Mobile Guard

Kurt Yousef M. Barrioga[1], John Rey M. Gamotin[1], Jess Patrick Francis S. Quaitchon[1],
El Jireh Bibangco[1], and Elmer T. Haro[1]

[1] College of Information Technology, University of Negros Occidental-Recoletos, Incorporated, Bacolod City, Philippines

ABSTRACT

Most security breaches have been attributed to human errors implying that personal-level cybersecurity is very important. As interaction with mobile devices increases, individuals may become more vulnerable to cyberattacks. In this perspective, information technology solutions that could protect users from cyberattacks at the personal level are necessary. Thus, this study aims to design and develop an Android application named Mobile Guard that serves as a tool to protect, secure, and safeguard mobile devices from cyber threats related to authentication, carrier interoperability, and physical access. This application has five main modules: configuration, application lock, blocking, reports, and settings. After development, a mix of Boehm's and McCall's models was used to evaluate the quality of the application. The key results show that the reports module is the best feature of Mobile Guard. Likewise, the application lock and blocking modules are excellent features. On the other hand, although the user interface is acceptable, it should be improved in terms of operability and communicativeness. In conclusion, the target application has been effectively and efficiently implemented; however, there is room for improvement, especially on the layout and design.

Keywords

Mobile Guard, application lock, message blocking, security, privacy, protection, unauthorized user access, authentication

INTRODUCTION

Modern societies are constructed around personal and organizational networks powered by digital networks and communicated by the Internet (Castells, 2014). For instance, various governments have implemented and introduced e-government systems to improve services and save resources (Alshehri & Drew, 2011). On the other hand, companies and businesses have been using computer networks to reach more customers, advertise products and services, and collaborate with suppliers and business partners from all over the world (Berisha-Shaqiri, 2014). In addition, academic institutions and universities have introduced distance learning to make education more available for learners regardless of location and time (Sagheb-Tehrani, 2011), while individuals have been actively using web platforms, such as social networks interact with other people (Younes & Al-Zoubi, 2015).

These pieces of evidence show that present societies are deeply dependent on computer networks and information technology solutions. Unfortunately, this dependence has led to significant growth in cyberattacks and security breaches worldwide (Jang-Jaccard & Nepal, 2014) that have resulted in several serious issues globally.

A statistics report shows an annual average of nine billion malware attacks worldwide (Johnson, 2020). This figure means that cybercriminals are ever active, especially with the introduction of cutting-edge technologies in the market. The annual average of successful attacks worldwide has increased by 67% since 2014 (Bissell et al., 2019), and forecasts reveal data theft attacks to possibly continue to persist in the future (Positive Technologies, 2019). An interesting finding is that 90% of cybersecurity breaches are caused by human errors (CybSafe, 2019), suggesting that individual-level cybersecurity should not be taken lightly.

Cyber threats at the individual level mostly revolve around mobile devices, especially that more than five billion, or 68% of the world population, are unique mobile users (Kemp, 2018). Sixty percent of fraud online is accomplished through mobile platforms (von Gravrock, 2019). As early as 2011, an estimated 84.91% or more than 88 million Filipinos are mobile subscribers (PNP Anti-Cybercrime Group, 2018). More significantly, Filipinos ranked first globally in terms of time spent on social media, where an average user spends almost four hours on social media every day (Global Web Index, 2018 as cited in DataReportal, 2018). However, most Filipino mobile users lack awareness of the security features of their mobile phones, thereby exposing their sensitive data to hacking, intrusion, and other mobile threats (Omorog & Medina, 2018). The National Institute of Standards and Technology (2016) provides a comprehensive list of mobile threats, including their origin and countermeasures.

Several applications have been introduced to address the individual needs to combat mobile cyberattacks. For instance, Kaspersky (2013) developed the Applock Web Security that provides application lock, authentication, and call block features; however, it does not have a short message service (SMS) block and reports features. An alternative solution is AppLock (Rowland, 2016), which DoMobile Lab developed. Similar to Kaspersky Applock Web Security, this application provides application lock, authentication, and call block features. Unfortunately, it also does not support SMS blocking and report generation. Another solution is G Data Internet Security, which has an SMS block and report generation features; however, it does not have features such as application lock and authentication (Consumer Reports, Inc., 2018).

One of the best available solutions for mobile security is Dr. Web Security Space (Williams, 2018) that offers authentication, application lock, SMS block, call block and reports generation features. However, the main issue with this application is that it is not free, especially the SMS and call block features. Thus, an application that provides free SMS and calls block features with authentication and application lock is necessary.

To address the current needs to tighten cybersecurity, this study aimed to design and develop an application, namely Mobile Guard. Specifically, this study outlines the analysis, design, and development of the Mobile Guard, including its functionalities and user interfaces.

PRODUCT DESCRIPTION

Mobile Guard is an Android application that addresses three mobile threats according to NIST (2016) under the following categories: authentication, carrier interoperability, and physical access. The sought application provides several enhanced lock features in terms of authentication, such as color pattern lock and two-way authentication. For carrier interoperability, the application allows users to block unsolicited calls and messages. As for physical access, the application does not allow unauthorized access and modification of data in the mobile device. Moreover, the application provides a report feature that allows the user to review statistics, such as the summary of unauthorized access attempts.

