International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531
(Print & Online)

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied


---

# Usable Privacy Mechanisms in Home SecurityCamera Systems

Muhammad Dahiru Liman[a]*, Binta Ali Shuwa[b], Muhammed Abubakar[c], Salamatu Osanga Ibrahim[d]

[a,d]*Department of Computer Science, Faculty of Computing, Federal University of Lafia, P.M.B. 146, Lafia, Nasarawa State, Nigeria*

[b]*Department of Cyber Security, Faculty of Military Sciences and Interdisciplinary Studies, Nigerian Defence Academy, P.M.B 2109, Kaduna, Nigeria*

[a]*Email: mlimand76@gmail.com,* [b]*Email: bintashuwa@gmail.com ,* [c]*Email:engrelmoh@gmail.com*
[, d]*Email: siosanga@gmail.com*

**Abstract**

IoT is the interconnection of People and things. When our home is connected to IoT devices it is referred to as smart home. The idea behind smart home is to make life easier such that there is little human intervention. The IoT devices in our smart home exchange data for storage and processing. This exchange of data leads to users concerns on data security and privacy. In this work, we implemented home security camera systems in such a way that the data is encrypted first before being sent to the cloud in a very simplified and almost automatic encryption process. This implementation was done putting in mind usability. A questionnaire was used to gather results on users' perception about the system. The user study conducted yielded positive result.

***Keywords:*** IoT; Smart Home; Usability; Security; Privacy; Camera; Prototype.

## 1. Introduction

This work aims to implement home security camera systems in such a way that the data is encrypted first before being sent to the cloud in a very simplified, almost automatic encryption process. Computer security can be seen in terms of CIA (confidentiality, integrity, and availability) [1,2].

---

* Corresponding author.

Confidentiality in this context means unauthorized people or entities should not have access to information they are not supposed to access [3]. In smart homes, users don't want any other person to have access to their data except themselves; the company managing the data is not exempted. Integrity means only authorized users can modify their data. Availability in this context refers to data being available for the owners to access. In this case study, the user can request his data at any convenient time. When the user requests his data the user wants it to be available (availability), the user wants the data to be accurate (Integrity), and also the user wants the data to be accessible by only him (Confidentiality). A system is considered usable if dangerous errors are not made by users, and users can do things without having difficulty, users are okay with the interface and at the end of the task users are satisfied with the system [4]. There is often a trade-off between usability and security. Sometimes poor usability can lead to poor security [5].

The notion of security is not just for computers, in real life people want to be protected from burglary and thieves. One way people explore to make their homes safe is to put security cameras in their homes. These cameras take video coverage of whatever is happening in that house. With the Internet of things, this even makes it easier, since the security cameras are connected with other devices and the data (pictures) captured are being sent to the cloud for storage. IoT has helped in making smart cities. In smart cities, we have automated homes. We have a lot of IoT applications. IoT is applied in industries, enterprises, and consumers [6]. In this work, IoT is considered in terms of consumers. IoT in terms of consumers here is regarded as smart homes. Smart homes have things like electronic devices, lighting devices, heating, and other smart appliances that can be monitored from a distance either with smartphones or computers [6].

Many devices are connected to the internet through IoT, this means that with IoT lots of data are being generated from users. These Data need to be protected. Data exchange by different devices through networks and other devices connected in IoT needs to be safeguarded; this technology is known as IoT security [6]. Users' personal information also needs to be protected; this is referred to as IoT privacy [6]. User privacy and security are major concerns. Users want their data to be given much protection from attackers and against any threat. Due to the nature of the connection of devices in IoT, only one vulnerability is needed by an attacker to change all the data and make it not usable [7]. Lack of device updates by manufacturers can make them vulnerable to attack. Another issue of concern is the fact that the personal data of individuals can be sold out by companies running these devices [6]. Hence, in this work we consider several measures to tackle these user concerns. The user can encrypt their data from their devices before it reaches the company managing it. Users can also request for their data to be erased from the company database.

## 2. Related Works

According to Perera and his colleagues [8], IoT is the connection of anything with any object at any time through any network path to things and people. These devices when connected become recognizable, addressable, and locatable [9]. These connections can be applied to any of the following areas health care, transportation, smart city, and smart home [10]. When things and people are connected to any of the mentioned areas through services and networks, there is usually an exchange of data to (data center) and from (smart home, smart city, etc.) for storage and processing [11]. These data that are sent for processing and storing are user data.

These data can include CCTV footage, images, voice recording, etc [12, 13]. When these data are sent there is a possibility of interception. This is a major problem for the user due to security and privacy issue. Some of the security concerns highlighted by [11] are stealing or change of information, viruses [1], unauthorized access to data, unauthorized access to service, denial of service attacks, attacks on the availability of information, network security, etc. Some of the privacy issues are privacy in the device, storage, communication, and processing [11]. However, Lin and his colleagues [1] have a different view about the Smart home security and privacy challenges. According to them, the major challenge is the Smart home user that doesn't know how to configure the devices. They suggested that auto management can help to solve this problem. Auto management involves auto-configuration and automatic update of firmware and system software. The authors made good suggestions and we think by removing the burden of configuration and updates from the user the security and privacy of user will be improve. Pawar and his colleagues [13] provide home security using Raspberry Pi. The security issues considered are gas leakage protection, glass break alert, door security, and fire security. Whenever any of the security issues occurred an alert is sent to the owner's email to notify him/her. Furthermore, images of the intruder are also captured and sent to the owner's email.

