Curbing Criminal Acts on Mobile Phone Network

Olasina Jamiu Rotimi, Sanjay Misra, Akshat Agrawal, Ezenwoke Azubuike, Rytis Maskeliunas, and Robertas Damasevicius

Abstract It is no longer a story that the criminal act is now the order of the day in Nigeria with the way mobile phones and network applications are being used. A lot of Nigerian citizens have in one way or the other fallen prey to this crime through online fraud, hacking into the person's account, retrieving vital information, and the likes. It is, therefore, necessary to detect some of these crimes, reveal them, and proffer possible solutions on how to avoid them, and possibly, how to solve such problems. To do this, the most recent papers were reviewed to create awareness of such criminal act detection and how to curb such activities to create a friendly environment for the usage of mobile phones and network applications without any panic. It is also evident that with the stated methods in this paper, such criminal acts would have been greatly mitigated.

Keywords Mobile phones · Criminal act · Crime · And network

O. J. Rotimi · S. Misra (✉) · E. Azubuike
Covenant University, Ota, Nigeria
e-mail: sanjay.misra@covenantuniversity.edu.ng

E. Azubuike
e-mail: azu.ezenwoke@covenantuniversity.edu.ng

A. Agrawal
Amity University, Gurgaon, Hairiyan, India

R. Maskeliunas · R. Damasevicius
Vytautas Magnus University, Kaunas, Lithuania
e-mail: rytis.maskeliunas@vdu.lt

R. Damasevicius
e-mail: robertas.damasevicius@vdu.lt

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_10

1 Introduction

Criminal offenses on mobile phones vary from one level of occurrence to another. This act is ranging from virus attacks, malware activities, hacking, and the likes to mobile phones. It is a criminal offense to illicitly have access to data such as contacts, files, private information (such as Bank Verification Number (BVN), passwords, account details, e-mails, and others) and also to induce destructive mobile software such as malware in the system. It is evident that mobile phone is a necessity, and as such, it makes life easier for people in the way we do businesses, carries out researches, fast-tracking of online processes and activities and for these; it has therefore become what we cannot do without. A paper iterated the outrageous development the Internet use and widespread acceptance [1]. The paper proved the increase in security threats and Nigeria of today, cybercrimes are committed in many ways, and these include frauds on e-mails, wrong identity, hacking, criminal harassment, spamming, spoofing on the use of ATM, piracy acts, phishing, and many more. Cybercrime is no doubt a threat to our immediate environment, and people who used their mobile phones to connect to the Internet are the major points of reference [2]. Information and communication (ICT) trends aided these activities by its enormous tools to perpetrate cybercrimes [3].

Viruses are illicitly introduced software into the system to disrupt the system activities, but malware includes SMS fraud—where users unknowingly subscribed to the service, and at the later end, a cruel way was used to charge users without their knowledge, Spyware—it steals data from users without prior permission of the owner, and so on. [4]. Also, the echo reflection of mobile phones has made them very important means of exchanging information, in the field of communication. Furthermore, there also exists a limitation to how to convey criminal activities to law agencies for quick and needed actions [5, 5]. According to [7], the growth of the telephone network and its availability to the Voice over Internet Protocol (VoIP) has made it a major contribution to its flexibility and also the very easy-to-use artifact for end users. This also contributed significantly to the increase in cyber-criminal activities, and these criminals use emergent technologies to conduct illegal and suspicious activities. Crime analysis is a law enforcement function, and it involves systematic analysis for patterns and trends identification and analysis in crime and disorder. Information acquired from this pattern can then be used in aiding the activities of detectives in identifying and apprehending criminals [8].

The likelihood that a crime is detected and its offender is appropriately charged is a central component of the standard economic model of crime. It is also critical to the incapacitation channel, by which societies can prevent hardened criminals from reoffending. Yet, the economics literature has barely devoted any attention to studying the determinants of crime detection in detail. Typical approaches include examining whether police numbers, police composition, or high visibility patrolling are associated with lower crime rates. The implicit assumption is that a change in these variables can lead to higher chances of catching offenders, which has an immediate deterrence effect as well as an incapacitation effect over longer horizons

[9]. As part of the study, it is necessary to incorporate the action of the police force and other law enforcers to the needed technologies to apprehend the offenders who are cybercriminals. At times, the police may visit the perpetrators at home for questioning as the data of the ownership of the phone in question would be automatically captured for necessary actions. Due to the rapid need for telephone by the service it renders, criminals are now abusing its use to perpetrate various cybercrime attacks, and it is therefore necessary to logically detect and study some of the already existing solutions to these problems and also propose a new solution as there have never been any of the existing solutions without its setback.