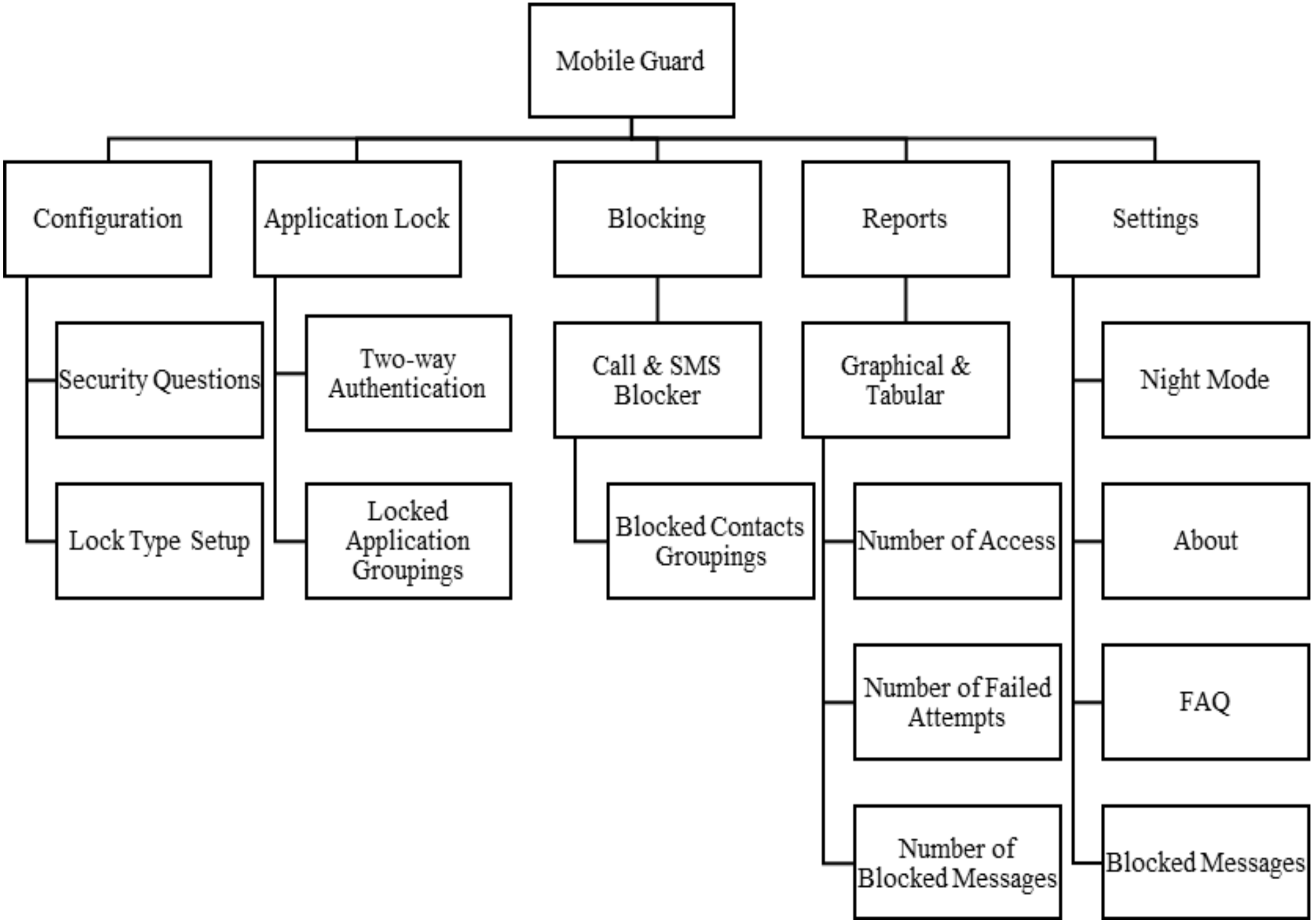
The application was developed in Android Studio, with Java used for its back-end activities. The specific operating system used during the development was Android 6.0 Marshmallow (Android, 2015). For user interfaces and prototypes, the proponents used Adobe XD, which is a recommended tool for user experience designers (Lindberg, 2019). The computer used during the development has two gigabytes of memory and a Quad-core 1.2 gigahertz Cortex-A7 processor. In addition, an Android mobile phone with a fingerprint scanner was used to test the application.

In order to ensure software quality, the proponents made use of a mixture of Boehm et al. (1978) and McCall et al. (1977) Software Quality Models. Thirty end users, all college students taking information technology-related programs, were selected using convenience sampling (Saunders et al., 2015) and recruited to evaluate the application. The proponents have properly explained the purpose of the evaluation process to the respondents. Moreover, the proponents secured formal consent from each respondent before a copy of the application is provided. The respondents were given at least one hour to test the application. After testing the application, the proponents distributed the software quality survey questionnaire based on Boehm's and McCall's models to measure the operability, learnability, device independence, assurance, consistency, completeness, accessibility, and communicativeness Mobile Guard.

Operability is a software attribute that measures how well the functions are working (Atzeni et al., 2019). Learnability is a software attribute that measures how fast the user improves their time using the application for specific functions (Lew et al., 2010). Device Independence refers to the ability of the system to adapt to a wide variety of devices without limiting its functions based on device specifications (Warner, 1983). Assurance is a software attribute that measures the consistency of the application to respond to the user's activities (McCall et al., 1977). Consistency is to repeat a similar action in multiples and still support the user with achieving the task while the application environment stays the same (Stahl, 2017). Completeness is a tool to verify that an application has the complete set of requirements that defines all system functions needed to satisfy the needs associated with performance and other non-functional requirements (Garcia et al., 2016). Finally, accessibility refers to the ability of the user to interact with the functionalities of the application (Boehm et al., 1978), while communicativeness refers to the ability of the system to communicate with the user and correctly project outputs expected by the user (Lee, 2014).

To determine the quality of the developed application, the researchers measured the following: data protection, blocking features, access summary, and user-friendly interface. Data protection focuses on the ability of the application to lock certain applications which the user chooses to protect. Its value is derived using the operability and learnability scored. The blocking feature focuses on the application's ability to block messages or calls from certain contacts of the user. Its value is derived using the operability, learnability, device independence, assurance, and consistency scores. Access summary focuses on the application's ability to provide a simple report from the activities done when a locked application accesses or had a failed attempt. Its value