A smart home is expected to meet the following security goals confidentiality, integrity, availability, authenticity, authorization, and non-repudiation [14]. When these goals are not met then there is a security problem. To achieve the above goals, for Confidentiality, the user wants to be assured that only authorized individuals will have access to their data. For Availability, the user wants data and services to be available when needed. For Integrity, the user wants the data he/she is using to be correct and not altered, this can be achieved by using a digital signature and hash function[15,16]. For Authentication, smart devices should be authenticated; this can be achieved by using a certificate [16,17]. For Authorization, the user's rights should be defined and access control should be specified [17]. When any of the above goals is compromised then it becomes a security threat. This security threat can be a Passive attack or an Active attack [2]. When the attacker is trying to get insights from the information without altering it, the attack is considered passive attack. Passive attack usually comes in form of traffic analysis or eavesdropping. However, when the attacker altered information or data it is considered Active attack. Active attack include malicious software, denial of service, message modification etc.

According to Shouran and his colleagues [2], the major problem of security in a smart home is a lack of security awareness among users of smart home devices. They suggested that users of smart devices should change the default password and deactivate any feature that is not in use. This is a good suggestion from the authors; however, it will be better if users are made aware of how important it is. I t will also be good if the process is easy for the users to carry out the task. This can be achieved by making the system usable. According to Chhetri and Motti, 2/3 of users which is equivalent to 67% specified their privacy concerns as follows discovery and disclosure of personal data, security of data stored in the cloud, tracking of a user, and smart home devices listening to users' conversations [18]. Personal data can be discovered and disclosed or even sold. Personal data stored in the cloud are at the risk of hacking by hackers. In Sivaraman and his colleagues [19], some smart home devices were tested to measure their security. The authors created four different fictitious scenarios. In the first case, they found that there was a man in the middle attack, and the information (video and motion sensor information) was not encrypted which means the attacker can know the content. In the second case, the smart home users make use of an email link that downloaded malware to their computer. This malware sent their

information to the attacker. In the third case, remote malware was used by a neighbor to attack the Wi-Fi traffic. In the fourth case, a hacker used password-cracking software to crack users' passwords and this was possible because they didn't change their default password and username. In the first scenario, if the information were encrypted it wouldn't have been easy for the attacker to know the content. In the second scenario, there is lack of user awareness on social engineering especially phishing. In the fourth scenario, simple change of default password and username name would have prevented the attack

In Plachkinova and his colleagues [20] analysis, five emerging trends were discovered. These include digital and forensic challenges, infrastructure vulnerabilities, privacy violations, risks for smart home devices, potential for remote security breaches. The privacy concern they highlighted has to do with selling users' data to third parties.

**Limitations**

From the above analysis the limitations identified are lack of user awareness [2,19], user don't know how to configure smart home devices [1], and information not encrypted [19]. To solve these problems there is need to create a system that is usable and secure by making the encryption process automatic and simple. A system that is usable is secured [5]. If it is not usable then users can make dangerous mistake.

**3. Concept and implementation**

This mechanism implements the home security camera system in such a way that the data is encrypted first before the data is transferred onto the cloud by the IoT Company for storage. It is designed as an application that can run on mobile devices such as android and IOS devices. This model requires that data should be stored on an interval of 24hours of which the user sets his preferred prompt time according to his schedule during the installation of the security system. The encryption key is also set up during the initial configuration of the system. The default encryption algorithm for the system uses Advanced Encryption Standard (AES) and the single encryption key is automatically generated and stored on the user's mobile device in a folder of his choosing which must be offline for security reasons.

After each 24-hour interval, the IoT system sends a signal to the user's device asking him whether he wants to transfer the data for that time frame for storage or not. If the user clicks "NO", the prompt quits and the data is discarded and not saved. This gives the homeowner the added capability to choose whether or not to save a particular data generated from his home, thereby further suiting his privacy needs.

If he answers "YES", i.e., he wants to save the data generated in the past 24hours, the system then prompts him to encrypt the data by popping up a window with the encrypt button on it. Once the user clicks the "ENCRYPT" button, his file explorer is opened for him to select the file that contains the encryption key. Once he selects the correct file, the data automaticallygets encrypted and transferred for storage.

The time between prompting the user to choose whether to save the data or not and the task of encrypting the data is estimated to be 20seconds for an average user who is conversant with the use of mobile applications. User studies will also be conducted to measure the actual time it takes different categories of users to complete the

process. On the other hand, if the user demands to be sent the data for a particular day or days, the data is sent in the encrypted form it was saved and the user can choose the "DECRYPT" option. His file explorer opens, and he will also need to navigate to the location where he saved the file containing the encryption key. Once he selects the file, the data gets decrypted and he can view the video footage on his device or any other device he chooses. This implementation is tailored towards finding a balance between privacy, usability, and security.

