deals with personal data protection [13]. So far, it is not entirely apparent whether or not the National Data Regulations have been given legal standing and are being actively implemented.

Like other worldwide data protection laws, the PDPL guarantees individual rights to privacy. Data subjects have the legal right to access, amend, delete, and transfer any personal information gathered on them. The rights of data subjects might vary widely depending on the particular data protection regulation. People whose personal or sensitive data is processed in Saudi Arabia are subject to the PDPL. Information on a deceased individual that may be used to track down a living relative is similarly protected under the PDPL. The PDPL does not cover personal data processing at home. Except in limited circumstances in the Draft Regulation, the PDPL makes it illegal for businesses to process individuals' data without their knowledge or consent. Consent to the processing of personal data may be revoked at any time by the data subject, and approval should not be required as a condition of the data controller's provision of a service or benefit. According to the PDPL, businesses must designate individuals (or a group of individuals) to carry out the law's requirements. In line with previous studies [25]-[29], and the current study's findings, a framework for protecting users' data in CCTV surveillance was proposed.

V. Discussions

In this study, the author conducted a semi-structured interview with 77 participants and evaluated their responses using a qualitative analysis approach. The study findings addressed three research questions. The thematic analysis extracted four themes for presenting a solution for achieving the study objectives. Firstly, the privacy invasion theme introduced the necessity of effective data privacy policies in public and private spaces. Secondly, the privacy awareness theme revealed the importance of awareness programs for educating individuals about data privacy invasions and their consequences. Thirdly, dilemmas in implementing security themes presented by the participants were highly motivated by social media platforms and avoided installing data security applications. Finally, the preventive measure theme aligned with the current security policies in KSA to protect users' information.

The study findings are consistent with the results of Mahmoud and Zohair [1]. There is a demand for strict policies protecting individuals' data in CCTV surveillance. In addition, this study discussed the current data privacy policies of KSA to avoid data misuse. In line with Birnhack and Perry-Hazan [3], the study's outcome revealed the significance of CCTV monitoring in public places.

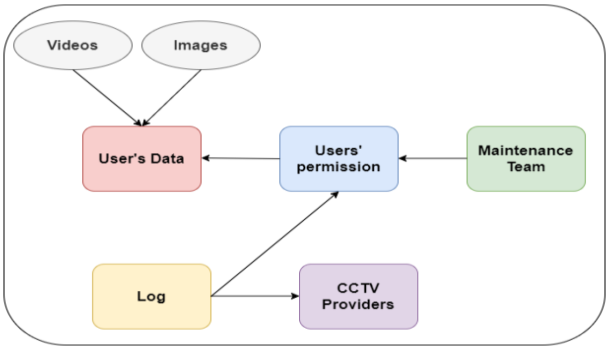

Fig. 2. Suggested data protection framework

In contrast to the findings of Golda et al. [5], there is no significant difference in the perceptions of male and female participants. In addition, the technically skilled participants did not favor CCTV surveillance in public places. Similarly, the findings did not converge with Wang et al. [4]. Wang et al. [4] investigated the role of drones and CCTV monitoring in public places, whereas the proposed study findings addressed the data invasions in the CCTV environment.

Furthermore, The study findings echoed the findings of Fisher et al. [6], Brinstill et al. [30], Tran et al. [8], Gupta et al. [11], and Yao et al. [19], [31] Users should be aware of the data privacy invasion in the public and private places. The unauthorized access of the users' data leads to negative consequences..

A. Recommendations

Based on the expert opinion and the participant's responses, the author proposed a framework in order to protect the user's privacy in the CCTV data access environment. Fig. 2 outlines the proposed data protection framework. In this framework, the CCTV maintenance team requires the users' or owners' permission to access the CCTV data. For instance, the data access credentials should not be disclosed to the maintenance team. They must request the owner login to the dashboard to delete or modify the content.

In addition, a log file should be updated each time and store the details, including the name of the head of the maintenance team, and the date and time of the modified files. The log file should be forwarded to the owner's and CCTV provider's email addresses to inform the owner. Using the suggested framework, the user's data cannot be exposed to unauthorized users, and the users' privacy will be preserved.

B. Limitations

Time constraint is the primary limitation of this study. It is recommended that a larger sample of ordinary individuals need to be interviewed in order to receive a broader range of responses and perspectives on CCTV systems. Nevertheless, in the future, the author extends this study by covering a wide range of participants. The study proposed a set of recommendations based on expert opinions. However, there is a demand to involve a larger number of experts to frame effective data privacy policies. Furthermore, the public comments may be examined and analyzed against current privacy practices to evaluate and discover the gaps in the existing rules.