In recent years, the number of online crimes, such as the various emerging scams and criminal schemes, has tremendously increased, and also, the online crime suspects utilize the anonymous nature of the Web to disguise their identity through various methods to evade detection and surveillance from law enforcement agencies. The prime suspect's communication methods and identifying numbers have become so hard to be verified under the electronic surveillance warrant for the Law Enforcement Monitoring Facilities (LEMF). When this is compared with traditional telephone and mobile phone communication records, online communication is more uncertain to be tracked, and its techniques require a sophisticated system [10]. Also, nowadays, providing information and security for mobile phones and also processing it in mobile network data is a great issue of importance and interest. As mobile phones and computers are provided with broader functions, the geometrical growth of vulnerabilities is also increasing in that regard. Today, an unauthorized person who is a criminal can make a call and eavesdrop on them, text message, drop malicious programs like malware, spyware, also steal money, and put the system out of order to his advantage without prior knowledge of the owner [11].

Mobile devices have become an integral part of our daily life, and there is no doubt about that. These have therefore proven to be an advantageous and almost the most successful scientific resolution of our time that fills personal and business needs in a very efficient manner [12]. In this era, the availability of mobile services has significantly increased because of the rich variety of mobile devices and essential applications provided by mobile device manufacturers as has been rightly emphasized in the previous chapter. At the same time, numerous mobile security issues and data privacy threats are challenging the use of this device in various aspects of human endeavor. Therefore, mobile devices are an ideal target for various security issues and data privacy threats in a mobile ecosystem [13]. Also, the impact of cybercrime poses a negative signal over the state of any system, and this can be felt on every individual, economy of a nation, international prospect, and integrity of a nation [1]. This paper, therefore, looks into threat detection and prevention, and also, necessary steps and algorithm to alert the security agencies are put up as a proposed framework and architectural modeling for the future most prominent solution to the problem at hand.

2 Background Information and Literature Review

Researchers have gone far as to carry out a lot of studies and investigations on the issues of threats posed by the use of mobile phones. Particularly, vulnerabilities of this amazing device to illegal act by cybercriminals have necessitated the prompt need of all researchers in the chosen area of the framework to be on their toes as the terror of criminal act has become the order of the day. Any attack on the use of the mobile phone that makes life uneasy for the user is indeed an action that has put such a user in a state of great concern. Therefore, any such challenges should be dealt with. Cybercrime issues encompass stakeholders such as the offender; its target/victim; technological; society and the law, and the architectural model was proposed. This does for the future reservoir of resources for mitigation of cybercrime [14]. The threat on the mobile phone includes (1) viruses, (2) malware, (3) spyware, and (4) limited way to convey information to the needed security agency. Authors [13] fully explained that the threat to the mobile device is multiple and it requires multiple means of protection and restrictions. These researchers proposed a defensive mechanism architecture that can simultaneously handle various threats on the use of mobile phones, but the security measure to alert the police was not put in place. Authors [15] explained that advanced persistent threat (APT) attack is a carefully planned attack that involved both social engineering and malware, where spear phishing is the most popular method that has been used by the attacker. The attacker will send an email to the targeted victim by including link (s) to the targeted Web or malicious attachment to carry out their illegal activities, but this was taken care of by the adoption of smartphones and implementation of security on bringing your device (BYOD). In [16, 17], authors launched preventive measures such as passwords, firewalls, encryption, and detection mechanisms such as tripwires, configuration-checking tools, and anomaly detection systems [18]. In their paper established a helping mechanism in investigating agencies in the detection and identification of criminal acts by the use of methods that involved six approaches—data extraction (DE), data preprocessing (DP), GSM technology, Google map representation, advanced embedded system (ES), and preprocessing of the dataset to safeguard its originality before its cluster analysis. Authors in [19] their paper posed that mostly threat is always from the Internet and therefore tackled by setting up Apache Hadoop cluster with Apache Ambari. Where master and slave nodes represent a Mesintempur as a cluster. Apache Hive was used to aggregate data from raw data for the attack type incorporated with related mechanism, deeper analysis was made, and the resultant attack data was converted to the dataset. The mining was done by the use of the SPMF tool. Besides, authors in [20] studied the Web site, using six different metrics, such as speed, SEO, security, broken links, updates, and availability to come to 54% of good Web sites of Web clustering.