### *3.1. Argument for Security*

The first argument in favor of security for this implementation is that the security footage is first encrypted before it gets to the IoT Company and sent to the cloud for storage, unlike traditional security camera systems. Secondly, the user's encryption key is randomly generated during the configuration process. Therefore, the company itself cannot predict user keys. Thirdly, the user's encryption key is stored offline on his mobile device and not on any central database that can be accessed by some staff in the company or compromised by a hacker. Also, if there's an event where a user loses his mobile device, he can click the "lost phone" button and a new encryption key is sent to his new device while the former encryption key gets disabled immediately. The "lost phone" recovery process requires 2 Factor Authentication not just the usual authentication to avoid impersonation. Furthermore, the application itself requires login authentication before usage.

### *3.2. Arguments for Usability*

Firstly, our system allows the user to choose a convenient time to receive the daily prompt for data encryption or deletion so that the prompts won't encroach into his busy periods and become "annoying". Secondly, the user doesn't need to know the details of the encryption or decryption process. All he needs to do is store the generated key in a convenient folder and when he needs to encrypt or decrypt, navigate to that folder and select the file. Also, since the system uses a notification feature, it reduces the cognitive load of the user in terms of always having to remember to log in to the app to do the encryption or deletion.

### *3.3. Arguments for Privacy*

The privacy of the user is further improved since the IoT Company only gets the security footage in an already encrypted format and also doesn't have the encryption key. Also, the user gets to choose which data to send for storage and which to delete immediately, before it gets to the company. Even when he wants to view particular footage, he can easily decrypt it and view it on his device.

### *3.4. The Prototype*

The paper prototype application is based on securing CCTV footage that is captured within smart homes. It aims to make the process of encrypting such data easier. It helps the users to access, manage and update the data conveniently. It ensures that the security being provided makes the data resistant to misuse.

### *3.4.1. Home screen*

The home screen displays the various actions that the application is capable of. The user may select any of the tabs, based on the required action they want to perform.


**Figure 1:** Home screen.

### *3.4.2. Upload/Encrypt*

The file is uploaded and automatically encrypted once the upload file button is clicked. The key generated is saved within a passcode-protected folder of the user's choosing. This tab has a dual function of uploading and encrypting data at the same time. This ensures that the burden of encryption on the user is lifted, making the system both secure and easy to use. Upon clicking the upload/encrypt tab a file explorer is opened for the user to choose the location of their stored encryption key. Upon selection of the encryption key, data for the past 24 hours is encrypted and transferred to the IoT Company for storage.

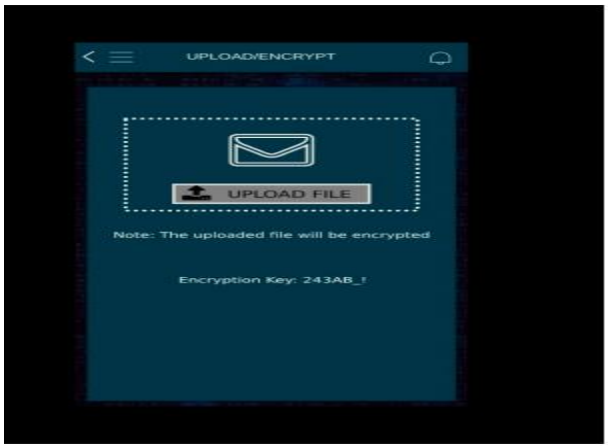


**Figure 2:** Upload/Encrypt.

### *3.4.3. Download/Requests*

The user can request to download the data from a particular date and time frame. Previously downloaded data is also given within this tab. After clicking on the tab, the page shows two buttons, "Enter date of data to download" and "Enter timeframe of data to download". The user chooses the start and end date as required, if the user requests for data from just one day, then the start and end date should be the same. The user then enters start and end times for data required and finally click on "OK" to retrieve data. Encrypted requested data is then downloaded after which the user has to decrypt it using his/her key to have access.

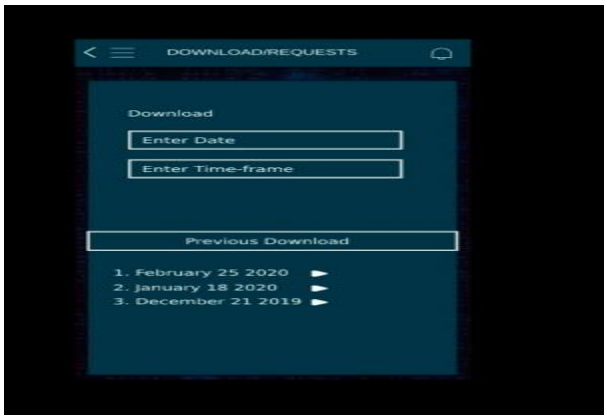


**Figure 3:** Download/Request.

### *3.4.4. Data Analytics*

The data analytics tab helps the user to access and retrieve upload and download statistics. It also has an option for the user to clear the entire log present and even access archives. When a user clicks on this tab, a page that shows his /her logs of data uploaded, data requested, and data deleted is displayed. This tab also provides the user with a graphical representation with relevant statistics of how often they have used the various features (i.e. upload and download) with a weekly report. Users can select a particular activity and delete it or he /she can click on the clear log button to clear all activities from the log.