VI. Conclusions

This study investigated the user's perceptions of CCTV usage and data security policies. CCTV surveillance systems have become vital for ensuring people's safety. However, there remain ongoing privacy issues that should be addressed. A qualitative approach was followed in order to obtain the responses. A total of 77 individuals from Riyadh province participated. Privacy invasions, the dilemma in implementing security applications, privacy awareness, and preventive measures were the primary themes extracted from the responses. The privacy invasions revealed the unauthorized usage of CCTV footage of public places. The dilemma in implementing security applications outlined the limitations of the security applications. Security applications require users' details to provide the services. Thus, the participants were reluctant to use such applications. Privacy awareness highlighted the importance of awareness programs in educating individuals about data privacy policies. Finally, the preventive measures provided recommendations to safeguard individual data from unauthorized access. The time constraint was the most significant limitation of this study and the challenge that needed to be overcome. Interviewing a larger sample of the general population can yield additional perspectives on the future of CCTV.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] L. Mahmoud and A. Zohair, “Public Views: How to Make CCTV Surveillance Systems Satisfy Security and Privacy Concerns?,” *Int. J. Inf. Technol. Lang. Stud.,* vol. 2, no. 2, pp. 12–27, Aug. 2018, Accessed: May 15, 2023. [Online]. Available: https://journals.sfu.ca/ijitls/index.php/ijitls/article/view/22.

[2] M. Birnhack and L. Perry-Hazan, “School Surveillance in Context: High School Students' Perspectives on CCTV, Privacy, and Security,” *https://doi.org/10.1177/0044118X20916617,* vol. 52, no. 7, pp. 1312–1330, May 2020, doi: 10.1177/0044118X20916617.

[3] L. Perry-Hazan and M. Birnhack, “The Hidden Human Rights Curriculum of Surveillance Cameras in Schools: Due Process, Privacy, and Trust,” *Cambridge Journal of Education,* vol. 48, no. 1, pp. 47–64, Jan. 2018.

[4] Y. Wang, H. Xia, Y. Yao, and Y. Huang, “Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US,” *Proc. Priv. Enhancing Technol.,* vol. 2016, no. 3, pp. 172–190, Jul. 2016, doi: 10.1515/POPETS-2016-0022.

[5] T. Golda, D. Guaia, and V. Wagner-Hartl, “Perception of Risks and Usefulness of Smart Video Surveillance Systems,” *Appl. Sci. 2022, Vol. 12, Page 10435,* vol. 12, no. 20, p. 10435, Oct. 2022, doi: 10.3390/APP122010435.

[6] B. W. Fisher, E. M. Higgins, and E. M. Homer, “School Crime and Punishment and the Implementation of Security Cameras: Findings from a National Longitudinal Study,” *Justice Q.*, vol. 38, no. 1, pp. 22–46, 2021, doi: 10.1080/07418825.2018.1518476.

[7] P. Birnstill, D. Ren, and J. Beyerer, "A user study on anonymization techniques for smart video surveillance," *AVSS 2015 - 12th IEEE Int. Conf. Adv. Video Signal Based Surveill.,* Oct. 2015, doi: 10.1109/AVSS.2015.7301805.

[8] K. Tran, T. Nguyen, L. Phan, M. Tran, M. Trinh, and L. Pham, "Stakeholders' attitudes towards the installations of closed-circuit television cameras in reducing school violence," *Heliyon,* vol. 8, no. 9, p. e10645, Sep. 2022, doi: 10.1016/J.HELIYON.2022.E10645.

[9] H. Turtiainen, A. Costin, and T. Hamalainen, "CCTV-Exposure: An open-source system for measuring user's privacy exposure to mapped CCTV cameras based on geo-location," Jul. 2022, Accessed: May 15, 2023. [Online]. Available: https://arxiv.org/abs/2208.02159v1.

[10] P. W. Khan, Y. C. Byun, and N. Park, "A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities," *Electron. 2020, Vol. 9, Page 484,* vol. 9, no. 3, p. 484, Mar. 2020, doi: 10.3390/ELECTRONICS9030484.

[11] P. Gupta and M. Margam, "CCTV as an efficient surveillance system? An assessment from 24 academic libraries of India," *Glob. Knowledge, Mem. Commun.,* vol. 70, no. 4/5, pp. 355–376, 2021.

[12] A. E. Waldman, *Privacy as trust : information privacy for an information age.* Cambridge, 2018.

[13] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.,* vol. 33, no. 3, p. e3677, Mar. 2022, doi: 10.1002/ETT.3677.

[14] Saudi Arabian Personal Data Protection Law (PDPL), "https://istitlaa.ncc.gov.sa/en /transportation/ndmo/pdpl/Documents/Draft%20of%20the%20Executive%20Regulation%20of%20Personal%20Data%20Protection%20Law%20-%20MARCH%209.pdf," 2022. .

[15] R. Ch, G. Srivastava, T. Reddy Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *J. Inf. Secur. Appl.,* vol. 55, p. 102670, Dec. 2020, doi: 10.1016/J.JISA.2020.102670.

[16] B. Custers, A. M. Sears, F. Dechesne, I. Georgieva, T. Tani, and S. van der Hof, *EU Personal Data Protection in Policy and Practice,* vol. 29. The Hague: T.M.C. Asser Press, 2019.

[17] T. Yu et al., "Learning context-aware policies from multiple smart homes via federated multi-task learning," *Proc. - 5th ACM/IEEE Conf. Internet Things Des. Implementation, IoTDI 2020,* pp. 104–115, Apr. 2020, doi: 10.1109/IOTDI49375.2020.00017.

[18] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities," 2019.

[19] Y. Yao, J. R. Basdeo, O. R. McDonough, and Y. Wang, "Privacy perceptions and designs of bystanders in smart homes," *Proc. ACM Human-Computer Interact.,* vol. 3, no. CSCW, p. 24, Nov. 2019, doi: 10.1145/3359161.

[20] L. Taylor and L. Taylor, "Data Justice, Computational Social Science and Policy," *Handb. Comput. Soc. Sci. Policy,* pp. 41–56, 2023, doi: 10.1007/978-3-031-16624-2_3.

[21] A. E. Waldman, "Cognitive biases, dark patterns, and the 'privacy paradox,'" *Curr. Opin. Psychol.,* vol. 31, pp. 105–109, Feb. 2020, doi: 10.1016/J.COPSYC.2019.08.025.

[22] P. E. Naeini et al., "Privacy Expectations and Preferences in an IoT World," 2017, Accessed: May 15, 2023. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini.

[23] O. Kudina and P. P. Verbeek, "Ethics from Within: Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy," *https://doi.org/10.1177/0162243918793711,* vol. 44, no. 2, pp. 291–314, Aug. 2018, doi: 10.1177/0162243918793711.

[24] S. A. Zhang, Y. Feng, A. Das, L. Bauer, L. Cranor, and N. Sadeh, "Understanding People's Privacy Attitudes Towards Video Analytics Technologies."

[25] S. Pink, S. Sumartojo, D. Lupton, and C. Heyes La Bond, "Mundane data: The routines, contingencies and accomplishments of digital living," 2017, doi: 10.1177/2053951717700924.

[26] T. Coughlan *et al.*, "Current Issues and Future Directions in Methods for Studying Technology in the Home," 2013, Accessed: May 15, 2023. [Online]. Available: http://www.psychnology.org/File/PNJ11(2)/PSYCHNOLOGY_JOURNAL_11_2_COUGHLAN.pdf.

[27] S. Pink, D. Lanzeni, and H. Horst, "Data anxieties: Finding trust in everyday digital mess," Big Data Soc., vol. 5, no. 1, pp. 1–14, Jan. 2018, doi: 10.1177/2053951718756685.

[28] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," *Technol. Forecast. Soc. Change,* vol. 138, pp. 139–154, Jan. 2019, doi: 10.1016/J.TECHFORE.2018.08.015.

[29] A. Burrows, D. Coyle, and R. Gooberman-Hill, “Privacy, boundaries and smart homes for health: An ethnographic study,” *Health Place*, vol. 50, pp. 112–118, Mar. 2018, doi: 10.1016/J.HEALTHPLACE.2018.01.006.

[30] M. S. Eastin, N. H. Brinson, A. Doorey, and G. Wilcox, “Living in a big data world: Predicting mobile commerce activity through privacy concerns,” *Comput. Human Behav.,* vol. 58, pp. 214–220, May 2016, doi: 10.1016/J.CHB.2015.12.050.

[31] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, “Defending my castle: A co-design study of privacy mechanisms for smart homes,” *Conf. Hum. Factors Comput. Syst. - Proc.,* vol. 12, May 2019, doi: 10.1145/3290605.3300428.