Figure 1
Mobile Guard Decomposition Chart



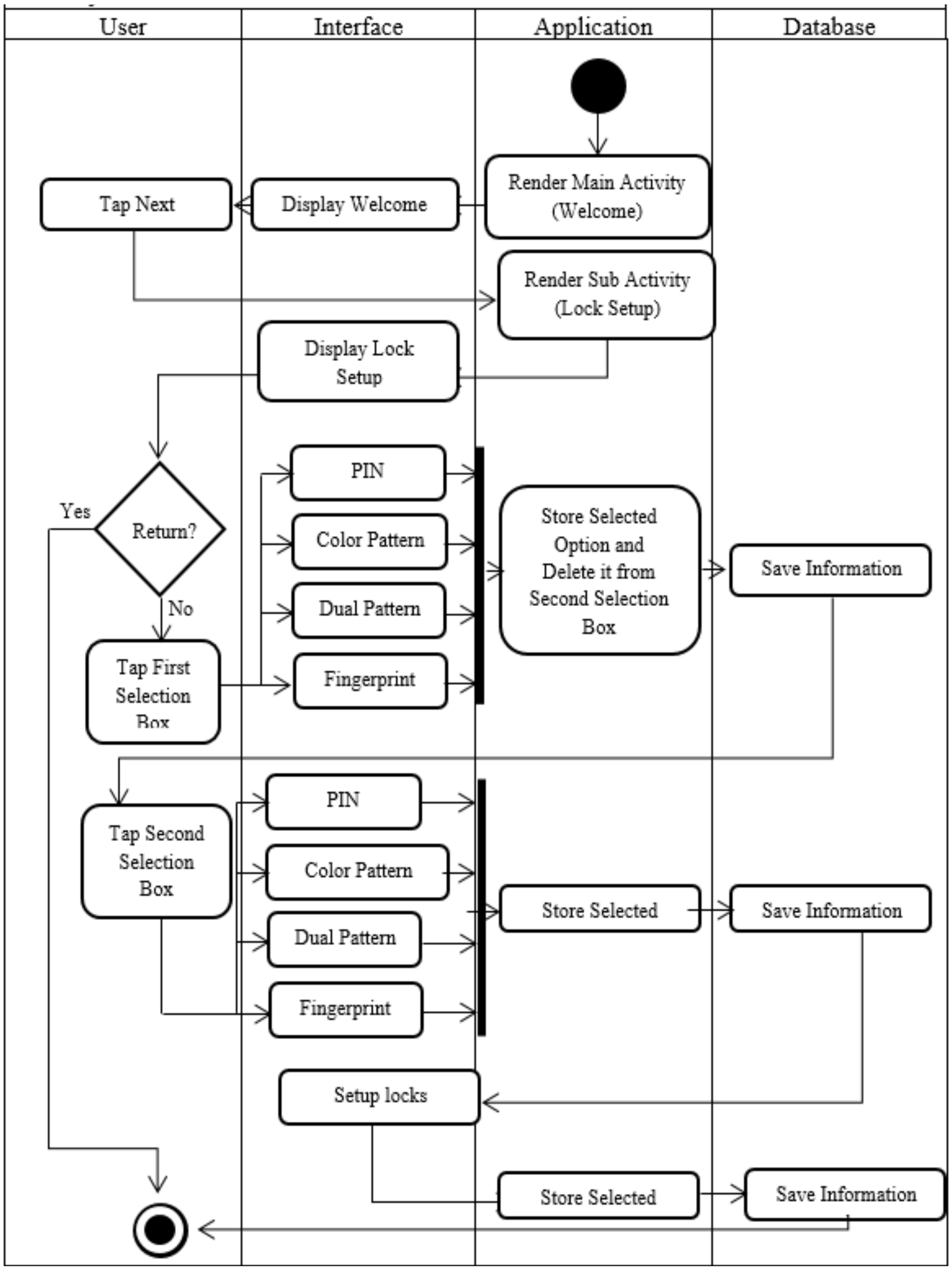
is derived using the assurance, consistency, and completeness scores. Finally, a user-friendly interface focuses on the application's ability to present itself simply for the user's convenience. Its value is derived using the operability, learnability, consistency, accessibility, and communicativeness scores.

SYSTEM FEATURES

Generally, Mobile Guard has five categories of features: configuration, application lock, blocking, reports, and settings. Figure 1 shows the functional decomposition of the sought application, including the categories of features and components.

There are two features under the Configuration category: security questions and lock type setup. Figure 2 shows the activity diagram of Configuration. After installation, the user must specify the security questions and provide the corresponding answers on the first run of the application. These questions will be used in case the user forgets the passcode for the application lock. Then, the user should set

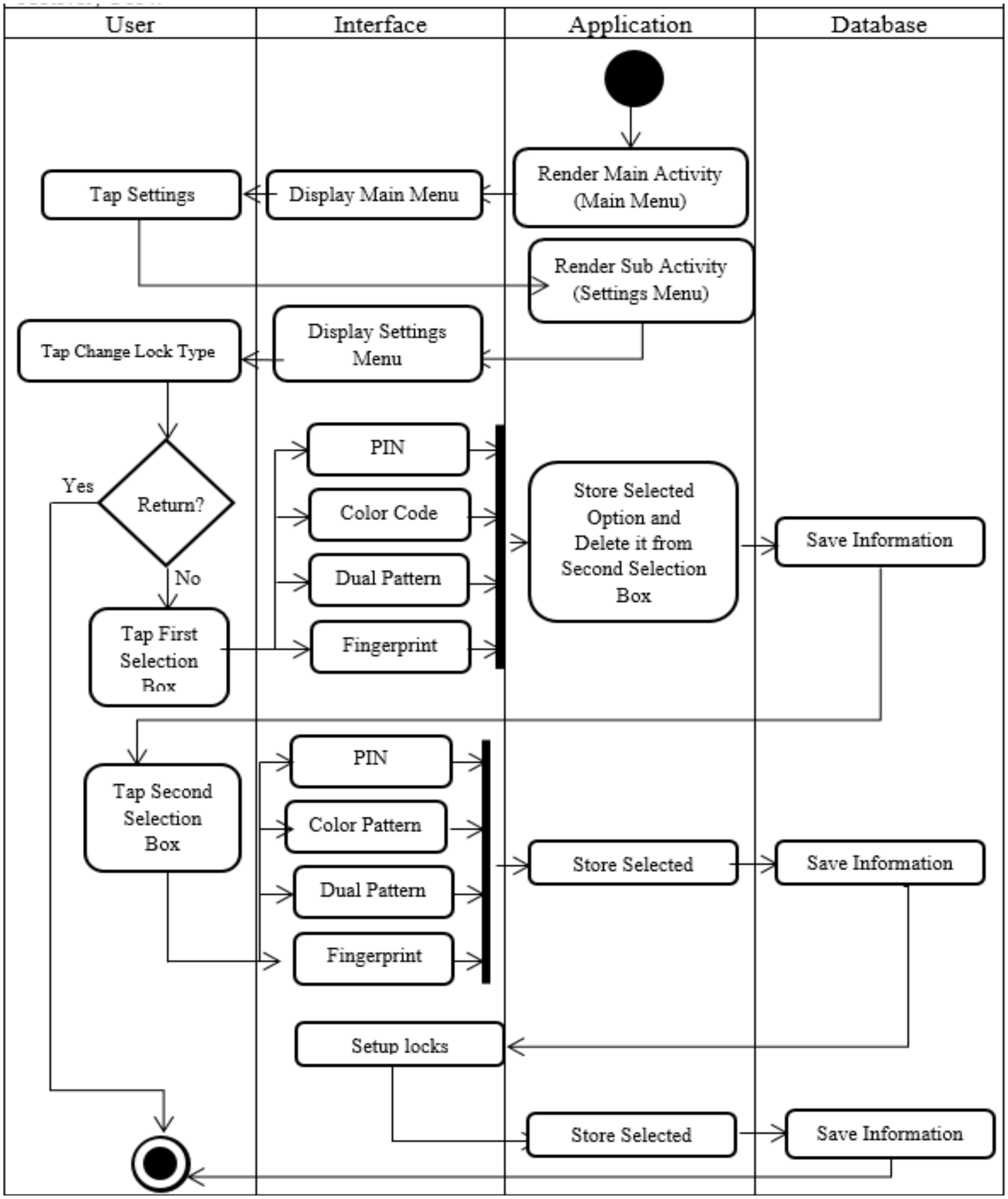
Figure 2
Lock types setup of Mobile Guard