**Figure 4:** Data Analytics.

### *3.4.5. Configuration*

This tab mainly deals with the general settings of the application. It also deals with the daily notification setup. After clicking on the tab, the page shows two tabs, "Configure notifications" and "General settings" On clicking "Configure notifications", the user chooses the timeframe for which data upload notifications shall be prompted on the user's device for:

- Discard data option
- Encrypt/upload option

"General settings" include data and privacy information. User can change their privacy settings here.


**Figure 5:** Configuration.

### *3.4.6. Configure Notifications*

This tab allows you to set up the daily notification prompt on your device. The prompt may be used for discarding data or uploading and encryption.


**Figure 6:** Configure notifications.

### *3.4.7. Legal Tab*

This tab mainly entails all of the legalities involved with data sharing, storage, and use. It explains the legal framework under which the application functions. It also provides an in-depth explanation on:

- How and where the data will be stored
- How the stored information is used
- Amount and methods of data sharing
- Privacy policies

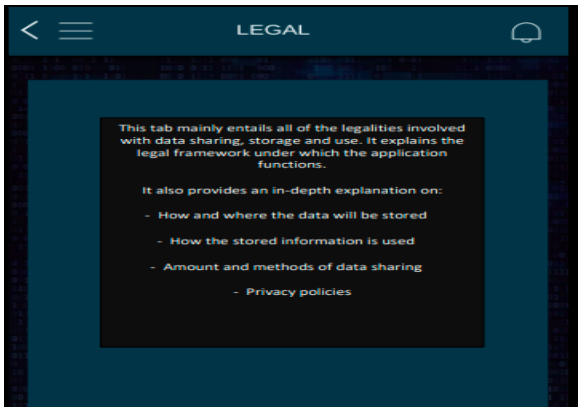


**Figure 7:** Legal tab.

### *3.4.8. About Us Tab*

This tab provides the developer's information:

- Establishment of the developing company
- Employee details
- Contact information for the company
- Helpline contact (in case of any issues that may arise)
- Feedback and responses


**Figure 8:** About Us.

## 4. Evaluation and User Study

The design evaluation corresponds with the Human Centred Design's phase of "evaluating the design" and according to usability heuristics. The tools used include design scenarios, evaluation through experimental research, and user feedback in form of a questionnaire. A low fidelity design paper prototype is implemented and evaluated heuristically for both the security and usability contexts of the application. The experimental user study has the following procedural outline specifications:

The goal of the study: To perform a preliminary user study on the evaluation of security and usability of an enhanced privacy-based home security camera mobile application. Independent variable: The paper prototype of the design implementation

Dependent Variables: Speed of achieving scenario tasks, user perception of usability, user perception of privacy, and security.

Design Structure: Within participants are used; this is preferred as it eliminates the potential of human variability becoming a confounding factor, also, fewer participants are needed to attain generazability of results.

Procedure and User tasks: 20 participants, 10 of which are fellow computing science master's students and the other 10 various students with non-computing backgrounds are used to conducti n g the evaluation experiment. This is to ensure different personas are captured for result generalizability. Participants were apprised of all evaluation procedures and task expectations. Care is taken to restrict control factors and variables; this is to ensure that only a change in the independent variable will result in a change of the dependent variable and nothingelse. The tasks required include;

- At the onset, users set preferred prompt time according to their schedule during installation, this time can be changed afterward to suit the user's preference.
- The user chooses a folder to store the encryption key.
- At each interval prompt, a user is notified to either upload or discard gathered data from security cameras. If the user chooses no, data is deleted. If yes, the user is further prompted to either encrypt the data before upload or be sent unencrypted. This is all done by clickingon buttons with appropriate visual metaphors and labels.
- The final scenario features when users demand their stored data. This is done by navigating through the app menu and selecting the "request uploaded data" button which prompts the user to enter the date and time of data requested and automatically retrieves it to save/download on local storage. Users can then access the saved data by decrypting it with their key.
- On completion of the above tasks, participants are then required to complete a questionnaire tailored to analyze users' perceptions on usability, privacy, and security of the implemented design prototype.

## 5. Results and Discussion

### *5.1. Demographics of Participants*

The number of participants involved in the study was 18 and therefore 18 questionnaires were generated and divided among 2 different personas or user groups. The demographics of the participants are as follows: The first group being students from the human-centered Security program at the University of Glasgow and the others being other students and individuals in non-related fields, this was to provide a fair perspective on the usability and security of home security camera prototype application. Participants were surveyed within 5-7 minutes. The non-technical participants were from India in the capital state of Delhi. The age range of the participants used for the study was from 21 to 60 years. The sex of the 18 participants is as follows; 8 girls and 12 boys.

