Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

Research Article

Mitigating Default Password Risks in CCTV: A Qualitative Study to Guide Recommendations for Device Makers

Sara Alghamdi, Noura Aleisa*

College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
E-mail: n.aleisa@seu.edu.sa

Received: 27 August 2024; **Revised:** 23 December 2024; **Accepted:** 27 December 2024

Abstract: The rapid growth of Internet of Things (IoT) devices has brought unmatched convenience, connectivity, and significant cybersecurity issues. One of IoT devices' predominant security risks is default passwords, making them vulnerable to various attacks and exploits. CCTV is highly susceptible to security breaches due to the reliance on default passwords. This paper identifies the risks associated with default passwords in CCTV and explores how they can be mitigated. Qualitative research was conducted to achieve this. Qualitative data was gathered through interviews with security experts, manufacturers, and CCTV end-users, and thematic analysis was subsequently analyzed. Through the research, the authors identified common security vulnerabilities and risks linked to default passwords in CCTV and employed password policies and authentication protocols. They recommended best practices to mitigate these risks. The results of this study have significant consequences for the area of IoT security, offering a broad understanding of the risks linked to default passwords in IoT devices, identifying optimal practices for mitigating them, and contributing valuable observations to more comprehensive discussions on IoT security. Eventually, the overarching goal of this study is to increase the safety and privacy of both individuals' and organizations' IoT devices and promote liable and ethical use of this technology.

Keywords: security, CCTV, default passwords, IoT, authentication

1. Introduction and literature review

Internet of Things (IoT) devices have significantly transformed our daily lives, work, and interaction with technology [1]. The proliferation of IoT devices, spanning smart homes, wearable tech, industrial controls, and medical equipment, has witnessed remarkable convenience, efficiency, and interconnectivity with IoT devices. These IoT devices have empowered us to perform tasks quickly and efficiently at unprecedented levels of connectivity with the world around us like never before.

1.1 *Problem statement and research aim*

The proliferation of IoT devices has brought about unprecedented convenience, efficiency, and connectivity, transforming how we interact with technology. While these IoT devices have brought remarkable advantages, they also introduce vulnerabilities that expose them to a broad spectrum of threats and exploits, compromising individuals and

DOI: https://doi.org/10.37256/cnc.3120255576

‘organizations’ safety and privacy. One of the predominant security issues of IoT devices is default passwords. Default passwords (PWs) refer to the pre-set passwords that manufacturers assign to their devices or systems upon initial installation or configuration. These passwords are intended to provide temporary access and are commonly shared among a specific product model or brand. Unfortunately, most manufacturers use weak default passwords, easily guessed or exploited by unauthorized individuals. This practice poses a significant security risk, and many users need to change the default PW when they install an Internet of Things (IoT) device. This failure to modify the default PW can be attributed, in part, to the perceived difficulty of the task. Default PWs are often weak, predictable, and shared among multiple devices, making them vulnerable to attacks and exploits. This is particularly true for CCTV, which is widely used for surveillance in homes, businesses, and public spaces. The study seeks to provide valuable insights into these risks and identify practical mitigation strategies, ultimately contributing to developing more secure and reliable IoT devices [2, 3].

Three central research questions guide the investigation:

- What are the prevalent vulnerabilities and security risks linked to default PWs in CCTV?
- What are the current password policies and authentication protocols used in CCTV?
- What are the optimal practices for mitigating the risks linked to default PWs in CCTV?

The study aims to enhance the security of these devices and contribute to the broader discourse on IoT security by highlighting the risks associated with default PWs in IoT devices and the need for more collaborative and interdisciplinary approaches to addressing these risks. It also recommends improving password policies and authentication protocols in CCTV cameras.

1.2 *Literature review*

The proliferation of Internet of Things (IoT) devices, particularly in Closed-Circuit Television (CCTV) systems, has ushered in new dimensions of connectivity and convenience. However, with this technological advancement comes an alarming increase in security vulnerabilities, prominently exemplified by the persistent use of default passwords. This literature review synthesizes insights from 13 research papers from [4, 5] to comprehensively explore the risks associated with default PWs in IoT devices, specifically CCTV systems. The review further delves into proposed strategies and best practices advocated by researchers to enhance the security posture of these devices.

Several papers contribute to understanding security challenges in IoT devices, emphasizing the vulnerabilities introduced by default PWs [6]. Highlighting the prevalence of default PWs as a significant threat vector makes devices easily accessible to malicious actors who intentionally try to harm systems through unauthorized access, steal information and harm the services. A similar idea is presented by [7], underscoring the ambiguity in technical best practices for IoT security and emphasizing the need for a precise vocabulary in advancing security. Additionally, [8] sheds light on companies’ challenges in adapting to technological advancements, particularly in securing smart home environments.

The importance of establishing best practices for IoT security is a recurring theme in the literature. Researchers introduce a working definition for best practices, insisting on their actionability [7]. It aligns with [9], which critically analyzes IoT security advice, stressing the need for actionable guidance to ensure proper execution. Furthermore, [10] meticulously evaluates security practices in two IoT hubs, emphasizing applying best practices to enhance security. The paper advocates for the development and implementation of best practices as a means to bolster the security landscape in the IoT domain.

Authentication mechanisms are pivotal in securing IoT devices, and several papers contribute valuable insights. For instance, TCpC [11] is a graphical password scheme to authenticate users accessing IoT resources. The paper emphasizes the scheme’s resistance to various attacks, offering advantages over traditional authentication methods. On the other hand, a One-Time Password (OTP) authentication scheme based on Identity-Based Elliptic Curve Cryptography (IBE-ECC) has been proposed by [12]. The paper addresses the limitations of existing authentication methods in the heterogeneous IoT landscape, advocating for enhanced security measures.

The vulnerability of passwords in IoT devices is explicitly addressed in [13], where the paper introduces three innovative models designed to surpass the performance of PassGAN, an initial GAN-based password prediction model. The research leverages Recurrent Neural Networks (RNNs) to improve password cracking performance, particularly with a dual discriminator structure. This paper provides practical guidance on model selection based on time constraints and computing capabilities, offering valuable insights into developing secure password-predicting dictionaries.

In the study [14], Biondi contributes to the literature by presenting a thorough security analysis of AroSheb_Jo, a hybrid Time Password (OTP) generation algorithm designed to secure data access in IoT environments. The paper reveals the algorithm's robustness against various security threats, ensuring the integrity and confidentiality of IoT data. It positions AroSheb_Jo as a realistic and efficient solution for securing data access in healthcare and other IoT applications.

The importance of conducting vulnerability assessments and penetration testing is evident in [15, 16], where researchers systematically evaluate the security aspects of IoT devices. Researchers in [15] specifically investigate the security of an IP camera, unveiling multiple vulnerabilities, including default credentials, unencrypted transmission of sensitive information, and vulnerabilities in associated Android applications. The TP-Link Tapo C200 IP camera has been used in vulnerability assessment and penetration testing to identify weaknesses, such as motion detection risks and susceptibility to DoS attacks [16].

Focusing on cloud-based systems hosted on Amazon Web Services (AWS), Aklamati's study has provided insights into the security analysis of Video Surveillance as a Service (VSaaS). The research identifies vulnerabilities within VSaaS and implements various attacks to exploit these weaknesses. A novel taxonomy is introduced to categorize attacks, offering a valuable framework for future research in the field [5].