up the screen lock, which will be used to lock the applications.

Mobile Guard allows users to lock specified applications on an Android device. Although other applications have a comparable feature, Mobile Guard provides an added layer of protection using a two-way authentication process using passcodes such as pattern, personal identification number (PIN), color PIN, and fingerprint. Figure 3 shows the activity diagram of the two-way authentication in the Mobile Guard. This process ensures that applications could not be accessed by unauthorized individuals. Moreover, Mobile Guard allows the user to group applications and lock applications according to the

Figure 3
Two-way Authentication of Mobile Guard

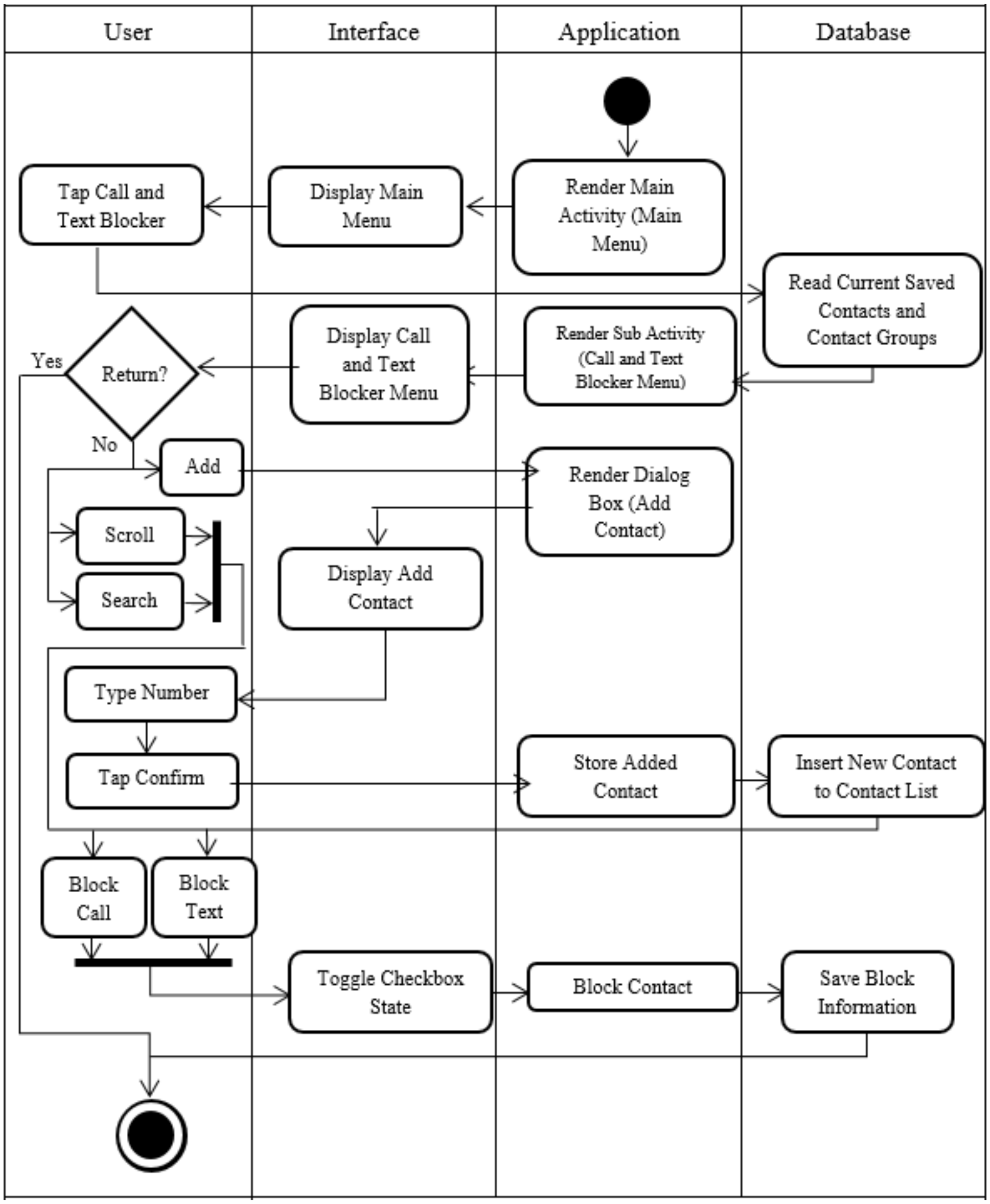


group.

Another key feature is the blocking mechanisms, as shown in Figure 4. In addition, the application features an SMS and call blocker, which provides users with options to block incoming calls and SMS from the specified phone numbers.

The target application is capable of generating reports, which allows the user to check the number of times a specific application has been opened. These reports allow the user to monitor the applications

Figure 4
Call and text blocker of Mobile Guard


User
Interface
Application
Database
Render Main Activity (Main Menu)
Display Main Menu
Tap Call and Text Blocker
Read Current Saved Contacts and Contact Groups
Render Sub Activity (Call and Text Blocker Menu)
Display Call and Text Blocker Menu
Return?
Yes
No
Add
Scroll
Search
Render Dialog Box (Add Contact)
Display Add Contact
Type Number
Tap Confirm
Store Added Contact
Insert New Contact to Contact List
Block Call
Block Text
Toggle Checkbox State
Block Contact
Save Block Information

that have been accessed, especially when a third party borrows the mobile device, as shown in Figure 5.