### *5.2. Result*

**Results from participant responses**

Out of a score of 5, 10 participants representing 55.6% rated their interaction and convenience of the paper prototype, as 4 and 8 participants representing a percentage of 44.4 gave a score of 5. This indicates that even those with a little understanding of human-centered security found their way about the paper prototype with key functions being easily accessible making the application more usable.

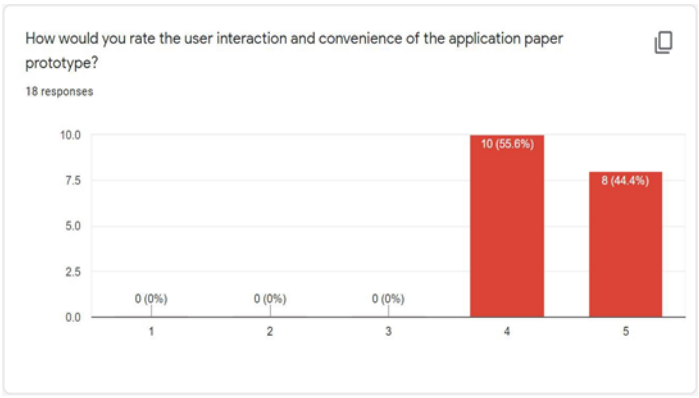


**Figure 9:** User interaction and convenience of the application paper prototype.

When asked if the use of our application reduced the number of steps it would have taken to complete the individual tasks manually, 5 participants representing 27.8% gave a score of 3 out of 5, 6 participants representing 33.3% gave a score of 4 out of 5 and 7 participants representing 38.9% gave a score of 5 out 5. Participants' responses indicate that the application is efficient and will make a difference with how encrypted data is stored and retrieved concerning home security cameras.

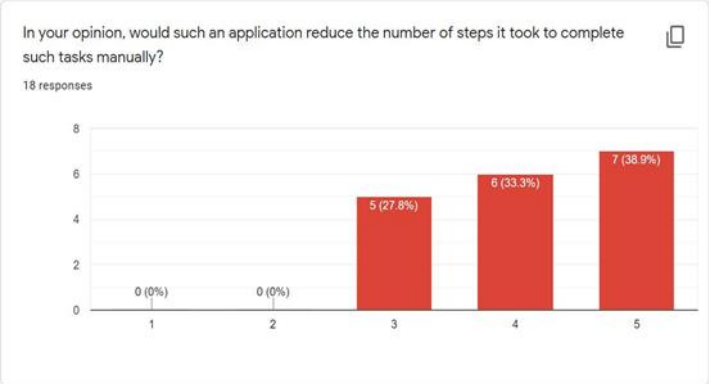


**Figure 10:** Perception of reduction of steps taken to complete tasks manually.

Participants' perceptions on the appropriate use of visual metaphors and labels were required. 2 participants representing 11.1 % gave a 3 out of 5 scores while 10 participants representing 55.6% gave a 4 out of 5 scores. 6 others representing 33.3 % gave a 5 out of 5 scores. This goes to prove that the buttons used, and their labels were explicit in terms of their functionalities with no ambiguity whatsoever. Participants expressed this with their positive responses.

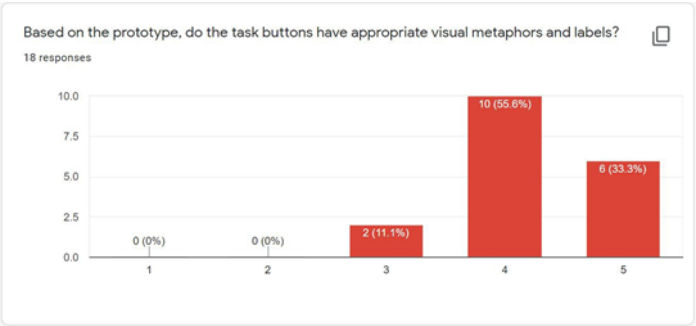


**Figure 11:** Perception of appropriate metaphors and labels.

Participants were asked about the encryption and decryption process and how easy it was to carry out. 13 participants representing 72.2% came up with a 4 out 5 score while 4 participants representing 22.2% gave a 5 out of 5 scores. Only 1 person gave a 3 out of 5 for the encryption and decryption process. The results indicate that the process involved in the use of the paper prototype application was well understood and steps to do the in-app prototype tasks were relatively simple.