Authors [21] in their paperwork validated the factual establishment of the generated results of their analytically solved problem that was based on leveraging phone numbers analysis in improving the world understanding of the underground markets, illegal activities with computers and software, and cybercrime in general

and by these emphatically stated that scam activities with phone numbers were often and more stable over the period than email addresses. This was backed up by the combination of graph analysis and geographical home location register (HLR) lookup. Authors in [22] went further in their work to gather dataset related to the criminal activities from the cloud, by making the criminal-related information available to the law enforcer to speed up their investigation of criminal identification by developing the police Android application and the general user mobile application.

In [23], authors stated algorithms and mechanisms such as statistics-based algorithm, decision tree-based algorithm, rule-based algorithm, Bayesian classification model to detect fraud in automobile insurance, Naïve Bayesian visualization for data analysis and interpretation, the classifier predictions, and the use of ROC curves data assessment. All these are used for data mining. As a proper check and unbiased technique, authors in [24] proposed discrimination prevention degree (DPD), discrimination protection preservation (DPP), misses cost (MC), and ghost cost (GC). The DPD and DPP measured the success of the proposed method in discrimination prevention which ideally should be 100%. The MC and GC, therefore, measured the degree of information loss that forms the impact on data quality, and it should ideally be 0%. Authors in [25] studied that the best-recommended cryptography application that can be used on IM is encrypt, followed by AES-Crypto, EnDe-Crypto, and Kryptokaz as it is a good way for securing data.

Nevertheless, authors [11] in his work studied three asymmetric encryption techniques: RSA, ElGamal, and elliptic curves to select the most efficient and appropriate algorithm for data transmission. Elliptic curves became the best, and RSA and ElGamal algorithms are not good for the text message at all. These comparisons were done on a carefully designed platform Java 2 Micro Edition (J2ME) using wireless messaging PI (API). The application runs on a mobile phone with an ARM9 processor with a frequency of 219 MHz and 10 Mb of internal memory and the Java virtual machine (JVM) with enabled just-in-time (JIT).

The key parameter of interest is to establish a framework to address spyware, malware, viruses, unauthorized access, and bad Web sites, as there is no single system or model which can take care of all the already existing cybercrimes at the present. Besides, there is no mobile-based app for this function, and in this work, HTML5, CSS, PHP, API-VIRUS TOTAL, and MYSQL would be greatly employed for the system design. One can find other security issues in mobile in various researches [26–29].

Motivation: The existing techniques are not on a mobile app, and besides, no existing solution used multiple solutions to solve the criminal acts. This system was proposed to use multiple techniques of different algorithms to mine data, detect unwanted data, and curb Internet crimes, and reporting to the necessary law enforcement agent using mobile phones at the discretion of the user is the required task. Also, the driven force centered on the gap created by the past researchers. This then enables us to come up with this tremendous model as a mobile app.

Aim and Objectives: The aim is to establish and build a mobile app to compliment the already existing algorithms, using different techniques of the framework

to prefer solutions to the cybercrimes. The objective is for the proposed framework to deliver real data to the receiving-end phone; send details of the sending-end phone handler to the law enforcement agent; and block any unwanted data from disrupting or intercepting the system.

3 Proposed Model

In this study, we propose an upgrade of existing technologies to curb cybercrimes on the use of mobile phones. In the upgrade, a Web-based application that will interrupt the activities going-on on a mobile phone will automatically be linked to the phone number of the police or law enforcer agencies for proper action. Besides, any bad Web would be kicked out of action, and only the good one will go through. We, therefore, propose the architectural framework that will detect, identify, and solve multiple problems of cybercrimes using a mobile app. The proposed model is shown in Fig. 1 below.