Other features include night mode, which has been implemented because of its user-centered benefits, especially when using the application at night; about, which provides basic information about the application; FAQ, which lists some frequently asked questions about the application with corresponding answers; and blocked messages, which is a collection of SMS from blocked phone numbers.

EXTERNAL INTERFACE REQUIREMENTS

Launching Mobile Guard for the first time after installation should redirect the user to the Setup Interface, as shown in Figure 6. The first step is authentication setup, which allows the user to choose either a one-way or two-way authentication.

Figure 5
Reports of Mobile Guard

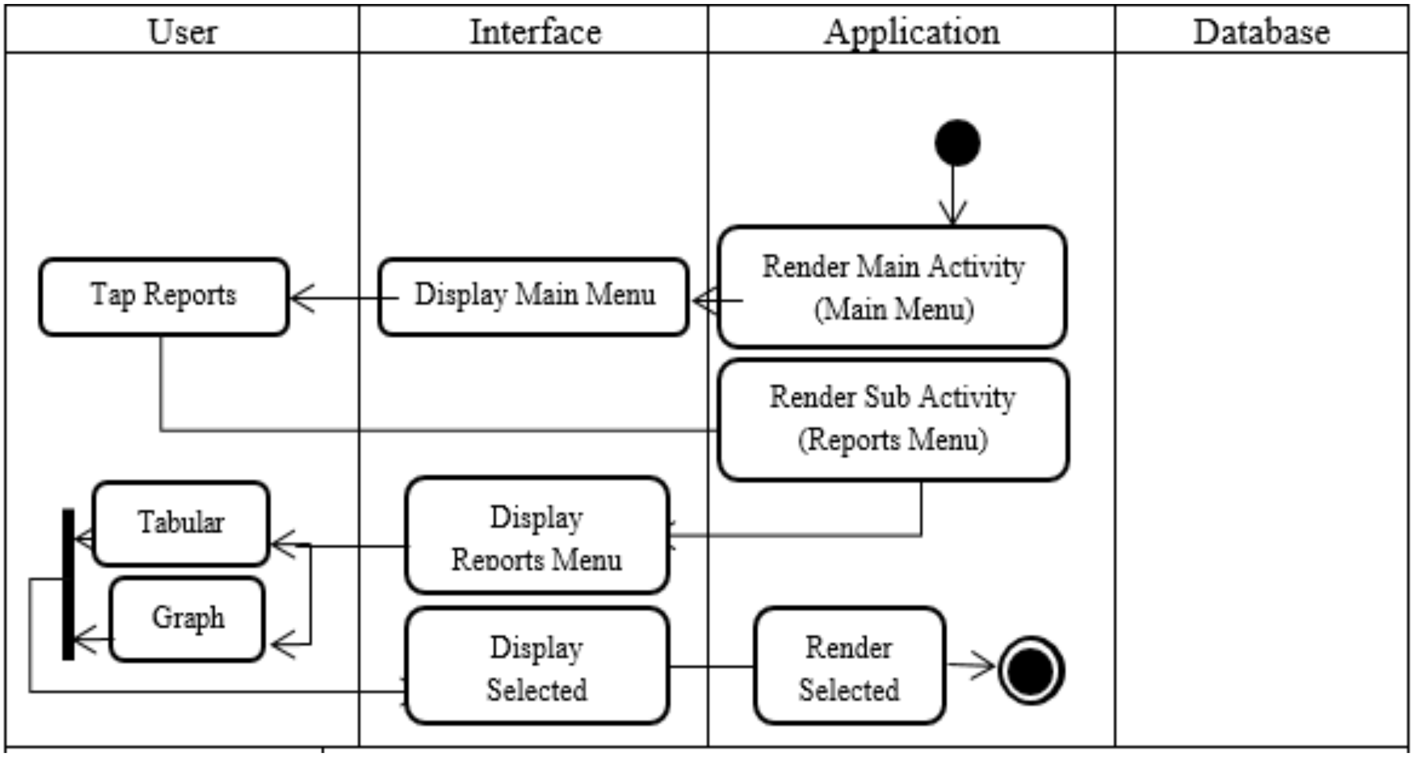
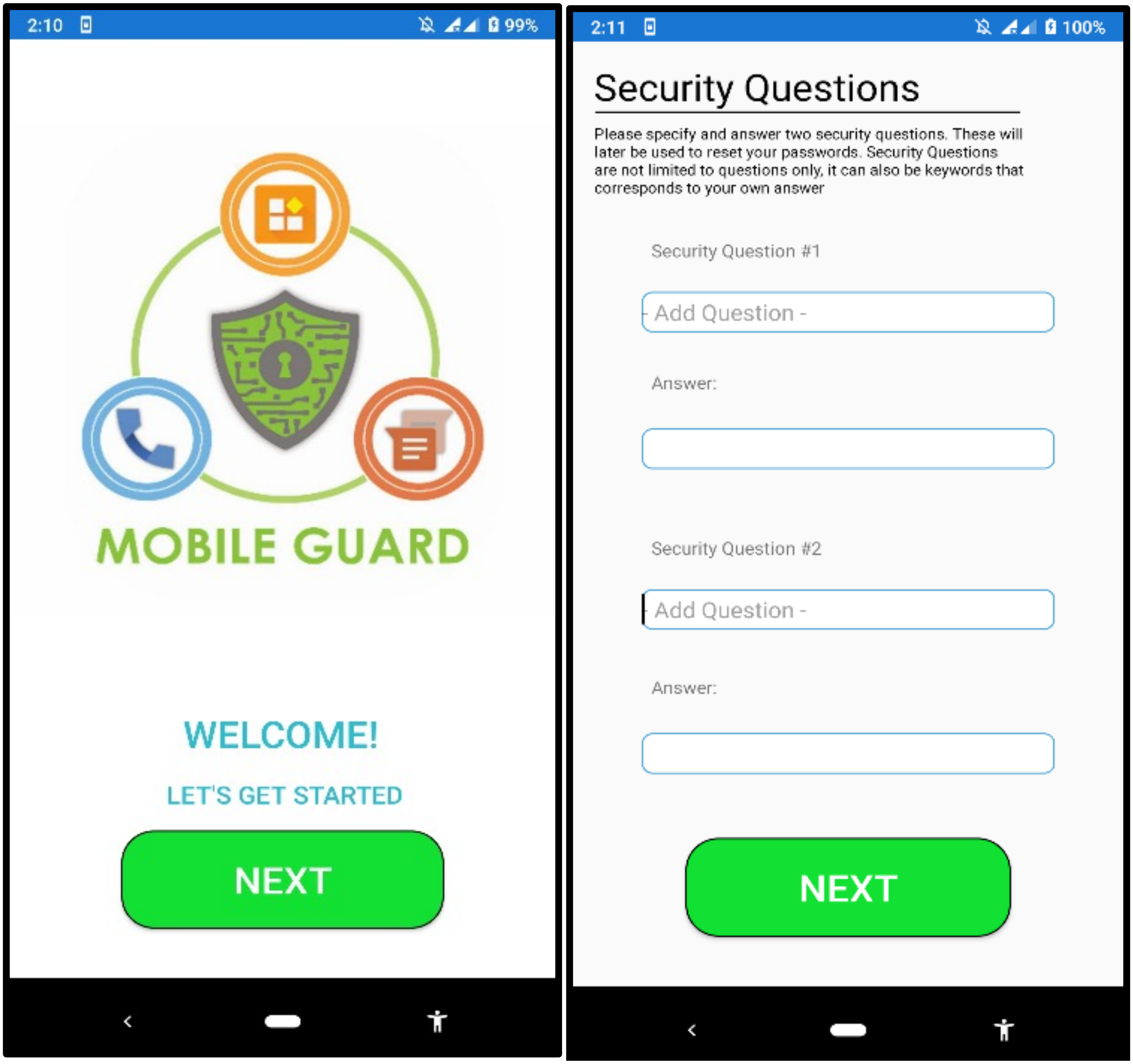


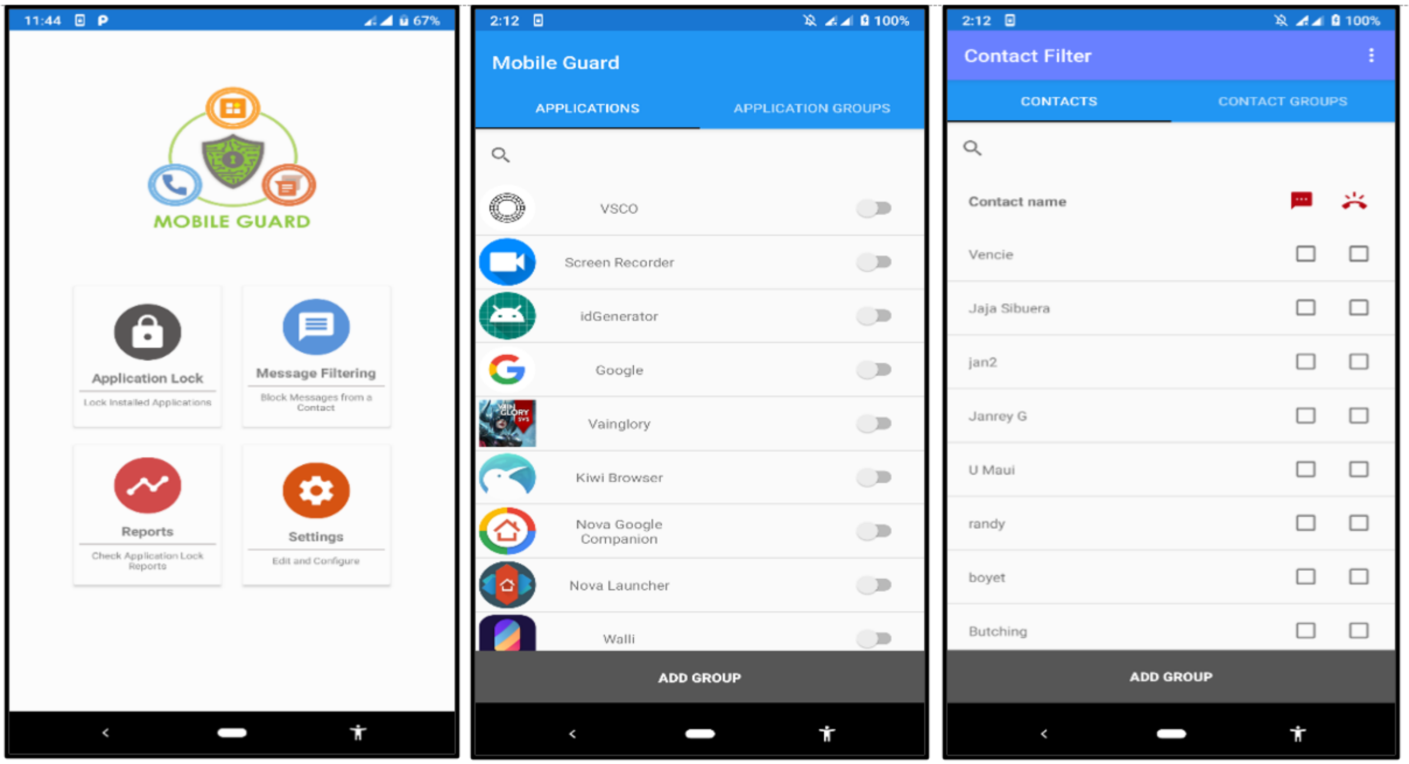
Figure 6
Setup Interface



Security Questions

Please specify and answer two security questions. These will later be used to reset your passwords. Security Questions are not limited to questions only, it can also be keywords that corresponds to your own answer

Figure 7
User Interfaces

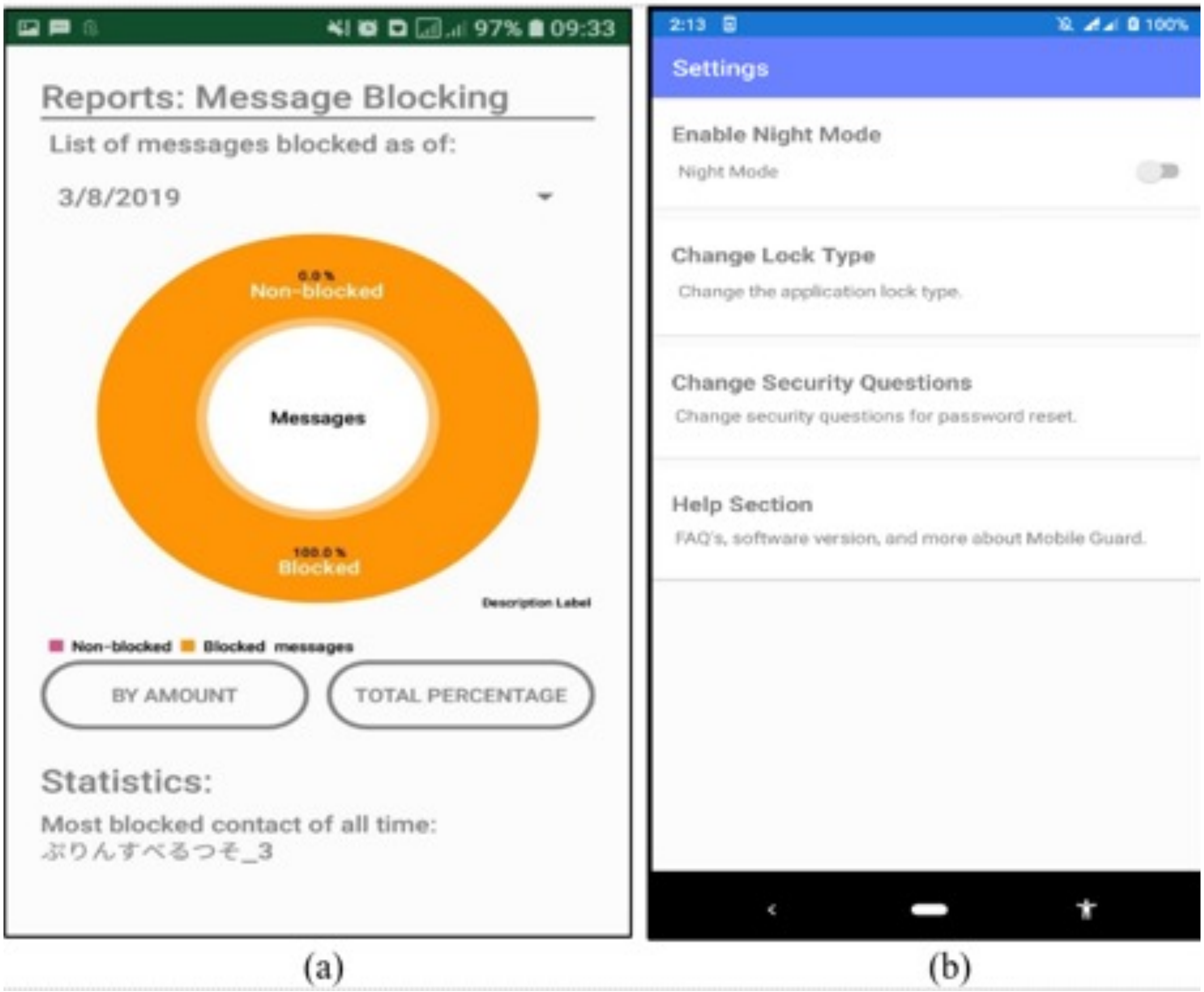


(a) (b) (c)

Once done, the user is required to set up the security questions and lock type.

Figure 7(a) shows the application's main menu loaded once the setup process is completed. The main menu consists of the main modules of the application: application lock, message filtering, reporting, and settings. On the other hand, Figure 7(b) shows the Application Lock interface, which lists the currently installed application on the mobile device. A toggle button is provided to easily lock a particular application. Figure 7(c) shows the Message Filtering interface of the application, which allows users to block a particular contact person. Two checkboxes are provided: one for SMS blocking while the other is

Figure 8
Reports and Settings Interfaces



Reports: Message Blocking

List of messages blocked as of:

3/8/2019

Statistics:

Most blocked contact of all time:
ぷりんすべるつそ_3

Settings

Enable Night Mode
Night Mode

Change Lock Type
Change the application lock type.

Change Security Questions
Change security questions for password reset.

Help Section
FAQ's, software version, and more about Mobile Guard.

for call blocking.

Figure 8(a) shows the Reports interface of Mobile Guard. It allows the presentation of the report in tabular or graphical form. Also, this module provides information about blocked messages from specified contacts of the user. Figure 8(b) shows the Settings interface of the application, which allows the user to enable the night mode, change lock type, and change security questions. In addition, this interface provides access to the Help Section of the application.

Table 1
Software Quality Evaluation Results

Product Features	Software Quality	Software Quality Attributes	Mean Value	Feature Mean Value
Data Protection	Usability	Operability	88%	90%
		Learnability	93%	
Blocking Features	Usability	Operability	88%	90%
		Learnability	93%	
	Portability	Device Independence	80%	
	Correctness	Assurance	100%	
		Consistency	90%	
Access Summary	Correctness	Assurance	100%	96%
		Consistency	90%	
		Completeness	100%	
User-friendly Interface	Usability	Operability	88%	89%
		Learnability	93%	
	Correctness	Consistency	90%	
	Human Engineering	Accessibility	90%	
		Communicativeness	86%	

Table 1 presents the summary result of the software quality evaluation with 30 respondents. As presented in the table, the application's best feature is access summary, which implies that the respondents considered the reports feature as helpful, consistent, and complete. The blocking and data protection features tied in the second place; albeit, their scores remained within the excellent range. These results imply that the respondents believe that both of the previously mentioned features are excellent application components. Finally, the user-friendly interface is placed last; its score is within the very good range. This result implies that the current user interface is acceptable, however, there are still features that need to be improved.

CONCLUSION AND RECOMMENDATIONS

This study mainly aimed to design and develop Mobile Guard, an application that provides Android users with a tool to protect, secure, and safeguard mobile devices from threats. It has five main modules: configuration, application lock, blocking, reports, and settings. The configuration module allows the user to configure the initial settings of the system. The application lock module provides the functionalities of locking a specific application. The blocking module allows the users to block incoming SMS and calls. The reports module provides a statistical summary of relevant interactions with the subject mobile phone. The last module, settings, provides an option to turn on night mode, change the lock types of the application, or change the security questions that were previously set.

The key results of this study show that the sought features of the application were successfully implemented. The reports module is considered the most important feature based on the software quality evaluation of the end-users. In addition, the blocking and data protection modules are excellent features. Although the interface design is considered acceptable and user-friendly, there is a lot of room for improvement. That being said, the proponents should improve the general layout and design of the user interfaces. Specifically, the proponents should focus on improving the operability and communicativeness of the application. In the future, the proponents believe that formal penetration testing is necessary to reinforce the claim that Mobile Guard is secure. Moreover, other cybersecurity-related features, such as malware defense, should be integrated into the application.

REFERENCES

Alshehri, M., & Drew, S. (2011). *E-government principles: Implementation, advantages and challenges*. https://doi.org/10.1504/IJEB.2011.042545

Android. (2015). *Android – Marshmallow* [Tech]. Android. https://www.android.com/versions/marshmallow-6-0/

Atzeni, A., Faily, S., & Galloni, R. (2019). Usable security. In *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics* (pp. 348–359). IGI Global.

Berisha-Shaqiri, A. (2014). Impact of information technology and internet in businesses. *Information Technology*, Q2.

Bissell, K., LaSalle, R. M., & Dal Cin, P. (2019). *Ninth Annual Cost of Cybercrime Study*. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Boehm, B.W., Brown, J., & Lipow, M. (1978). *Quantitative evaluation of software quality* (Vol. 69). John Wiley & Sons.

Castells, M. (2014). The impact of the internet on society: A global perspective. *Change*, *19*, 127–148.

Consumer Reports, Inc. (2018). G Data Internet Security—2018 Antivirus Software [Tech]. *Antivirus Software*. https://www.consumerreports.org/products/antivirus-software-33143/antivirus-for-windows-33142/g-data-internet-security-2018-395972/

CybSafe. (2019). *Human error to blame for 9 in 10 UK cyber data breaches in 2019*. CybSafe. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

Alshehri, M., & Drew, S. (2011). *E-government principles: Implementation, advantages and challenges*. https://doi.org/10.1504/IJEB.2011.042545

Android. (2015). *Android – Marshmallow* [Tech]. Android. https://www.android.com/versions/marshmallow-6-0/

Atzeni, A., Faily, S., & Galloni, R. (2019). Usable security. In *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics* (pp. 348–359). IGI Global.

Berisha-Shaqiri, A. (2014). Impact of information technology and internet in businesses. *Information Technology*, Q2.

Bissell, K., LaSalle, R. M., & Dal Cin, P. (2019). *Ninth Annual Cost of Cybercrime Study*. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Boehm, B.W., Brown, J., & Lipow, M. (1978). *Quantitative evaluation of software quality* (Vol. 69). John Wiley & Sons.

Castells, M. (2014). The impact of the internet on society: A global perspective. *Change*, *19*, 127–148.

Consumer Reports, Inc. (2018). G Data Internet Security—2018 Antivirus Software [Tech]. *Antivirus Software*. https://www.consumerreports.org/products/antivirus-software-33143/antivirus-for-windows-33142/g-data-internet-security-2018-395972/

CybSafe. (2019). *Human error to blame for 9 in 10 UK cyber data breaches in 2019*. CybSafe. https://

www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

DataReportal. (2018). *Digital 2018: Q3 Global Digital Statshot*. DataReportal. https://datareportal.com/reports/digital-2018-q3-global-digital-statshot

Garcia, I., Rodrígues, I., & Ahmad, M. (2016). Evaluation of the Non-functional Requirements, of Usability: A Systematic Study. *International Journal of Advanced Research in Computer Sciense*, *3*(3).

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993.

Johnson, J. (2020). *Cumulative detections of newly-developed malware applications worldwide from 2015 to March 2020*. https://www.statista.com/statistics/680953/global-malware-volume/

Kaspersky Lab. (2013). *Kaspersky Total Security*. Kaspersky Lab. https://kaspersky-total-security-multi-device.en.softonic.com/android

Kemp, S. (2018). Digital in 2018: World's internet users pass the 4 billion mark—We Are Social. *We Are Social Inc*. https://wearesocial.com/blog/2018/01/global-digital-report-2018

Lee, M.-C. (2014). Software quality factors and software quality metrics to enhance software quality assurance. *British Journal of Applied Science & Technology*, *4*(21), 3069–3095.

Lew, P., Olsina, L., & Zhang, L. (2010). *Quality, quality in use, actual usability and user experience as key drivers for web application evaluation*. 218–232.

Lindberg, O. (2019). Ask a UXpert: The Best Adobe XD Features Introduced in 2018 [Tech]. *Adobe Blog*. https://blog.adobe.com/en/publish/2019/01/30/design-experts-share-best-adobe-xd-features-from-2018.html

McCall, J. A., Richards, P. K., & Walters, G. F. (1977). *Factors in software quality. Volumes 1, 2, & 3* (Vols. 1, 2, 3). GENERAL ELECTRIC CO SUNNYVALE CA.

National Institute of Standards and Technology. (2016). *Mobile Threat Catalogue*. National Institute of Standards and Technology. https://pages.nist.gov/mobile-threat-catalogue/

Omorog, C. D., & Medina, R. P. (2018). Internet Security Awareness of Filipinos: A Survey Paper. *International Journal of Computing Sciences Research*, *1*(4), 1–13.

PNP Anti-Cybercrime Group. (2018). *Cybercrime Threat Landscape in the Philippines*. PNP. https://acg.pnp.gov.ph/main/quality-policy/20-publications/42-cybercrime-threat-landscape-in-the-philippines

Positive Technologies. (2019). *Cybersecurity Threatscape 2019*. Positive Technologies. shorturl.at/prtG9

Rowland, S. (2016). AppLock: A solid choice for security (Review) [Tech]. *AndroidGuys*. https://www.androidguys.com/reviews/applock-a-solid-choice-for-security-review/

Sagheb-Tehrani, M. (2011). Distance learning: An empirical study. *Information Systems Education Journal*, *9*(1), 41.

Saunders, M., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (7th ed.). Pearson Education.

Stahl, M. (2017). The Unspoken Requirement: Testing for Consistency [Tech]. *StickyMinds*. https://www.stickyminds.com/article/unspoken-requirement-testing-consistency

von Gravrock, E. (2019). Here are the biggest cybercrime trends of 2019. *World Economic Forum*. https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

Warner, J. R. (1983). Device Independence and Intelligence in Graphics Software. In *Computer Graphics* (pp. 60–66). Springer.

Williams, M. (2018). Dr.Web Security Space review | TechRadar [Tech]. *TechRadar*. https://www.techradar.com/reviews/drweb-security-space

Younes, M. B., & Al-Zoubi, S. (2015). The impact of technologies on society: A review. *IOSR Journal of Humanities and Social Science*, *20*(2), 82–86.