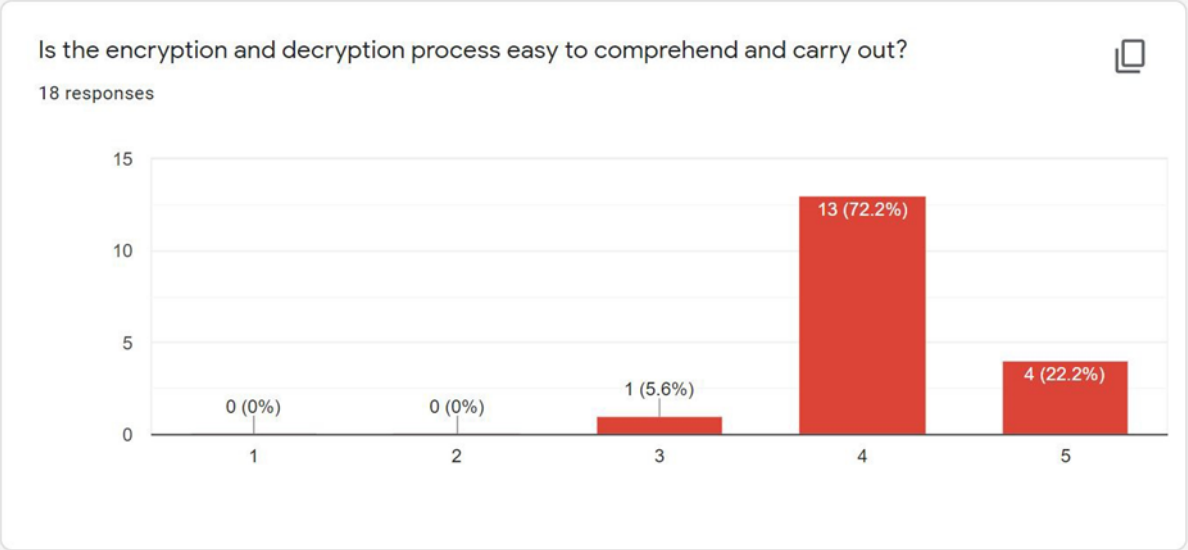


**Figure 12:** Perception of ease of encryption and decryption process.

Participants' perceptions were requested on how adequately the prototype considered privacy and security. 50% of respondents gave a response of 4 out of 5 and the other half responded with a 5 out of 5 scores. This proves that the prototype captured requirements to ensure that privacy and security for the application are adequately considered.

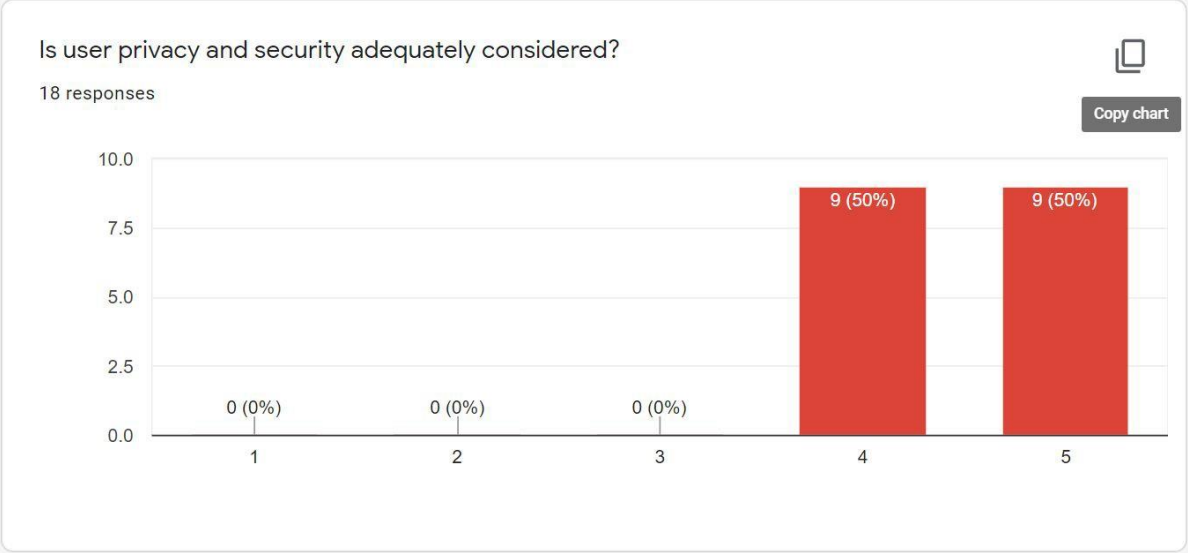


**Figure 13:** Perceptions on consideration of user privacy and security.

Perception on the usability of the application had decent scores with 4 participants (22.2%) giving a 3 out of 5 scores, 8 participants (44.4%) giving a 4 out of 5 scores, and 6 participants (33.3%) responding with a 5 out of 5 scores. This means that on average the application is very usable and non-technical participants appreciated what it takes to have a usable privacy mechanism in home security camera systems.