The model is divided into four categories, and these categories include the sending-end section, intruder section, mobile app section, and receiving-end

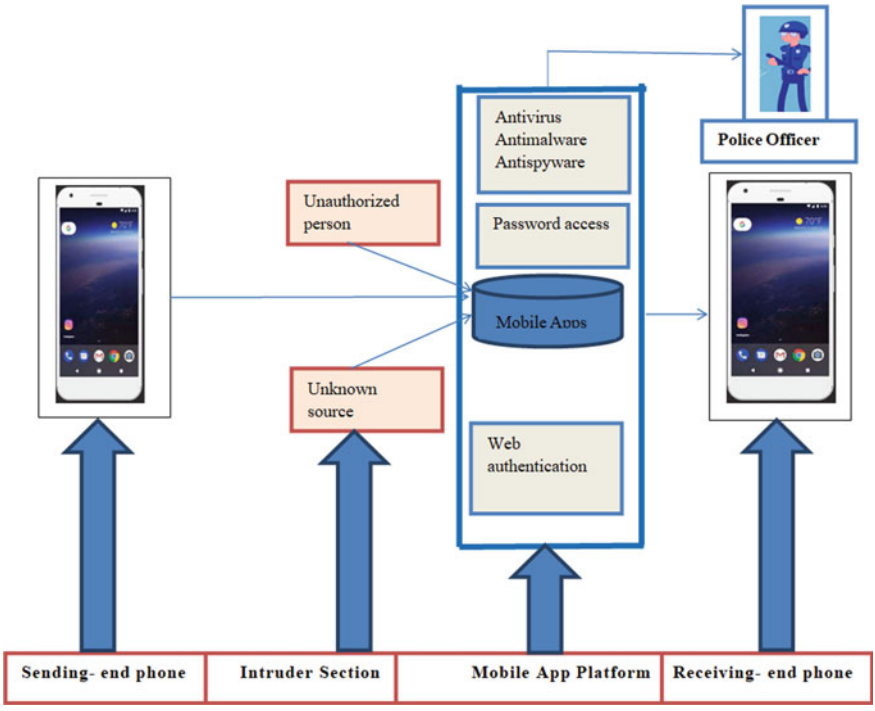

Fig. 1 Proposed architectural framework for the model

section. At the sending-end section, data which would either be a text message or multimedia message and so on is to be sent to the receiving-end phone section. But before then, such data would have to go through the mobile app section for necessary actions before it is finally received at the receiving-end phone. For the scope of this work, data from the sending-end phone is called real data, while data from unauthorized access and unknown sources, virus, malware, spyware, and the like is called unwanted data. The main function of the mobile app section is to detect unwanted data and block it, and a platform is provided to dial security code for necessary action or sanction of the culprit. The app will send personal information of the culprit to the law enforcer agent that is with such a phone identity number. The algorithm that explains the operational flow of the proposed framework and flowchart is shown in Fig. 2.

0 Start.
1 Log in your detail to open the APP (APP Launching).
2 If no details, create one (Create One).
3 Check if there is any data from an unauthorized person (Duk).
4 Check whether a good Web site (GWS) or bad Web site.
5 Check for any software threat (THREAT).
6 Allow the real data on the device (REAL DATA).
7 Block any unwanted data (UD) from having access to the recipient phone.
8 Forward the address of the sending-end phone to the closest law enforcer.
9 Stop.