To sum it up, the recurring themes of security challenges, best practices, authentication mechanisms, password cracking, hybrid OTP generation, vulnerability assessments, and cloud-based surveillance systems collectively contribute to the discourse on enhancing IoT security. By leveraging the insights and proposed strategies from these papers [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], it becomes evident that a holistic and proactive approach is essential to mitigate the risks associated with default PWs in IoT devices, ensuring a more secure and resilient IoT landscape.

While the existing literature introduces valuable insights into the security challenges posed by default passwords in IoT devices, including CCTV systems, there is a lack of comprehensive research that focuses on identifying the prevalent vulnerabilities and security risks related to default passwords in CCTV, analyzing the current password policies and authentication protocols used in CCTV systems, and providing recommendations to mitigate these risks. This study aims to fill this gap by conducting a qualitative investigation to understand the problem better and provide practical solutions to enhance the security of CCTV devices.

1.3 *A comparative analysis between CCTV camera brands*

Table 1 summarizes the available information on various surveillance equipment brands and their features, access controls, types of passwords accepted, and recommendations for users to enhance the security of their systems. Hikvision, Dahua [17], and Samsung Techwin [18] all advise using secure and complicated credentials to protect their surveillance equipment. At the same time, Swann [19] does not do identity management but suggests using sophisticated credentials for safety. Lorex [20] and Axis [21] recommend using rugged credentials for their surveillance equipment, especially Closed-circuit television. All brands, except for Hikam [22], suggest that users should be able to change their passwords regularly to enhance the system's security. For Hikam, it is recommended that users should contact Hikam support to inquire about password-changing options and follow their advice. All brands suggest that users should be aware of the importance of using strong and/or rugged, complicated credentials and changing passwords regularly to reduce the risk of unauthorized access and data breaches. Overall, the absence of uniform security practices and the dependence on inadequate password policies across these brands pose significant risks to user data and device integrity.

Table 1. A comparative analysis between CCTV camera brands

Brands	Access controls	Types of passwords
Hikvision	Account administration. To safeguard admission, create user identities, allocate responsibilities and privileges, and define authentication rules.	Complicated and essential passwords.
Dahua	Digital certificate, chip, and face identification authorization solutions.	Dahua does not stipulate a certain level of password. Complexity.
Swann	Swann does not do identity management.	No complicated or easy passwords. Sophisticated credentials are suggested for safety.
Lorex	Slot reviewers: Lorex sells micro Sd devices that permit or deny entry depending on a verified admission code. Theft or missing credentials may be cancelled.	Lorex suggests rugged credentials.
Axis	Entrance processors. Chip cards and secure regulation systems may be used with these computers.	Rugged credentials.
Samsung	Streaming and taped recordings, webcam adjustments, and gesture recognition notifications are available. Location tracking lets people watch their property remotely from any location.	Complicated credentials for device protection.
Hikam	Visual confirmation.	Secure, complicated credentials for memberships

2. Methods

The interview strategy's central question was: "What is the level of awareness among CCTV users about the importance of changing and using complex passwords?" This question guides the development of the interview questions, the selection of participants, and the data analysis. The study aims to understand better CCTV users' perspectives and experiences related to password security and identify potential areas for intervention or policy development to promote better password practices among CCTV users based on a qualitative interview study of CCTV systems users. The authors interviewed professional CCTV surveillance system users to answer the research question.

2.1 *Structure of the methodology*

The methodology in interview research typically consists of several vital steps that guide the entire research process. Here is an outline of the typical steps involved in conducting interview research in Figure 1:

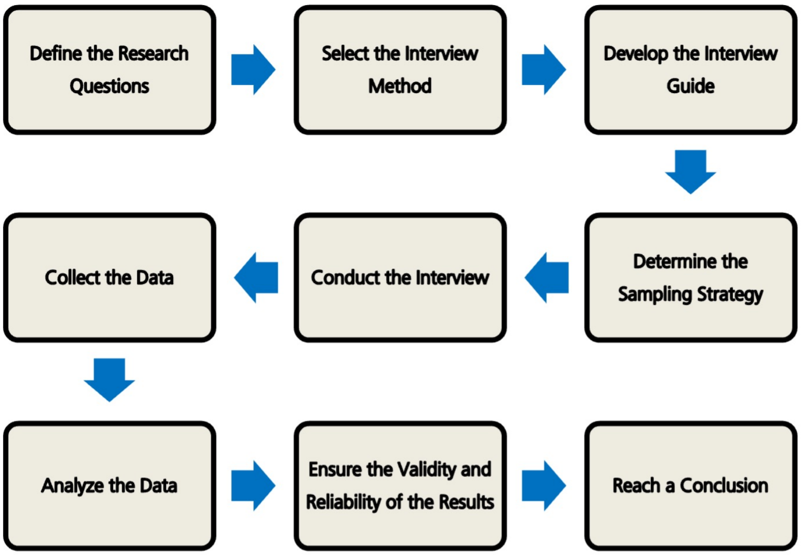
Define the Research Questions
Select the Interview Method
Develop the Interview Guide
Determine the Sampling Strategy
Conduct the Interview
Collect the Data
Analyze the Data
Ensure the Validity and Reliability of the Results
Reach a Conclusion

Figure 1. Methodology structure

Figure 1 Alt Text: A flowchart showing the stages of conducting research, from defining research questions to concluding. Each stage is connected sequentially by blue arrows.

2.2 *The sampling strategy*

The population of this study consists of individuals and organizations that use Closed-Circuit Television (CCTV). This includes a diverse range of users, such as homeowners, businesses, and public institutions that employ CCTV cameras for surveillance. For this study, the authors' inclusion criteria were individuals or organizations that use or have experience with CCTV or have knowledge and expertise in IoT or CCTV security.

Purposive sampling, a non-random sampling strategy where the researcher selects participants based on specific criteria relevant to the research question, was used for this research. In this case, we selected participants with experience using passwords to access their CCTV systems due to their relevance to the research question on password security for CCTV cameras. Qualification criteria included prior use of CCTV devices for personal and professional purposes, acquaintance with setting up and managing CCTV systems, and further knowledge of password policies. While purposive sampling may limit the generalization of the findings to the broader population of CCTV users, it allows us to focus specifically on the topic of interest and obtain in-depth information from participants with relevant experience [23].

2.3 *Data collection*

The data collection process involved gathering information using a semi-structured interview guide that included open-ended questions about CCTV users' awareness and practices of changing and using complex passwords from selected participants. The following steps were taken to collect the data: Firstly, participants were recruited using a purposive sampling strategy, and once a sample was selected, participants were invited to participate in the study. They were given information about the study's purpose, the interview process, and their rights as participants. Secondly, before the interview began, participants were asked to sign an informed consent form that explained the study's purpose and procedures, their rights as participants, and the confidentiality of their responses. Thirdly, the interview was conducted in person or over the phone, and detailed notes were taken. Fourthly, follow-up questions were asked to clarify the participants' responses or to explore the topic in more detail. Fifthly, the data collected during the interviews was stored securely and confidentially, and the audio recordings were transcribed verbatim. Sixthly, the transcribed data were analyzed using a qualitative analysis approach, where the data were coded, categorized, and themes were identified. Two or more researchers analyzed to increase reliability. Lastly, participants were asked to review and verify the accuracy of the transcripts to ensure that the findings accurately reflected their perspectives. The study gathered in-depth information on CCTV users' awareness and practices of changing and using complex passwords [24].