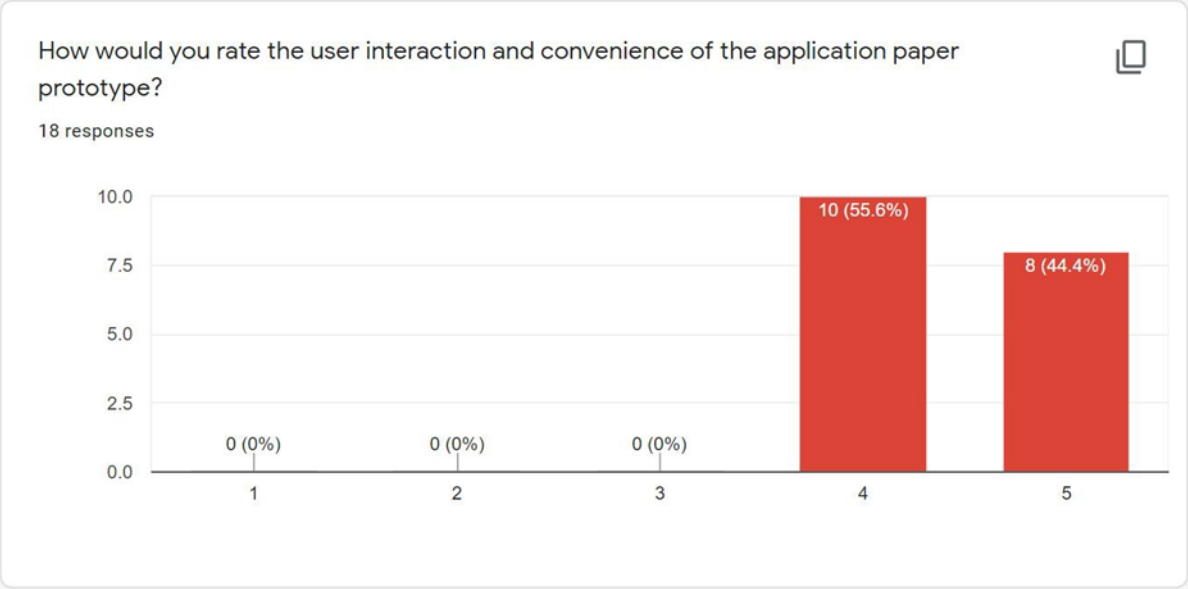


**Figure 14:** Perceptions of user interactions and convenience of the application paper prototype.

### *5.2.1. Non-Technical Group*

All the participants of the Non-Technical group scored the use and interaction of the application prototype a score of 4 or 5 indicating that they appreciated the prototype as easy to interact with and use in general. Only one participant indicated a 3 out of 5 scores for the reduction in the steps taken to complete tasks manually. All other participants indicated a 4 or 5 score, showing that the application was efficient for the non-technical group and made their lives easier. The non-technical group gave a 4 or 5 out of 5 scores for the use of visual labels and metaphors. These labels were the main features used to interact with users to ensure that the tasks involved in the app were completed seamlessly. This group also indicated through their score of either 4 or 5 out of 5 that, the processes involved in completing tasks were easily understood and in turn made the functions easier to carry out. They also implied through their score that privacy and security in the prototype were adequately considered. In this section majority of the participants gave a score of 4 with the rest scoring 5 out of 5.

Generally, the participants rated the prototype to be a good model of enhancing security and privacy in home security cameras.

### *5.2.2. Technical Group*

It was expected that the technical group would be more critical of the prototype since their previous knowledge on the subject informed their decisions. However, they gave equally good responses like the Non-technical group, on each section of the questionnaire. Their results are as follows;

All the participants of the Technical group scored the use and interaction of the application prototype a score of 4 or 5 clearly showing that they appreciated the prototype as they had no issues with its interaction and use in general. For the reduction in the steps taken to complete tasks manually, the majority of the 8 technical

participants (50%) gave a score of 3 out of 5, with the rest scored either 4 or 5 out of 5. This proves that the application was efficient in its use for the technical group. Like the steps taken to complete tasks majority (50) of the participants also rated a 4 out of 5 scores for the use of visual labels and metaphors with the others giving a score of either 3 or 5 out of 5 scores. This group participant also indicated through their score of either 4 or 5 out of 5 that, the processes involved in completing tasks were easily understood and in turn made the functions easier to carry out which was an impressive remark from a technical group. The group implied through their score of 4 or 5 out of 5 that privacy and security in the prototype were adequately considered. Even though the scores from the technical group on each section of the questionnaire were good, some feedback was suggested to be recommendations for future works.

#### *5.2.3. Summary of results*

The results obtained showed that both technical and non-technical users are comfortable with the application. They didn't find any difficulty while interacting with the application. They can make use of it without making dangerous errors. They could easily identify the metaphors used and appreciated the visual labels. The system was rated high on user interaction and convenience by both technical and non-technical group. Participants rated the encryption and decryption process to be easy. They didn't find it difficult. In terms of security and privacy, Participants considered the application to have provided adequate security and privacy. Overall, the application is considered usable, secured and has privacy.

## 6. Conclusion and Future Work

Our work aims at improving the security, usability and privacy needs of users of home security camera systems by encrypting the data before it's being sent to the cloud for storage, making the encryption process almost automatic and also giving the user the option of discarding the security footage of a particular day if he so desires.