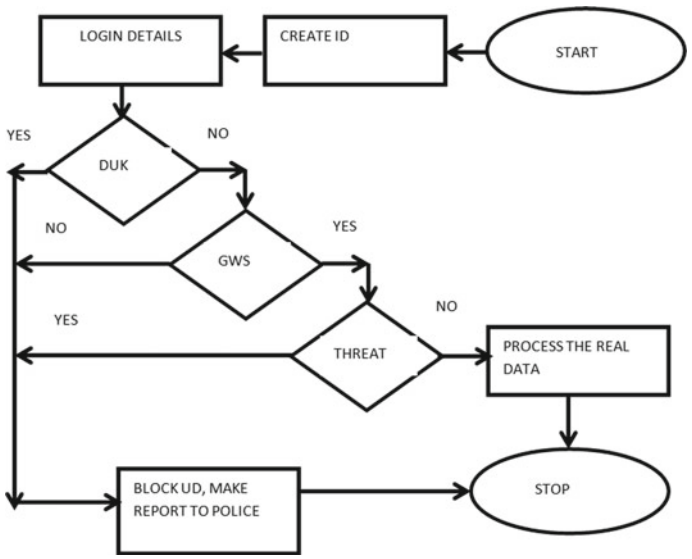

Fig. 2 Flowchart

3.1 Implementation of the Proposed Model

The process is divided based on the aim of the proposed work, and this goes down the line from specification to the evaluation across tasks to be handled by the mobile app section. The app should synchronize between the incoming data and the receiving-end phone. See Fig. 3, being a model for interoperability of the entire development process. The process is discussed below:

Specifications: The app will remove viruses, malware, spyware, and block bad Web sites and unwanted data. It will relay the good data to the intended receiver and channel details of any detected criminal act to the police agency if necessary by the user.

Design: The design was done by the use of HTML5, CSS, JQUERY, and PHP. These software tools were used to design both the front end and back end. The database that was used is MYSQL, and the Android-based application that was used for virus detection function is API-VIRUS TOTAL.

Implementation: The design as it has been listed is implemented following all algorithms incorporated in the mobile app model, and the necessary results were generated.

Evaluation: The mobile app was evaluated through deployment to check if any aspect will require visitation for the betterment of the system.

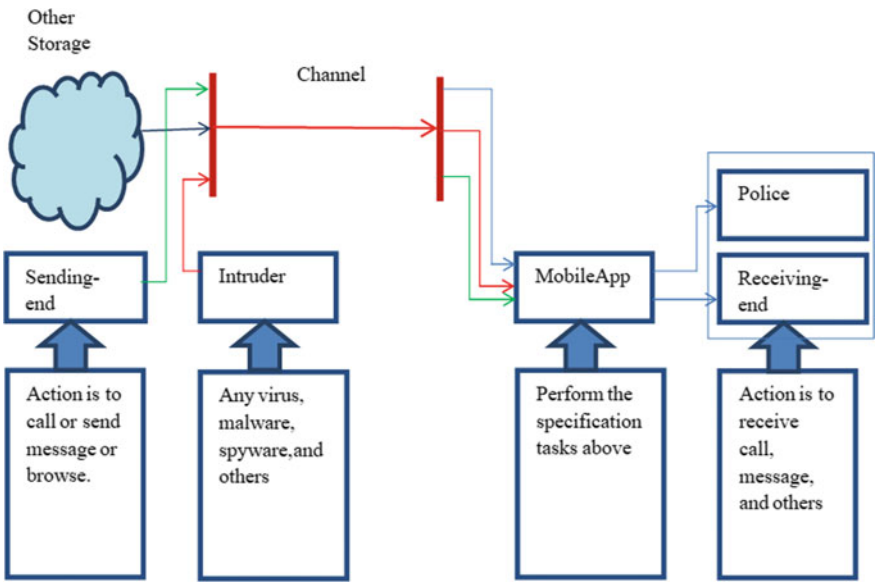

Fig. 3 Model for interoperability of the entire development process

4 Experimental Results

The results obtained are demonstrated in cropped screenshot pictures. The interface for each stage is shown under appropriate sections. See Figs. 6, 7, and 8, for the front-end view of options for test link, test files, file report, and help. The help option will guide any new user on how to use the app, for there are links that such users will follow to help with how it works.

When the mobile app is launched, it will display the front end as shown in Fig. 4 below. As soon as the requirement for logins is satisfied, it will launch the front end in Fig. 5, and from there, the option will be chosen for the link test, file test, file report, and help. The test link option will help to check if the link is a good one or not. The file option will check if the file is free from viruses and the data does not contain any malicious program. The file report option helps to show the environment where the user may decide to let law enforcer such as the police be aware.

Figure 6 is the front end that provides a space for testing any link whether such link is free of any software problem.

Figures 7 and 8 show the interfaces for the help menu and test file, respectively. At the help menu interface, the new user or any first-timer will be able to learn about the app and get familiar with how it works. On the other end, the test file platform provides a space to test a particular file and establish its state whether it is a problem-free file or not.

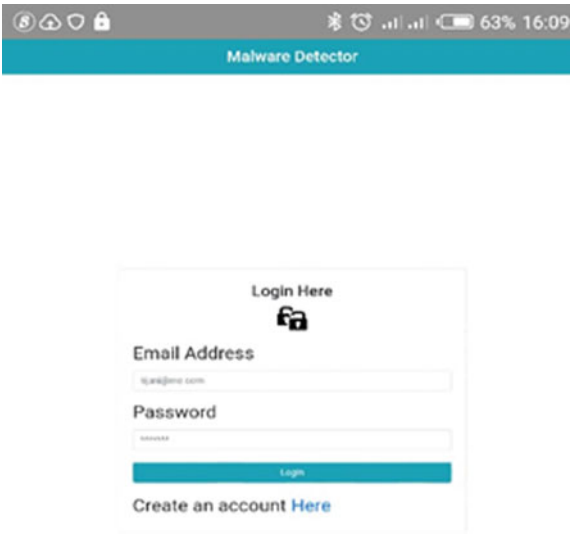

Fig. 4 Link for login

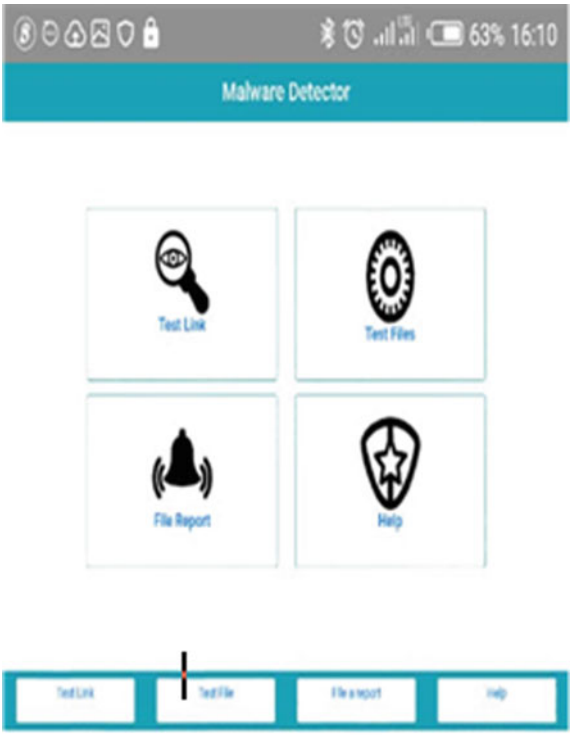

Fig. 5 Links for necessary actions

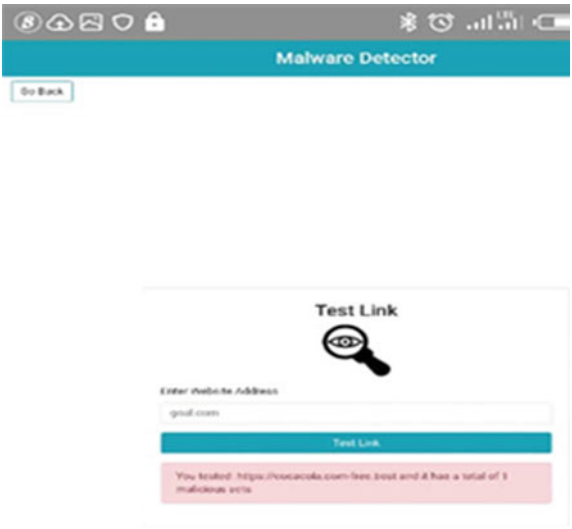

Fig. 6 Test link

Fig. 7 Help

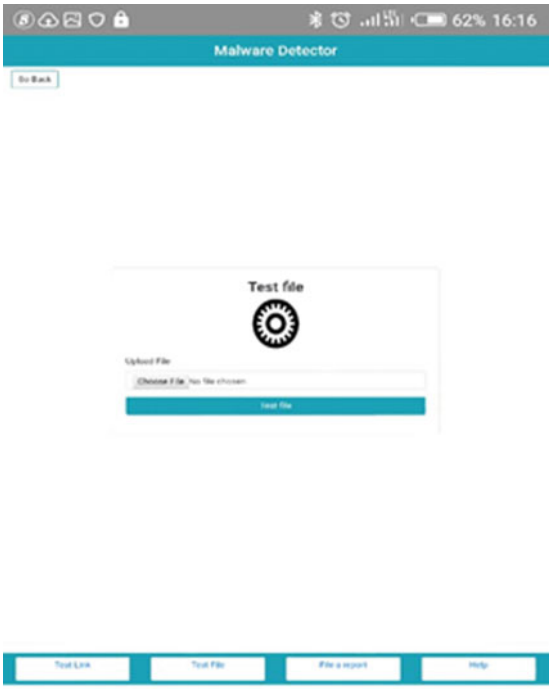

Fig. 8 Test file

5 Conclusion and Future Work

The proposed model was deployed using HTML5, CSS, JQUERY, and PHP to design the front end and back end of the Android-based mobile app, MYSQL was used for the database, and API- VIRUS TOTAL was used for virus detection application. This app has been implemented, and it works on Android mobile phones perfectly. This app can check for viruses, spyware, and malware, and also, it can link the phone caller for the option to send messages or details of any criminal activities to any law enforcer such as a police officer for necessary action. Also, it will disallow any infected data from affecting the receiver system, and it equally blocks such data. This work can further be extended by capturing detailed information of the criminals, block all his channels by which he was carrying out his usual criminal activities. Also, future work should address the identification of the criminal and his locations using the techniques of deep learning and artificial neural network.

Acknowledgements The authors appreciate the sponsorship from Covenant University through its Centre for Research, Innovation and Discovery, Covenant University, Ota Nigeria.

References

1. Omodunbi, B.A., Odiase, P.O., Olaniyan, O.M., Esan, A.O.: Cybercrimes in Nigeria: analysis, detection and prevention. FUOYE J. Eng. Technol. **1**(1), 37–42 (2016)
2. Ishwarya, T.A.S.K.: Cyber crime : prevention and detection **4**(3), 45–48 (2015) https://doi.org/10.17148/IJARCCE.2015.4311
3. Tanui, D.K.: Use of ICT in the detection and prevention of crime in Kenya **6**(9), 62–71 (2016)
4. Rashid, A.M., Al-oqaily, A.T.: Detect and prevent the mobile malware. Int. J. Sci. Res. Publ. IJSRP **5**(5), 9–11 (2015)
5. Agangiba, W.A., Agangiba, M.A.: Journal of Computing: mobile solution for metropolitan crime detection and reporting. J. Emerg. Trends Comput. Inf. Syst. Univ. Cape Town, South Africa **4**(12), 916–921 (2013)
6. Agangiba, W.A., Agangiba, M.A.: Journal of computing: mobile solution for metropolitan crime detection and reporting. J. Emerg. Trends Comput. Inf. Sci. (2019)
7. Bordjiba, H.E., Karbab, E.B., Debbabi, M.: Data-driven approach for automatic telephony threat analysis and campaign detection. Digit. Investig. **24**, S131–S141 (2018). https://doi.org/10.1016/j.diin.2018.01.016
8. Umamaheswari, B., Nithya, P., Chandran, N.S.: Survey on web crime detection using data mining technique **5**(1), 177–184 (2016)
9. Blanes, J., Kirchmaier, T.: The effect of police response time on crime detection ∗ 1–47 (2015)
10. Chen, C., Chen, W., Wang, Y., Lo, C.: Procedia engineering a real-time crime detection system based on lawful interception—a case study of msn messenger (2011). https://doi.org/10.1016/j.proeng.2011.08.304.
11. Starikovskiy, A.: Text messages protection system text messages protection system text messages protection system text messages protection system. Procedia Comput. Sci. **123**, 457–466 (2018). https://doi.org/10.1016/j.procs.2018.01.070

12. Dong, Y., Pinelli, F., Gkoufas, Y., Nabi, Z., Calabrese, F., Chawla, N.V.: Inferring unusual crowd events from mobile phone call detail records **2**, 474–492 (2015) https://doi.org/10.1007/978-3-319-23525-7
13. Khan, J., Abbas, H., Al-Muhtadi, J.: Survey on mobile user's data privacy threats and defense mechanisms. Procedia Comput. Sci. **56**(1), 376–383 (2015). https://doi.org/10.1016/j.procs.2015.07.223
14. Singh, M.M., Bakar, A.A.: A systemic cybercrime stakeholders architectural model a systemic cybercrime stakeholders architectural model. Procedia Comput. Sci. **161**, 1147–1155 (2019). https://doi.org/10.1016/j.procs.2019.11.227
15. Zulkefli, Z., Singh, M.M., Mohd Shariff, A.R., Samsudin, A.: Typosquat cyber crime attack detection via smartphone. Procedia Comput. Sci. **124**, 664–671 (2017). https://doi.org/10.1016/j.procs.2017.12.203
16. Smith, J.L., Smith, M., Smith, J.L.: The perpetration and prevention of cybercrimes. Available at SSRN 1123743
17. Prasanthi, M.M.L.: Cyber crime: prevention and detection. Ijarcce **4**(3), 45–48 (2015). https://doi.org/10.17148/ijarcce.2015.4311
18. Sathish, A., Prathyusha, M., Priyanka, M.: Crime detection and criminbal identification using IOT **4**(1), 2–4 (2018)
19. Hidayanto, B.C., Muhammad, R.F., Kusumawardani, R.P., Syafaat, A.: Network intrusion detection systems analysis using frequent item set mining algorithm FP-max and Apriori. Procedia Comput. Sci. **124**, 751–758 (2017). https://doi.org/10.1016/j.procs.2017.12.214
20. Rakhmawati, N.A., Ferlyando, V., Samopa, F., Astuti, H.M.: A performance evaluation for assessing registered websites. Procedia Comput. Sci. **124**, 714–720 (2017). https://doi.org/10.1016/j.procs.2017.12.209
21. Costin, A., Isacenkova, J., Balduzzi, M., Antipolis, S.: The role of phone numbers in understanding cyber-crime schemes
22. Dabhere, A., Kulkarni, A., Kumbharkar, K., Chhajed, V., Tirth, S.: Crime area detection and criminal data record **6**(1), 510–513 (2015)
23. Bhowmik, R.: Journal of digital forensics, security and law data mining techniques in fraud detection data mining techniques in fraud detection **3**(2) (2008)
24. Hajian, S., Domingo-Ferrer, J., Martinez-Balleste, A.: Discrimination prevention in data mining for intrusion and crime detection. IEEE SSCI 2011 Symp. Ser. Comput. Intell. CICS 2011 IEEE Symp. Comput. Intell. Cyber Secur. 47–54 (2011). https://doi.org/10.1109/CICYBS.2011.5949405
25. Liwandouw, V.B., Wowor, A.D.: The existence of cryptography: a study on instant messaging. Procedia Comput. Sci. **124**, 721–727 (2018). https://doi.org/10.1016/j.procs.2017.12.210
26. Jambhekar, N.D., Misra, S., Dhawale, C.A.: Mobile computing security threats and solution. Int. J. Pharm. Technol. **8**(4), 23075–23086 (2016)
27. Osho, O., Mohammed, U.L., Nimzing, N.N., Uduimoh, A.A., Misra, S.: Forensic analysis of mobile banking apps. Lecture Notes Comput. Sci. **11623**, 613–626 (2019
28. Alhassan, J.K., Oguntoye, R.T., Misra, S., Adewumi, A., Maskeliūnas, R., Damaševičius, R.: Comparative evaluation of mobile forensic tools. Adv. Intell. Syst. Comput. **721**, 105–114 (2018)
29. Osho, O., Musa, F.A., Misra, S., Uduimoh, A.A., Adewunmi, A., Ahuja, R.: AbsoluteSecure: a tri-layered data security system. Commun. Comput. Inf. Sci. **1078**, 243–255 (2019