The questions were open-ended to determine the participants' awareness of and practices regarding system security. The questions included:

- What approach are you currently using to manage the password of your CCTV system?
- When you changed or updated default passwords, did you encounter any challenges?
- What is your level of trust in the security of your CCTV system?
- In case of security breaches, what notification method do you expect?

2.4 *Sample size*

The sample size was determined using a power analysis considering the study's expected effect size, significance level, and power. The power analysis recommended a sample size of 10 to 30 participants [25].

To select the sample, a systematic sampling strategy will be used to select the individuals that will comprise the sample, where we will select elements from a target population by randomly choosing an initial starting point and then consistently selecting sample members at a set interval from that starting point. Systematic sampling is generally more suitable than random sampling because the relevant data does not display discernible patterns. This helps minimize the risk of data manipulation that will lead to poor data quality outcomes [25]. Systematic sampling aimed to obtain a representative sample of CCTV users with experience using passwords to access their CCTV systems. The sample was selected, and participants were contacted and invited to participate. Around 10–30 participants were considered sufficient for a sample to obtain a range of perspectives on the research question and to provide a reliable estimate of the awareness among CCTV users about the importance of changing and using complex passwords [25].

2.5 *Research variables*

In interview research, variables fall into two main types: independent (manipulated by researchers to impact the dependent variable) and dependent (outcomes of interest). Independent variables, such as demographic, socioeconomic, environmental, and experiential factors, are explored to understand their influence on participants' responses. Dependent variables, like attitudes, knowledge, behaviours, and emotional reactions, are analyzed on research goals. Qualitative research introduces complexity, with variables needing to be more clearly defined and context-specific, evolving throughout the research process [26]. For this research, the types of variables that will be used are as follows (see Table 2):

Table 2. Research variables

Independent variables	Dependent variables
CCTV systems' user.	The participants' awareness about the practices of using complex passwords. The participants' level of trust in CCTV devices. Preferred method of notification of security breach. Preferred method of authentications.

2.6 *Analyze the data*

A thematic analysis approach was employed for the qualitative analysis. Thematic analysis is proper for examining user's insights, perspectives, knowledge, expertise, or beliefs from interview transcripts. It provides flexibility in data interpretation and facilitates handling large datasets by sorting them into broad themes through coding, categorizing, and theme identification. The semi-structured interviews focused on participants' awareness and practices related to changing and using complex passwords. Open-ended questions allowed a detailed exploration of their experiences. The qualitative analysis comprised transcribing audio recordings verbatim, coding segments with descriptive terms, categorizing coded segments based on similarities and differences, analyzing categories to identify overarching themes, and interpreting themes about the research question [27].

2.7 *Validate the results*

Several measures were used to validate the study results. Participants were initially required to sign an informed consent form clarifying the study's purpose, procedures, and rights. This ensured their understanding and willingness to participate. Pilot interviews were then conducted with a small group to refine questions and procedures. Data collected were securely stored, with verbatim transcription of audio recordings, ensuring accuracy—qualitative analysis involved coding, categorization, and theme identification by two or more researchers for increased reliability. During this study, several concerns were raised by participants regarding confidentiality, and those concerns were handled by ensuring anonymity and providing an explanation related to the study's purpose.

Furthermore, participants were doubtful about the usability of complex password and their lack of ability to implement the changes, which were documents for analysis. In the data review stage, the participants focused on transcript accuracy, which was solved by granting them permission to review and confirm their responses. These concerns were then added to the analysis to understand user challenges and perceptions effectively [22].

2.8 *Making the results reliable*

This research focused on bolstering the reliability of the qualitative findings through a comprehensive approach. Multiple data collection methods were employed to enhance validity and trustworthiness, embracing triangulation to compare diverse perspectives. Acknowledging potential biases, we ensure transparency in the purposeful sampling techniques and document the entire research process, fostering accountability. Striving for data saturation, information was collected until no new insights emerged, ensuring the completeness of the findings. Engaging participants in feedback loops and maintaining a detailed audit trail further validate the results. Seeking external input through discussions with colleagues and reflexive peer reviews adds rigour to the research, promoting a robust and reliable study [28].

3. Study results

Data analysis revealed critical themes related to participants' awareness and practices of changing and using complex passwords in CCTV systems. The themes entailed understanding password security, challenges in changing default passwords, perceptions of risks associated with default passwords, trust in CCTV systems' security, preferred notification methods in security breaches, and preferences for authentication methods. The results also shed light on participants' trust in CCTV systems and perceptions of associated risks with default passwords. Participants expressed concerns about unauthorized access, privacy breaches, and potential misuse of CCTV systems. Their preferred methods of notification in security breaches varied. Some favoured immediate alerts, and others preferred regular security updates.

3.1 *Demographic overview*

This study investigated the perspectives of individuals aged 25 to 47 from both genders, 54.55% female and 45.45% male, regarding the Internet of Things (IoT)-connected security cameras, as shown in Figure 2. The distribution of the participant gender shows important demographic insights that may affect security awareness. The participants, a mix of midlife professionals, technology enthusiasts, and those involved in property management, represent diverse backgrounds and technical expertise. Including individuals from various sectors and technical backgrounds provides a comprehensive understanding of CCTV security. This diversity allows for a nuanced exploration of generational gaps in cybersecurity practices. Despite differences in origin and technological proficiency, the everyday use of CCTV systems among participants establishes a shared foundation for this research. The invaluable insights from their experiences, expertise, and behaviours can inform the enhancement of more secure IoT devices and understanding of end-user behaviour linked to these technologies.

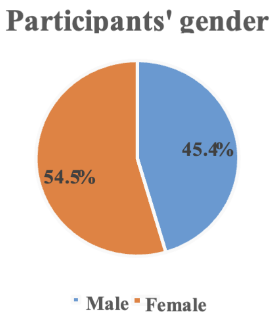

Figure 2. Participants' gender

Figure 2 Alt Text: The pie chart titled "Participant Gender" shows 54.55% female in orange and 45.45% male in blue.

3.2 *Participants' awareness*

Most respondents (85%) believe that CCTV cameras primarily serve essential security functions, such as collecting video feeds. In comparison, only 15% think they are used for more advanced purposes like position monitoring or accessing personal phone records. Although most people understand their CCTV cameras, only 40% read the device policy when purchasing a new gadget, and 60% never read it. This lack of policy awareness highlights the need to educate users about data-gathering practices and other crucial factors affecting the safety and privacy of their CCTV systems. Surprisingly, 90% of surveyed individuals admitted to not reading the rules before using their CCTV cameras, revealing a significant knowledge gap. Moreover, only 40% were required to sign a waiver and read the rules before usage, raising concerns about the communication of product policies during the onboarding process. While users are generally familiar with their CCTV camera features, there needs to be more awareness regarding data-gathering techniques, emphasizing the risk of unexpected privacy and security vulnerabilities.

3.3 *Participants practice changing and using complex passwords*

The results found that 75% of participants opt for simple passwords, such as consecutive numbers, posing a potential risk as they are easier to guess or break using brute force techniques. Additionally, 30% of individuals write down passwords, compromising their security. Alarmingly, 60% admitted to using the same password across multiple accounts, including critical systems like CCTV. This practice amplifies the risk, as a breach in one account could lead to unauthorized access in others, highlighting a crucial vulnerability in CCTV security practices. Despite these concerning trends, 90% of respondents recognize the importance of strong passwords and regular updates. Paradoxically, the majority (60% or more) express confidence in their ability to create secure passwords, a sentiment at odds with the observed prevalence of weak or repeated passwords.

Furthermore, the findings reveal a need for more emphasis on password security during consumer purchases, with only 40% actively seeking security-focused hardware. Notably, 90% of participants need more time to implement two-factor authentication (2FA) for their CCTV systems, primarily due to a need for more awareness or certainty about the setup process. This heightens the vulnerability to unauthorized access, as in Figure 3.

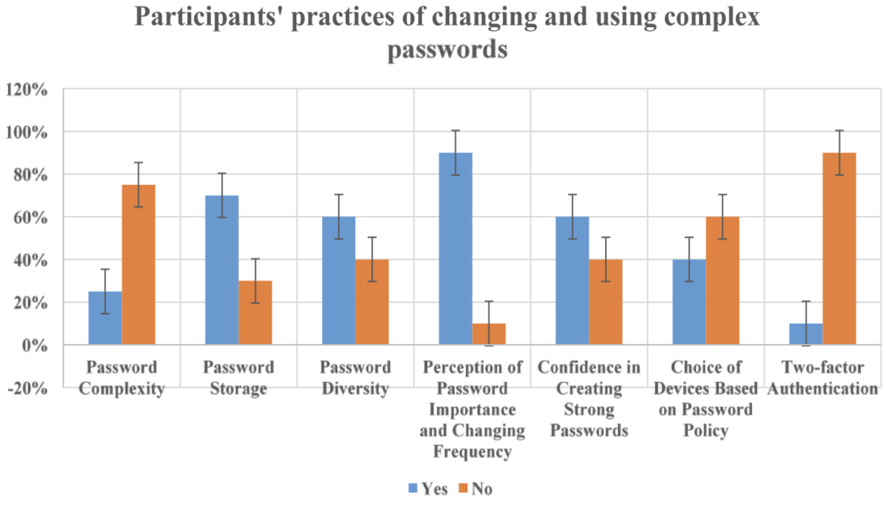

Figure 3. Participants practice changing and using complex passwords

Figure 3 Alt Text: A bar chart showing participants' practices for changing and using complex passwords. The chart is divided into five categories, choosing yes (blue bars) and no (orange bars) for each category.

3.4 *Trust in CCTV devices*

When asked which brand of CCTV cameras they prefer, 65% of respondents said they used Hikvision. The variety of products available, reasonable prices, and good quality of this brand are all selling points for them. There is no information on the precise brands the remaining 35% used or the rationale for their preferences. This result indicates that the popularity of Hikvision can be attributed in part to the high quality and variety of the brand's CCTV offerings. Almost all participants (90%) have complete faith in their CCTV systems to protect their homes, businesses, and other valuables. This high level of trust indicates that users are generally delighted with the effectiveness of their devices, and positive experiences and strong perceived reliability influence this. Only 10% of the participants reported feeling doubtful or lacking trust in their systems. Participants' faith in CCTV may be attributable to their favourable experiences or general impressions of the technology's usefulness.

80% of respondents prioritize safeguarding the CCTV system's captured and stored data (including films, passwords, and audio recordings). Conversely, 20% believe it to be less significant. This discrepancy may result from different perspectives on the dangers of data breaches and knowledge levels of what sensitive data is. This assurance may originate from familiarity with the CCTV brand in use, faith in the existing security procedures, or simply a lack of forethought about the existence of any potential data security vulnerabilities, as in Figure 4.

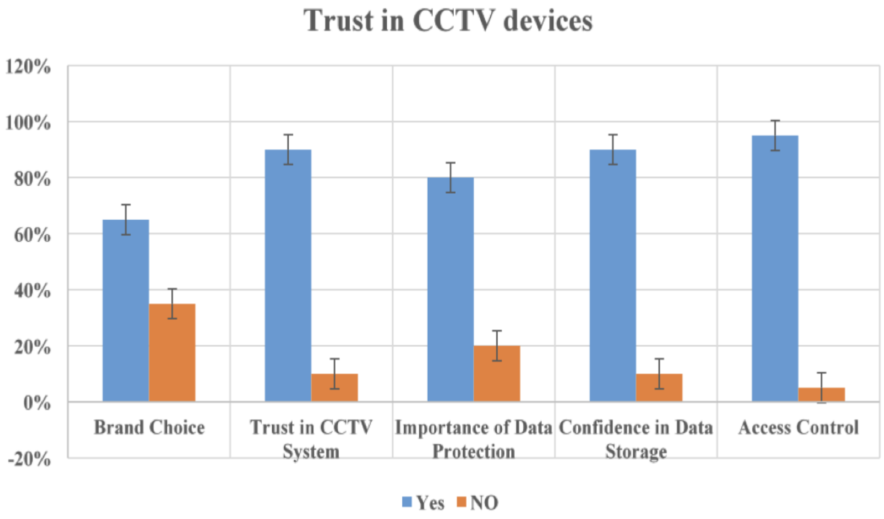

Figure 4. Trust in CCTV devices

Figure 4 Alt Text: A bar chart titled "Trust in CCTV devices" showing percentages for two categories, yes (blue) and no (orange). The categories include brand choice, trust in the CCTV system, data protection importance, data storage confidence, and access control.

Most respondents (95%) said they had implemented solid passwords and two-factor authentication to restrict access to their CCTV systems to authorized staff only. Other unidentified techniques are used by a smaller percentage of users (5%), which may indicate less secure practices or other security measures. People who participate in the study have much faith in their CCTV systems for physical security and the safety of the information they store. Although some users do not care about keeping their information secure, most do. The overwhelming trust in CCTV also concerns user satisfaction with security practices. Despite the confidence communicated, it is essential to note that depending on technology alone does not mitigate the risks related to weak password practices. This figure underscores the need for persistent education about the inherent vulnerabilities of CCTV systems and the importance of proactive security measures. The findings point to the necessity for further training and publicity on the significance and means of data protection in CCTV systems.

3.5 *Preferred notification method in case of a security breach*

As in Figure 5, only 10% of interviewees said they had heard of a security breach involving the brand of CCTV they were using, while the majority (90%) said they had not. This can point to low-security incidents or ineffective consumer communication from businesses regarding such occurrences. 90% answered that they had not received any notices of a security breach, while 10% claimed they had. This low number of warnings might be attributed to the excellent quality of the brands' security procedures or to a failure to disclose and report breaches. 90% of respondents said they have never had a hacking or security breach occur on their CCTV system. Emails were sent to the minority (10%) who had a security violation. While this information demonstrates the value of CCTV security systems, it also highlights the need for open lines of communication inside businesses during crises. When asked if they expected to be notified immediately or within 24 h after a security breach, 70% of participants said they did. The remaining 30% said they expected to be notified immediately. It illustrates that, in the case of security problems, there is a common expectation for prompt, proactive contact from CCTV system suppliers. Most participants (95%) want to be told about a security breach, be informed, and act when necessary. A tiny percentage (5%) prefers that the developer or supplier handle the matter, maybe out of a lack of awareness of the potential effects. The data did not provide a breakdown of the preferable notification methods in case of a security violation (email, phone call, text message). However, it was disclosed that 95% of participants would like to be notified. Businesses must have clear and diverse communication channels to reach their consumers effectively during such occurrences. Participants may experience few security breaches, but they strongly prefer timely alerts and open dialogue once any occur. Overall, the figure shows user preferences and the broader impact of communication practices in improving the security posture of CCTV systems. Improved notification methods can greatly impact users' perceptions of security and trust in the technology.

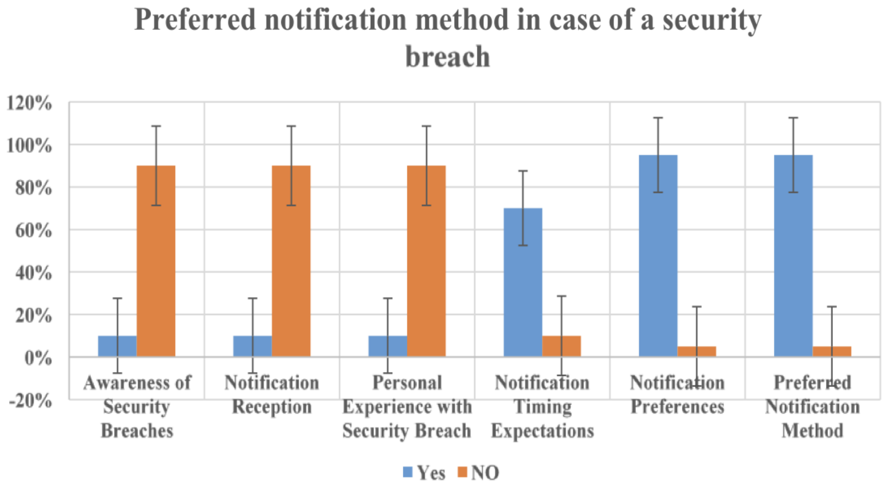

Figure 5. Preferred notification method in case of a security breach

Figure 5 Alt Text: A bar chart titled "Preferred notification method in case of a security breach" shows preferences between "yes" and "no" for the different methods: Awareness of security breaches, notification reception, personal experience with security breach, notification preferences, and preferred notification method.

3.6 *Preferred authentication method*

More than half (58%) of those interviewed participants had gotten warnings from their CCTV supplier about potentially vulnerable passwords, as represented in Figure 6; however, nearly a quarter (22%) have yet to receive them. It indicates that many users have been made aware of the importance of using robust passwords but that a sizable minority have not. It may suggest that some service providers must do more to steer their customers actively towards safe habits. One-factor authentication, which is commonly accomplished using a password, is used by most participants (90%), whereas two-factor authentication is only employed by a tiny percentage (10%). This striking discrepancy suggests a broader shift toward easier login processes prioritizing convenience over better security. Despite their present methods, all participants (100%) said they would prefer two-factor authentication if given a choice. All users would like a more secure login mechanism, but their low adoption rate may indicate a gap between user expectations and security practices. The vast majority (83%) of people have read their device policy, which means they are familiar with the basic safety rules or regulations set out by their CCTV supplier. Only 17% of people have taken these precautions. 78% of respondents favour the tried-and-true username/password option for accessing their CCTV system, while 22% favour biometric verification. Despite the widespread support for two-factor authentication, the ongoing preference for old techniques suggests a probable lack of accessible or user-friendly multi-factor authentication alternatives.

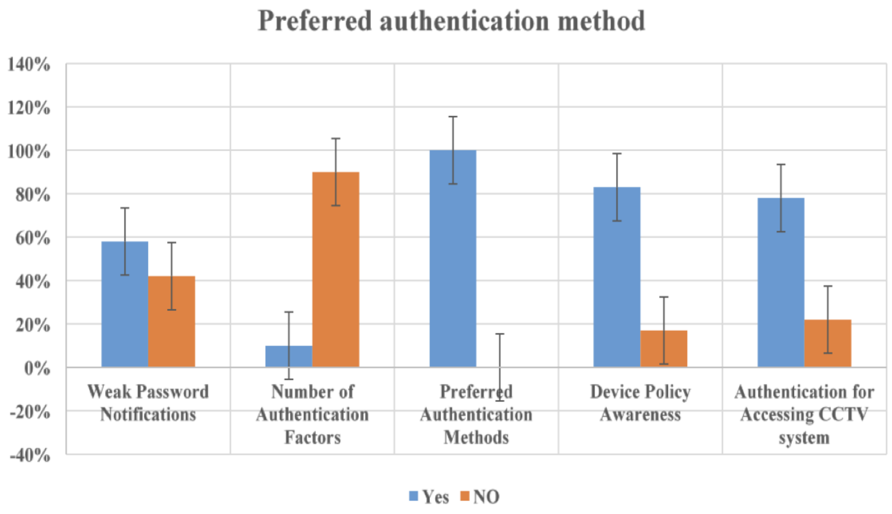

Figure 6. Preferred authentication method

Figure 6 Alt Text: A bar chart titled "Preferred Authentication Method" comparing preferences between "yes" and "no" for five methods: "Weak Password Notification", "Number of Authentication factors", "Device Policy Awareness", and "Authentication for Accessing CCTV System" The bars for "yes" are blue and for "no" are orange.

3.7 *Correlation between interview results and security analysis in CCTV cameras*

- The participants' awareness:

According to the results, 60% of consumers must read the privacy policy or terms of agreement before buying a CCTV camera. It is consistent with the results of the literature analysis, which found that customers typically need more familiarity with or comprehension of the security features, like password management, available in their preferred CCTV brand. Consumers must read and comprehend these security procedures, as companies like Hikvision, Dahua, and Swann highlight the need for user knowledge for safe passwords.

- The participants' practices of changing and using complex passwords:

75% of those surveyed admitted that weak passwords protected their CCTV systems. Even though manufacturers, including Hikvision, Dahua, Lorex, Axis, Samsung, Uniview, and Hikam, advocate or even demand strong passwords, this result is cause for alarm. It indicates a discrepancy between what CCTV manufacturers advertise as best security practices and what users do.

- Trust in CCTV devices:

Most interviewees (90%) expressed confidence in their CCTV systems. According to the brand assessments, most companies offer a wide range of security options and access management mechanisms, which may explain why they have such widespread credibility. Users may overestimate the security of these systems, as it depends heavily on how well they manage their passwords.

- Preferred notification method in case of a security breach:

The interviews revealed that 95% of respondents wanted to be alerted during a security breach, but only 10% had yet to. It is apparent from the brand study that more investigation and openness are needed from the brands regarding how they handle notifications of security breaches.

- Preferred authentication method:

100% of those polled preferred two-factor authentication, although 10 use it. The brand research reveals that most brands primarily rely on username and password authentication, with only a few, like Dahua and Lorex, offering alternatives like digital certificates or fingerprint verification; this may be owing to a lack of viable two-factor authentication choices.

4. Discussion

The outcomes of this paper have significant implications for the IoT security landscape. They offer a deeper understanding of the risks associated with default passwords in CCTV systems and provide actionable recommendations to address these vulnerabilities. The insights gained can inform the development of more secure and reliable IoT devices, ultimately enhancing individuals' and organizations' safety and privacy.

While users understand the need to use strong passwords and modify them consistently, research indicates that they often struggle to put this knowledge into practice due to the difficulty of remembering complex passwords and a lack of clear understanding of the risks associated with using weak or default passwords. This highlights the need to raise user awareness about cybersecurity issues.

Through the study, it is observed that there is a massive difference between the user preference for MFA and how many actual users use it. Despite users' strong preference for MFA, adoption remains limited due to challenges like awareness and technical barriers. Such include the need for more understanding, difficulty setting up the authentication method, and technical challenges such as poor compatibility with the system or network problems. It showcases the requirement for more technical education, more straightforward methods of setup, and better support from the manufacturers.

It was discovered that levels of trust differ significantly between different brands and characteristics. There needs to be more openness from manufacturers about how their products store and protect consumer information. Email and app alerts were the most popular choices for alerting users about security incidents. However, timely communications and user receptivity are essential to the success of such initiatives. Two-factor authentication was the most effective method since it satisfied the needs of both the researchers and the people using the system. Various approaches to access restrictions, password types, and general awareness emerged from comparing many CCTV companies. This comparison underlined the necessity for standardized security measures and standards across manufacturers of CCTV devices.

The results are consistent with previous research, which further emphasizes the need for better user education and awareness, more manufacturer openness, and the adoption of more robust security mechanisms. Moving forward, suggestions for enhancing CCTV security were made, including raising user awareness, increasing manufacturer accountability, employing password managers, routine updates, putting two-factor authentication into place, regulatory measures, promoting security research, enhancing security features, and standardizing.

CCTV systems offer significant security advantages but can pose privacy issues if not adequately protected. Producers, governing authorities, and users must collaborate to ensure these technologies are helpful and secure.

Default PWs on devices were determined to be a significant threat to home security, according to research by [29]. It is consistent with what we learned from the interviews and brand analysis: many people leave their CCTV systems' default PWs unchanged, which can be a security risk. This research backs up the worries voiced by interviewees about the dangers of using the factory-default password.

According to research by [30], default PWs are still a significant issue. 61% of apps used default or blank passwords at the initial inspection. When asked to change their password, 58% permitted an empty string, while 35% accepted only a single character. All respondents favoured two-factor authentication, although only a few manufacturers (including Dahua and Lorex) provided it. The analysis backs up the interviewees' worry that CCTV systems do not have enough cutting-edge authentication mechanisms.

Timely warnings of security breaches are crucial, according to research by [27] on IoT security. The outcomes of the interviews corroborate this, showing that the vast Preponderance (95%) of people want to be informed when a security breach occurs. CCTV brands should address the report's finding that many IoT devices, including CCTV systems, do not give sufficient notification choices. In essence, compared to previous studies, there is a widespread problem with the security of various home security equipment, including CCTV systems, the use of default passwords, the absence of sophisticated authentication mechanisms, and insufficient notification systems. The interview results and the brand analysis corroborate the magnitude and relevance of these worries.

4.1 *Prevalent vulnerabilities and security risks linked to default PWs in CCTV (RQ1)*

The qualitative data analysis revealed several prevalent vulnerabilities and security risks associated with using default passwords in CCTV systems. First, it showed that the interviewees consider Default Passwords weak and predictable. They unanimously agreed that these passwords are easy to guess and are often shared across multiple devices, making them highly susceptible to unauthorized access.

It also revealed the difficulty of changing the default passwords. Many CCTV users, particularly those with limited technical expertise, find it challenging to modify the default PWs, leaving their systems vulnerable to threats.

In addition, the general lack of user awareness about the security risks of default passwords fails to implement proper password management practices.

The study also revealed that the inadequate security measures in CCTV systems often lack robust security features, such as multi-factor authentication, to complement passwords and enhance the overall security posture.

4.2 *Forensic implications of breaches caused by default passwords*

The study highlights that breaches resulting from default passwords result in challenges for digital forensic investigation because of the predictable nature of these credentials. For instance, the study found that 75% of the participants used simple and guessable passwords, such as consecutive numbers. In comparison, 60% used the same passwords across different accounts, including their CCTV systems. These practices make it difficult to guess about the individual behind unauthorized access because multiple individuals and devices share similar default credentials. This makes it challenging to connect maliciously to a specific person because of the need for the uniqueness of a password.

The majority of forensic investigations mostly rely on IP address tracking, authentication logs, configuration files, and timestamps to distinguish the origin of the breach and contrast a timeline of the attack. However, the CCTV fails to give a thorough logging mechanism for extensive analysis. For example, the study revealed that 90% of the participants had not used two-factor authentication, and 58% of others had never received any warning about weak passwords from CCTV suppliers. The findings indicate systematic problems, improper logging, and notification systems result in sensitive forensic evidence going unrecorded, impacting the scope of forensic analyses.

The attackers also use obfuscation methods such as proxies or identity or location masking to make forensic analysis hard. Moreover, the limited ability of standardization in logging practices among different manufacturers makes it more complicated. For example, some devices offer essential information, while others do not provide necessary details, such as failed login attempts. This lack of consistency results in loopholes in data trials, which undermines the forensic investigation [26, 27].

The insights of the qualitative analysis showed that the need for more user awareness about password practices further increases forensic challenges. At least 90% of the participants in the research didn't read device policy or security recommendations, which resulted in bad password hygiene and ineffective security configurations. Without the implementation of effective forensic methodologies—such as synchronized timestamps, encrypted log storage, and advanced anomaly detection systems, the investigators face challenges linking the breaches to default passwords. Addressing these points is critical for improving forensic analyses' reliability and comprehensive cybersecurity practices.

Forensic investigators should endorse enhanced logging means on CCTV and similar devices to ensure complete capture of critical information, such as failed login attempts. Two-factor authentication should be enforced across all devices to add a layer of security against unauthorized access. Standardizing logging practices across manufacturers is necessary to reach consistency in data collection, enabling more effective investigations. Raising user education on password and security best practices is required, as it increases awareness of the significance of modifying default passwords and adopting strong password policies. Further, investigators should leverage advanced forensic approaches, such as synchronized timestamps and encrypted log storage, to improve evidence integrity. Finally, cooperation with device manufacturers is critical to highlight the essential user notifications about weak passwords and vulnerabilities, enhancing overall cybersecurity resilience.

4.3 *Current password policies and authentication protocols used in CCTV (RQ2)*

The findings identified inconsistent Password Policies used by CCTV manufacturers and service providers vary significantly, with some companies providing clear guidance on password management. In contrast, others have more lenient or inadequate policies.

The analysis showed that companies like Dahua and Lorex have progressed by incorporating strong password policies and multi-factor authentication (MFA). Furthermore, they have also incorporated biometric authentication and time-sensitive one-time passwords (OTP) to improve the security of their product. Moreover, Lorex has made a system that periodically asks the users to keep updating their passwords, which results in reduced risks of credentials and reuse of passwords. While on the other hand, manufacturers like Axis and Hikvision only rely on default password-based systems. The attackers can make use of these vulnerabilities to exploit the security measures. Hikvision, despite being popular (chosen by 65% of participants in this study), provides an MFA, which is optional, and its products are based on weak password-based systems. The dependence on only the optional upgrades makes many its users exposed and unable to upgrade to advanced features. On the other hand, Axis CCTV has bound MFA ability, and during the initial step, it allows the incorporation of default passwords, which increases the risk of breaches.

Another critical difference lies in notification systems. Manufacturers like Dahua have implemented comprehensive mechanisms to alert users about weak passwords, suspicious login attempts, or outdated security configurations. These alerts provide actionable insights for users, enabling them to address vulnerabilities promptly. However, manufacturers like Hikvision and Axis provide limited notification systems, reducing users' ability to respond effectively to emerging threats. Table 3 summarizes the practices employed by major CCTV manufacturers based on the insights from the conducted study and the literature review.

Table 3. Comparison of practices of major CCTV manufacturers

Manufacturer	Strong password enforcement	Multi-factor authentication (MFA)	Password change notifications	Default password use
Hikvision	Optional	Optional	Limited	Common
Dahua	Mandatory	Available	Comprehensive	Rare
Lorex	Mandatory	Available	Limited	Rare
Axis	Optional	Limited	Comprehensive	Common

The study indicates that there is limited use of advanced authentication, and most CCTV systems rely on basic password-based authentication, with limited adoption of more secure authentication methods, such as two-factor or multi-factor authentication. In addition, the lack of industry-wide standardization or guidelines for password policies and authentication protocols in the CCTV domain will also lead to a fragmented and inconsistent security landscape. These inconsistencies directly influenced the participant's trust. They indicated higher confidence in the brands with enforced security protocols and robust notification systems, emphasising the critical link between manufacturer practices and participants' perception of device security.

4.4 *Recommendations for mitigating the risks of default passwords in CCTV (RQ3)*

The study emphasizes several key areas where improvements in security practices and user experiences are crucial for developing robust CCTV systems. To improve the overall security posture of IoT devices, especially in the realm of CCTV cameras, developers should consider the following recommendations:

- **Mandatory Two-Factor Authentication (2FA)**

Given users' unanimous preference for two-factor authentication, developers should prioritize integrating 2FA as a required security feature. This will significantly enhance the authentication process and fortify the overall security of CCTV systems.

- **Educational Initiatives**

Develop comprehensive educational programs targeting end-users to raise awareness about the significance of using strong and unique passwords. Emphasize the risks associated with default or weak passwords through user-friendly campaigns and guidelines.

- **Transparent Communication**

Establish clear and transparent communication channels between CCTV manufacturers and end-users. Provide regular and detailed notifications about security breaches, ensuring users are promptly informed and empowered to take necessary actions.

- **Biometric Authentication Options**

Acknowledge the user preference for biometric verification and consider expanding authentication options to include biometric features. This could enhance the user experience and provide an additional layer of security.

- **Enhanced Default PW Policies**

Collaborate with regulatory bodies to establish stringent default PW policies for CCTV devices. Encourage users to configure distinctive PWs during the starting configuration, mitigating the risk associated with factory-default passwords.

- **Continuous Software Updates**

Implement a robust and user-friendly system for regular software updates. This ensures that users have access to the latest security features, bug fixes, and improvements, reducing vulnerabilities associated with outdated software.

- **Collaboration for Standardization**

Engage in collaborative efforts within the industry to establish standardized security measures and protocols for CCTV devices. This will provide a unified approach to addressing security concerns across different brands and models.

- **User-Friendly 2FA Implementation**

Simplify the implementation of two-factor authentication to encourage widespread adoption. Strive to make 2FA user-friendly, reducing barriers for users needing help with the process.

- **Use of Password Managers**

Password managers should be encouraged since users may need help remembering complicated passwords. Password managers improve safety by generating and storing strong passwords in an encrypted format. A device's security can be significantly improved if users are encouraged to update their firmware frequently. Updates frequently include security patches to remedy any gaps in protection.

- **Manufacturer Responsibility**

Producers should do more to guarantee their products' safety. The data gathered, intended use, and retention period should all be spelt out in a transparent and readily available policy. During setup, users should be prompted to change default passwords on the devices. They should consider adding further layers of protection, such as two-factor authentication and encrypted data storage.

Incorporating the recommendations mentioned above allows CCTV manufacturers to develop more secure CCTV cameras that consequently contribute to a safe and secure IoT infrastructure. Moreover, the recommendations increase the authenticity and practicality of IoT systems using CCTV-based surveillance systems.

5. Conclusions

The study aimed to gain insight into users' perspectives on CCTV equipment security, focusing on password management, user trust in CCTV cameras, preferred intrusion notification channels, and authentication preferences. In addition, the study compared the different procedures and functions of popular CCTV manufacturers. The study provides valuable insights into the vulnerabilities and security risks associated with default passwords in CCTV systems, a vital component of the broader IoT landscape. By identifying prevalent risks, analyzing current password policies and authentication protocols, and recommending best practices, this research enhances the security of CCTV devices and promotes more secure IoT technologies. The findings of this study will inform device manufacturers, security professionals, and policymakers in their efforts to mitigate the risks posed by default passwords and foster a more secure and trustworthy IoT ecosystem. In conclusion, the study adds to the current conversation on CCTV security and provides stakeholders with a framework for improving the security and efficiency of these tools.

6. Future work

This research was carried out at a particular location and societal setting. Users' attitudes and behaviours regarding password security and data privacy may be influenced by various variables, including cultural, social, economic, and even legal concerns. Therefore, future studies must consider investigating these factors in different spatial and cultural settings. Research bridging cultures or comparing places at various stages of technological development might fall under this category. The findings of such an investigation would be both culturally nuanced and generally relevant because of their global scope. Research should be done in the future to learn about certain brands' security features and the benefits or drawbacks they present. Furthermore, other up-and-coming brands may be added to further research.

- CCTV equipment was the main emphasis. Future studies may broaden the scope to incorporate other IoT devices, painting a complete picture of the IoT security environment.
- The current norms and regulations concerning CCTV and IoT security may be further examined in future work. This may help to identify problem areas and give policymakers suggestions for fixing them.
- Security measures change along with the development of new technologies. New technologies like AI and blockchain may improve CCTV security in the future, which might be the subject of more study.

- Studying how training programs affect users' knowledge and behaviour regarding CCTV safety would be interesting. Such findings suggest the best strategies for raising user awareness and encouraging safer behaviours.
- Integrated authentication standards and easy-to-implement the Multi-Factor Authentication (MFA) solutions to address the critical need for easy-to-use security standards. Future work should rely on finding the reason behind the low adoption rates of MFA despite its being preferred by users. A mixed approach, consisting of specific surveys and interviews, can be used to distinguish factors such as compatibility issues, behavioral perceptions, technical awareness, and ease of use. The result gained from such work will help the manufacturer design more user-friendly CCTV systems that offer simple setup guidance with improved compatibility.

For the limitations, the study lacks an in-depth analysis of different password policies and authentication protocols. Future work should also focus on quantitative methods, such as statistical analysis of user compliance with security protocols, such as the number of times the default passwords were changed or the frequency of breaches due to default passwords across different CCTV models and geographical locations. Furthermore, incorporating data from real-world breaches will result in more actionable metrics, such as the mean time to breach. Using such quantitative analysis will complement the qualitative data, improve the finding's reliability, and provide a broader understanding of default PW risks in CCTV devices.

Data availability statement

The data supporting this study's outcomes are obtainable on inquiry from the first author.

Conflict of interests

There is no conflict of interest declared by the authors.

References

[1] E. L. Piza, "The history, policy implications, and knowledge gaps of the CCTV literature: Insights for the development of body-worn video camera research," *Int. Crim. Justice Rev.*, vol. 31, no. 3, pp. 304–324, 2021.

[2] K. Daimi, G. Francia, L. Ertaul, L. H. Encinas, E. El-sheikh, *Computer and Network Security Essentials*. Heidelberg, Germany: Springer, 2018.

[3] J. Anand, A. Sivanathan, A. Hamza, H. H. Gharakheili, "PARVP: Passively assessing risk of vulnerable passwords for HTTP authentication in networked cameras," in *Proc. 2021 Works. Descript. Approaches IoT Secur. Netw. Appl. Config.*, Virtual Event, Germany, Dec. 7, 2021.

[4] P. W. Khan, Y. Byun, and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, pp. 484, 2020.

[5] D. Aklamati, B. Abdus-Shakur, and T. Kacem, "Security analysis of AWS-based video surveillance systems," in *Proc. 2021 Int. Conf. Eng. Emerging Technol. (ICEET)*, Istanbul, Turkey, Oct. 27–28, 2021.

[6] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet Things*, vol. 14, p. 100129, 2021.

[7] C. Bellman and P. C. van Oorschot, "Best practices for IoT security: What does that even mean?" *arXiv*, 2020, arXiv:2004.12179.

[8] Z. Shouran, A. Ashari, and T. Priyambodo, "Internet of things (IoT) of smart home: Privacy and security," *Int. J. Comput. Appl.*, vol. 182, no. 39, pp. 3–8, 2019.

[9] D. Barrera, C. Bellman, and P. Van Oorschot, "Security best practices: a critical analysis using IoT as a case study," *ACM Trans. Priv. Sec.*, vol. 26, no. 2, pp. 1–30, 2023.

[10] B. Momenzadeh, H. Dougherty, M. Remmel, S. Myers, L. J. Camp, “Best practices would make things better in the IoT,” *IEEE Secur. Priv.*, vol. 18, no. 4, pp. 38–47, 2020.

[11] P. Matta and B. Pant, “TCpC: a graphical password scheme ensuring authentication for IoT resources,” *Int. J. Inf. Technol.*, vol. 12, pp. 699–709, 2020.

[12] V. L. Shivraj, M. A. Rajan, M. Singh, P. Balamuralidhar, “One time password authentication scheme based on elliptic curves for internet of things (IoT),” in *Proc. 2015 5th Nat. Symp. Inf. Technol.: Towards New Smart World (NSITNSW)*, Riyadh, Saudi Arabia, Feb. 17–19, 2015.

[13] S. Nam, S. Jeon, H. Kim, J. Moon, “Recurrent GANs password cracker for IoT password security enhancement,” *Sensors*, vol. 20, no. 11, p. 3106, 2020.

[14] R. Shantha, K. Mahender, A. Jenifer, “Security analysis of hybrid one time password generation algorithm for IoT data,” *AIP Conf. Proc.*, vol. 2418, p. 030021, 2022.

[15] P. A. Abdalla and C. Varol, “Testing IoT security: The case study of an IP camera,” in *Proc. 2020 8th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 1–2, 2020, Beirut, Lebanon.

[16] P. Biondi, S. Bognanni, and G. Bella, “Vulnerability assessment and penetration testing on IP camera,” in *Proc. 2021 8th Int. Conf. Internet Things: Syst. Manag. Secur. (IOTSMS)*, Gandia, Spain, Dec. 6–9, 2021.

[17] CCTVdirect, Dahua Technology Review and Features. Accessed: Jun. 30, 2022. [Online]. Available: https://cctvdirect.co.uk/blogs/industry-news/dahua-review.

[18] G. Matuszek, “CCTV systems—technological and legal aspects. The present and the prospects for future,” *Zeszyty Naukowe SGSP/Szkoła Główna Służby Pożarniczej*, vol. 73, pp. 317-338, 2020, https://doi.org/10.5604/01.3001.0014.0784.

[19] T. Henderson, T. Swann, and J. Stanford, “Under the employer’s eye: electronic monitoring and surveillance in Australian workplaces,” 2018. Accessed: Nov. 21, 2018. [Online]. Available: https://goo.su/4689B1.

[20] S. S. Khan, P. K. Mishra, N. Javed, B. Ye, K. Newman, A. Mihailidis, A. Iaboni, “Unsupervised deep learning to detect agitation from videos in people with dementia,” *IEEE Access*, vol. 10, pp. 10349–10358, 2022.

[21] N. Kalbo, Y. Mirsky, A. Shabtai, Y. Elovici, “The security of IP-based video surveillance systems,” *Sensors*, vol. 20, no. 17, pp. 4806, 2020.

[22] T. Subarsyah, “Korespondensi Analytical Descriptive Study of Article 363 of the Criminal Code: Optimization of Law Enforcement for the Crime of Motor Vehicle Theft,” 2022. Accessed: Jun. 30, 2022. [Online]. Available: http://repository.unpas.ac.id/60999/1/Gmail-Korespondensi%20Baltic-Subarsyah.pdf.

[23] V. O. Etta, A. Sari, A. L. Imoize, P. K. Shukla, M. Alhassan, “[Retracted] Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique,” *Mobile Inf. Syst.*, vol. 2022, no. 1, p. 7936236, 2022.

[24] J. W. Creswell and C. N. Poth, *Qualitative Inquiry and Research Design: Choosing among Five Approaches*. Thousand Oaks, CA, USA: Sage Publications, 2016.

[25] J. M. Morse, “Critical analysis of strategies for determining rigor in qualitative inquiry,” *Qual. Health Res.*, vol. 25, no. 9, pp. 1212–1222, 2015.

[26] N. L. Leech and A. J. Onwuegbuzie, “Beyond constant comparison qualitative data analysis: Using NVivo,” *School Psychol. Quart.*, vol. 26, no. 1, p. 70, 2011.

[27] M. O’Reilly and N. Parker, “’Unsatisfactory Saturation’: A critical exploration of the notion of saturated sample sizes in qualitative research,” *Qualitative Res.*, vol. 13, no. 2, pp. 190–197, 2013.

[28] M. Shin, W. Paik, B. Kim, S. Hwang, “An IoT platform with monitoring robot applying CNN-based context-aware learning,” *Sensors*, vol. 19, no. 11, p. 2525, 2019.

[29] Y. D. Ko and B. D. Song, “Complementary Cooperation of CCTV and UAV Systems for Tourism Security and Sustainability,” *Sustainability*, vol. 13, no. 19, p. 10693, 2021.

[30] B. Knieriem, X. Zhang, P. Levine, F. Breitinger, I. Baggili, “An overview of the usage of default passwords,” in *Proc. Digit. Forensics Cyber Crime: 9th Int. Conf. ICDF2C 2017*, Prague, Czech Republic, Oct. 9–11, 2017.