Though the user study we conducted yielded positive results, one major challenge was the lack of access to the actual people who make use of these smart homes, like the elderly, disabled, or wealthy individuals. We tried to remedy this shortcoming by conducting part of the user study with students who do not have any form of technical background.

Based on the feedback we got from the participants, several improvements can be made to the current system. Firstly, the encryption and decryption process could be made completely automatic even though the encryption key is stored in the user's device. Secondly, subsequent user studies should endeavor to include participants from the elderly people, the disabled and wealthy individuals, who are the actual users of smart homes.

## References

[1] H. Lin and N. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments", *Information*, vol. 7, no. 3, p. 44, 2016. Available: 10.3390/info7030044.

[2] Z. Shouran, A. Ashari and T. Kuntoro, "Internet of Things (IoT) of Smart Home: Privacy and

Security", *International Journal of Computer Applications*, vol. 182, no. 39, pp. 3-8, 2019. Available: 10.5120/ijca2019918450.

[3] K. Beckers, *Pattern and security requirements*. Cham: Springer, 2015, p. 100.

[4] A.Whitten and J. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", in *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., 1999, pp. 169–184.

[5] E. W, "Security and usability: you CAN have it all!", *National Cyber Security Center*, 2018. .

[6] S. Shea and I. Wigmore, "What is IoT Security?", *IoT Agenda*, 2021. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security. [Accessed: 01- Mar- 2022].

[7] A.Gillis, "What is IoT (Internet of Things) and How Does it Work?", *IoT Agenda*, 2021. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed: 01- Mar- 2022].

[8] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey", *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414-454, 2014. Available: 10.1109/surv.2013.042313.00197.

[9] H. Atlam and G. Wills, "IoT Security, Privacy, Safety and Ethics", *Internet of Things*, pp. 123-149, 2019. Available: 10.1007/978-3-030-18732-3_8 [Accessed 1 March 2022].

[10] O. Vermesan, P. Friess and A. Furness, *The Internet of Things 2012 - New Horizon*, 3rd ed. Halifax, UK: Internet of things European Research cluster, 2012.

[11] J. SathishKumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20-26, 2014. Available: 10.5120/15764-4454.

[12] P. Kumar and U. Pati, "IoT Based Monitoring and Control of Appliances for Smart Home", in *IEEE International Conference On Recent Trends In Electronics Information Communication Technology*, India, 2016, pp. 1145 - 1150.

[13] M. Pawar and P. Umale, "Internet of Things Based Home Security Using Raspberry Pi", in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, India, 2018.

[14] G. Mantas, D. Lymberopoulos, and N. Komninos, "Security in Smart Home Environment," 2011.

[15] C. Lee, L. Zappaterra, K. Choi and H. Choi, "Securing smart home: Technologies, security challenges, and security requirements", in *2014 IEEE Conference on Communications and Network Security*, San Francisco, CA, 2014, pp. 67–72.

[16] S. Lee, J. Kim and T. Shon, "User privacy-enhanced security architecture for home area network of Smartgrid", *Multimedia Tools and Applications*, vol. 75, no. 20, pp. 12749-12764, 2016. Available: 10.1007/s11042-016-3252-2.

[17] S. Chitnis, N. Deshpande and A. Shaligram, "An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures", *Wireless Sensor Network*, vol. 08, no. 04, pp. 61-68, 2016. Available: 10.4236/wsn.2016.84006.

[18] C. Chhetri and V. Motti, "Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective", *Information in Contemporary Society*, pp. 91-101, 2019. Available: 10.1007/978-3-030-

15742-5_8 [Accessed 1 March 2020].

[19] V. Sivaraman, H. Gharakheili, C. Fernandes, N. Clark and T. Karliychuk, "Smart IoT Devices in the Home: Security and Privacy Implications", *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71-79, 2018. Available: 10.1109/mts.2018.2826079 [Accessed 1 March 2020].

[20] M. Plachkinova, A. Vo and A. Alluhaidan, "Emerging Trends in Smart Home Security, Privacy, and Digital Forensics", San Diego, 2016.

**Appendices**

A: Evaluation Questionnaire

**Appendix A: Evaluation Questionnaire**

Please fill in the following questionnaire in response to evaluation of the security camera application functionality. Collection is for analysis purposes only; all participants remain anonymous.

How long does it take to complete all tasks given the paper prototype?

<1 min within 2 mins within 4 mins >5mins

Please tick the number that best describes your answer in the following questions (1 being the lowest and 5 the highest)

A. How would you rate the user interaction and response of the application?

1 2 3 4 5

B. The app minimized the number of steps it took to complete tasks.

1 2 3 4 5

C. Task buttons have appropriate visual metaphors and labels.

1 2 3 4 5

D. Is the encryption and decryption process easy to comprehend and carry out?

1 2 3 4 5

E. Is user privacy and security adequately considered?

1 2 3 4 5

F. How would you rate the usability of the application?

1 2 3 4 5

H. Comment on limitations of the prototype in terms of usability, privacy and security

Comment:

I. Comment on recommendations to enhance the design prototype

Comment: