Signature based Network Intrusion Detection System using Feature Selection on Android

Onyedeke obinna Cyril[1], Taoufik Elmissaoui[2], Okoronkwo M.C[,3], Ihedioha Uchechi .M[4], Chikodili H.Ugwuishiwu[5], Okwume .B. Onyebuchi[6]

Department of Computer Science, University of Kairouan, Tunisia[1]
Innov'Com , SUP'COM,University of Chartage & Higher Institute of Applied Mathematics and Computer Science, University of Kairouan, Tunisia[2]
Department of Computer Science, University of Nigeria, Nsukka (UNN), MNCS, MCPN[3]
Department of Computer Science, University of Nigeria, Nsukka (UNN)[4, 5]
Department of Computer Science, University of Nigeria, Nsukka (UNN)[6]

***Abstract*—This paper Smart Intrusion Detection System (IDS), is a contribution to efforts towards detecting intrusion and malicious activities on Android phone. The goal of this paper is to raise user's awareness of the high rate of intrusions or malicious activities on Android phones and to provide counter measure system for more secured operations. The proposed system (SIDS) detects any intrusion or illegal activities on android and also takes a selfie of the intruder unknown to him/her and keep in the log for the view of the user. The object oriented analysis and design method (OOADM), was adopted in the development. This approach was used to model and develop the system using real intrusion features and processes to detect intrusions more flexibly and efficiently. Signature detection was also used to detect attacks by looking for specific patterns. The system detects intrusions and immediately sends an alert to the user to notify of an illegal or malicious attempt and the location of the intruder.**

Keywords*—Signature Detection; Feature Selection; android phone; Smart Intrusion Detection System (SIDS)

I. INTRODUCTION

Smartphones, tablets, and other mobile platforms are rapidly emerging as popular appliances with progressively amazing computing, networking, and detecting abilities. Smartphones are currently the overwhelming individualized computing devices with so many features, and strength comparable to mini computers. Some of the attractive features of these smartphones include calls, short messages, multimedia, email, video calling, voice dictation, eservices, file exchange, internet browsing, services, etc. According to Pew Research Centre in 2015, about 43% of the global population uses a smartphone device [1]. Also, there were 5.11 billion interesting portable clients worldwide in 2019, and 2.71 billion of them use smart phones, it evaluated that there will be 2.87 billion smartphone clients worldwide in 2020, and 2.5 billion dynamic Android gadgets around the world, this value was based on Google's Play store Statistics, and this implies that the number is higher. These numbers of Android devices and users additionally underscore the size of the fracture challenge and Google hopes to apply essential updates and security principles to all Android gadgets across various renditions, districts, and producers. Android was launched by Google and Open Handset Alliance in September 23, 2008. Android has experience a vast growth since its inception because of its user friendliness, open source, ease of developing and publishing applications.

The ubiquitous usage of Android OS has induced the burst of mobile application market. Google Play is the largest app store followed by Apples App store. According to [2], The Android Applications are available for download through Google Play Store and third party agents. Though intrusion is not specific to android phones; most smart devices are used for e-businesses; which expose both private and financial data to public domain. Several techniques have been proposed and implemented to detect, prevent and reduce malicious intrusions on smartphones.

Notwithstanding, intrusion is any unapproved action on a computer network. Much of the time, such undesirable action retains network assets expected for different utilizations, and about consistently compromises the security of the system as well as its information. Appropriately structuring and sending a system intrusion detection system will help obstruct the interlopers. Recognizing an intrusion relies upon the protectors having a clear understanding of how assaults work [3]. Intrusion activities seek to unsettle the confidentially, availability or integrity of a resource or the controlling applications. As a result of high prevalence, intrusion detection systems (IDS) are provided to checkmate intrusions. IDS is a sort of security measures use to alert the right owner of a device when a person or thing is attempting to bargain data framework through vindictive activities or through security approach encroachment. The Proposed system (SIDS) is focused at developing a model that will identify malicious intrusions on smart phones, through finger print and password validity and also takes a selfie of the intruder unknown to him/her and keep in the log for the view of the user.

The techniques used for detecting intrusion can be arranged into Signature based location and Anomaly based recognition. Signature based detection is termed as misuse detection which helps in the detection of attacks by looking for specific patterns. Here, the dataset has number of occasions and each data must be named as typical or malevolent. In [4], AI calculations are utilized to prepare the informational collection as indicated by their name, and abuse identification strategy is made naturally. Contingent upon the

vigor and earnestness of a mark that is initiated inside the framework, alert reaction or warning is sent to the correct authorities. Anomaly detection strategy is intended to reveal the examples that are a long way from the ordinary and others are hailed as an interruption. Irregularity discovery is helpful for discovering assaults like abuse of convention and administration ports, DoS dependent on made payloads, DoS dependent on volume, cradle flood and other app payload inconsistency [5].

II. Android Malware Detection

Intrusion detection system (IDS) is an instrument for finding attempts to bargain a framework [6]. Possibly, such endeavors can be forestalled; in such case, the framework is called an interruption avoidance framework. Interruption recognition components applied in Android phones depend on indistinguishable standards from instruments utilized in different frameworks (for example PCs and computer networks). In spite of the reality the frameworks are distinctive in their sort and design; the establishments of assurance against assaults continue as before. This takes into consideration the appropriation of existing procedures and their use in the Android security zone. Interruption recognition frameworks can be arranged by the discovery approach and based on the sort of dissected information. Another characterization approach distinguishes the area of the IDS. [6].These classifications are described in this section below.

A. Detection Approach

Intrusion detection systems are ordered by the location approach utilized to distinguish meddling exercises [7]. The most generally discovery strategies are irregularity and abuse location.

Anomaly detection is intended to distinguish malevolent activities through recognizing deviations from an ordinary profile conduct. Despite the fact that this sort of IDSs performs better in distinguishing novel assaults, they ordinarily experience the ill effects of high FP rate. [4]. Signature recognition, is the place the location procedure depends on known marks or patterns, and plans to recognize authentic occurrences from the malignant ones. Without the downside of inconsistency detection, it is solid for recognizing known assaults with low FP rate. However, this sort of IDSs can't recognize obscure assaults or varieties of known ones [4].

B. Android Architecture

Android Stack is based on Linux kernel and it consists of four layers that manage the whole system starting from hardware sensors to the user's high-level apps. It consists of different layers running on one another, the lower ones offering types of assistance to the upper level layers [8]. This architecture explains the functions of each layers on android phones.

The first layer; the Linux Kernel is the most important represents the heart of Android system. It provides the OS services and manages the hardware's functions such as memory, power, drivers, network stack, security settings, shared libraries and hardware abstraction.

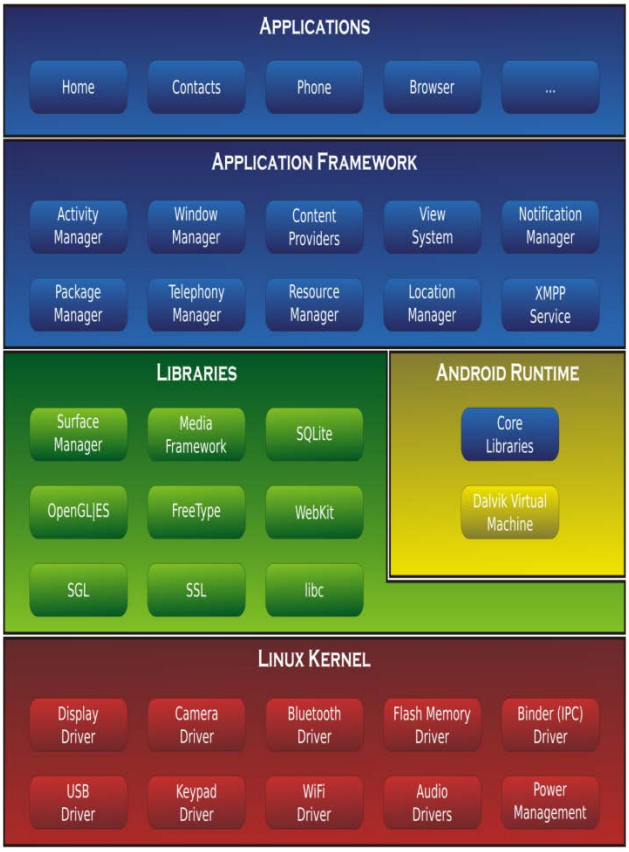

Fig 1. Android's Stack Structure (Adapted from [8]).

The second layer; the library, provides native libraries which are a set of instructions that manage data processing. It provides the open source libraries and the android runtime.

The third layer; the Application Framework, includes the Android APIs. The APIs are classes and interfaces for Android apps' development. This layer interacts with the running apps and manages the basic functions on the device.

The fourth layer; the Application provides the phone's functions to the end-user such as making calls, managing contacts, sending messages, and browsing web. Also this layer provides a set of core applications, such as email client, calendar, browser, maps, contacts, SMS program, gallery, etc. Fig. 1 illustrate the architecture of an android.

C. Feature Selection

The general methodologies for feature elites are classified into three: filter method, wrapper technique, and embedded technique, each component decisions to calculate and make effective use of any of the three element choice systems [9].

The point of feature selection is to discover a subset of the qualities from the first set that are more delegate for the information, and for which the inherent part in the subset are applicable to the expectation; it improves the forecast presentation of Artificial Intelligence models by wiping out noisy factors. It also provide less difficult models that gives better explanations of the complex random procedure, reduced expense of huge trial estimations and subset of factors that can be analyzed for causal induction [10].

D. The Filter Approach

This Approach survey the importance of the highlights from the dataset; the choice of the features depends on the measurements, the arrangement execution is utilized in wrapper techniques as a piece of the component subsets assessment and determination forms. As opposed to wrapper draws near, installed approaches are process of mathematical calculations less serious than wrappers since they consolidate a collaboration between feature determination and learning process. Albeit inserted approaches incorporate a regularized hazard capacity to upgrade the features assigning limit and indicator parameters, it is hard to roll out an improvement in the arrangement model to get better [11].

E. Review of Related Literature

This section, examines a portion of the past methodologies used by researchers for recognizing intrusions. Various approaches have been used to detect intrusions and they can be generally assembled into filter, wrapper and embedded. Below, we give a concise survey of research studies that have been conducted using these approaches.Filters approach don't depend on the classifier calculation, yet utilize other criteria dependent on relationship ideas [9], while Wrappers consider include subsets by the nature of the presentation on a demonstrating calculation, which is taken as a discovery evaluator. Implanted techniques perform include features during the demonstrating calculation's execution [9].The venture embraces the filter techniques for IDS. Because of the continuous development of information dimensionality, include determination as a pre-handling step is turning into a fundamentals part in structure intrusion detection frameworks.

In [12], proposed a novel stage free conduct based oddity discovery system for smartphone. It can distinguish vindictive exercises on smartphone progressively by utilizing solo AI methods called K-implies grouping. The procedure utilized is constrained in light of the fact that it depends on static examination of use consent and system calls.

A host based IDS model for advanced mobile phones and make evidence of idea app for android stage was proposed [13]. The framework arrangements depend upon customers' current system, diverse approach stage is included and discovery instrument is on higher alarm in broad daylight systems. The significant constraint is on client experience dangers, cost creating danger and protection encroaching dangers isn't comprehended.

According to [6], presents a novel AI based IDS to expand the exactness and proficiency of arrangement. The framework diminishes the preparation and testing time from 113.53 and 2.93 to 44.78 and 2.06 on the CIC – IDS 2017, it additionally accomplishes the most elevated F-proportions of 0.998 and least bogus alert rate and dispose of insignificant highlights.

In [9], develop a system that detects any illegal/malicious intrusions in android phones using filter based feature selection algorithm. It evaluates the dependence between features and output classes, also scan to ascertain between legal/illegal users through pin validity. However the authentication level is not strong enough using pin and it does not track the location of the user.

In [14], proposed the utilization of an orderly depiction plot for managing the portrayals used to portray IDS capacities. This methodology ought to take into account an assessment of IDSs dependent on their depictions, without requiring experimentation. The weakness of this methodology is the prerequisite of exact depictions. Right now, such a methodology doesn't exist so executing it is beyond the realm of imagination. This methodology holds a specific guarantee for what's to come.

According to [15], manages the importance of each component in KDD 99 intrusion recognition dataset to the discovery of each class. Their exact outcomes uncovered that a few features (hot Login, number of Compromised situations, number of record creation assignments, visitor login) have no pertinence in intrusion detection. Harsh set level of reliance and reliance proportion of each class were utilized to decide the most isolating features for each class.

In [16], proposed a novel method to deal with break down factually the system traffic unrefined information. The enormous measure of rough information of real system traffic from the IDS is investigated to decide whether traffic is an ordinary or hurtful one. The issue is currently transformed into the sensor system to build the exact recognition rate, on the grounds that no hunt spaces are diminished.

In [17], present the different structures of IDS, measures that help to characterize the level of adequacy of IDS and the continuous work of institutionalization and homogenization of IDS. The system enables us to update the analyzer to find conceivable new assaults or varieties of assaults. Their limitations don't guarantee 100% security, ridiculous and the disservice of this arrangement is the rate of FP because of strange or unordinary conduct of clients, who are not really hurtful.

In [18], proposed a framework so as to improve the security of the portable applications which will assess the versatile applications security dependent on the distributed computing stage and information mining. The assessment results shows that it is reasonable to use appropriated computing stage and information mining to confirm all put away applications routinely to filter through malware applications from versatile application markets. The weakness is the moving of the security usefulness into the cloud could likewise be perilous, if not all pieces of the phone can be imitated into the cloud.

In [19], evaluated data in regard to classifiers configuration, utilized dataset, feature extraction, clustering strategies, exactness location measures and so on. The work of numerous and cross breed classifiers, improves the precision of the grouping and encourages understanding troublesome issues. The shortcoming is that binomial or typical (measurable circulations) can't delineate example acknowledgment conduct, which implies that standard systems of parametric techniques may not work.

In [20], proposed another solid half breed technique for an oddity system based IDS utilizing artificial bee colony (ABC) and Adaptive Boosting calculations (ADA Boost) so as to pick up a high recognition rate with low FP rate. The exactness and

identification rate of this technique has been improved in correlation with unbelievable strategies. The shortcoming is the bogus alert report of intrusion to the system and intrusion detection precision that occurs because of the high volume of system information.

According to [21] proposed a mutual data based calculation that logically chooses the ideal element for grouping. The evaluation results shows that the feature selection calculation contributes progressively basic features(Logs records, hot logins, number of compromised condition) for least square help vector machine based interruption discovery framework for a better precision and lower computational expense. The deficiency is that "huge information" thwarts the entire detection process and may prompt inadmissible grouping precision because of the computational challenges.

In [22], used both static and dynamic investigation to recognize malware in android applications. They consolidated the static investigation (consent) and dynamic examination (System call following) with AI. They performed static investigation by removing authorizations from the Android's manifest.xml record and analysed the complexity between the quantity of consents mentioned by favourable and vindictive applications. They understood that the quantity of authorizations mentioned by charitable and dangerous application is marginally the equivalent. This strategy was tried on different benevolent and threatening applications.

III. Description of the Existing System

Based on the literature reviewed, the previous work done on the existing system of IDS specifically those that use anomaly based approached is described as follows:

1) Most of the system of IDS authentication access is through pin and emails.

2) The system barely tracks the location of the phones.

3) They don't have a reliable accountability system (i.e. keeping a records of all activities carried out on the phone – like a shot of the intruder face unknown to him and send to as MMS to the user's phone and also kept on the app for record purpose.

4) One noteworthy issue of the current framework is the false alert that is brought about by ICMP (web control message convention). This is a mistake announcing convention arrange gadget like router/host use to create blunder messages and operational data showing that a mentioned administration isn't accessible or that a host/router couldn't be come to.

A. Analysis of the Proposed System

The proposed system seeks to address all the problems identified in the existing system by effectively detecting intrusions in Android phones. The following are the features of the proposed system:

1) The proposed system authentication access is through finger print and password.

2) The system has a GPS Tracker to help in the location of the phone.

3) The system has a feature that helps take a selfie of the intruders face during attempt on the phone and sent the intruders face to the MMS of the user other phone and also keeps all facial logs attempts for record purpose .

4) The problem of false alarm is avoided because the proposed system major alert agent is through SMS, MMS and not e-mail that requires ICMP.

5) The proposed system is design in a format that makes installation very simple and easy for the user thereby making navigation accessible.

The role of each actor representing the system flow and activities carried out:

1) Smart intrusion detection system (SIDS): This is the proposed application; its role is to detect, Filter and authenticate Intrusion.

2) User: He/she will download/install the app, configure settings and also check intruders' selfie records.

3) Sensor Agent: The agent audit, selfie of intruder, log and mail alert of an attempt to the user. Fig. 2 present a Use Case diagram of the proposed system (SIDS).

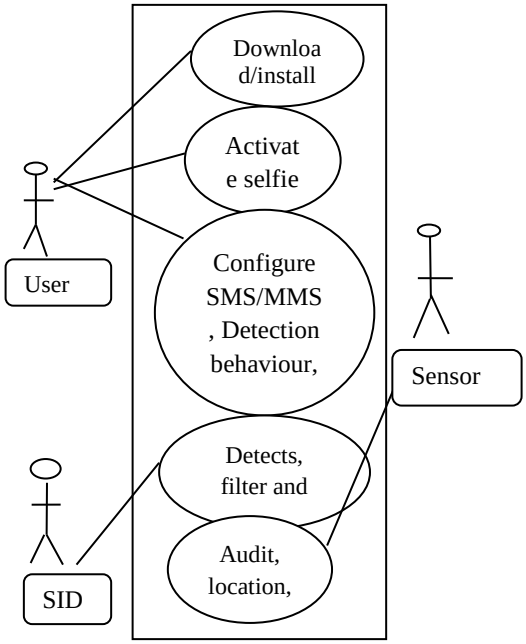

Fig 2. Use-Case Diagrams of the System.

B. System Architecture

The architectural design of the Proposed System (SIDS) is of 4 (four) tiers as shown in Fig. 3. SIDS was designed based on four layers that manage the activities on the system starting from;

Data Collection are sensors in charge of information accumulation and are in this manner the data wellsprings of IDS. This data is drawn from different sources, for example, enlisted information and log documents. **Data Pro-Processing** in this stage information gets changed or encoded to carry it to such an express, that the machine can without much of a

stretch parse it and are processed to generate the basic features.

Attack Recognition, here the system compare information's in the dataset, after analysing the data it makes decision if it's a normal flow or an intrusion.

Result is the outcome that tells if an intrusion is recognized. It takes the information and contrast and the prepared dataset, and match on the off chance that the information is assaulted or typical, on the off chance that the information is assault, at that point an alarm will be sent to the phone number of the client (showing intrusion and location). Fig. 3 presents the structure of the proposed system (SIDS).

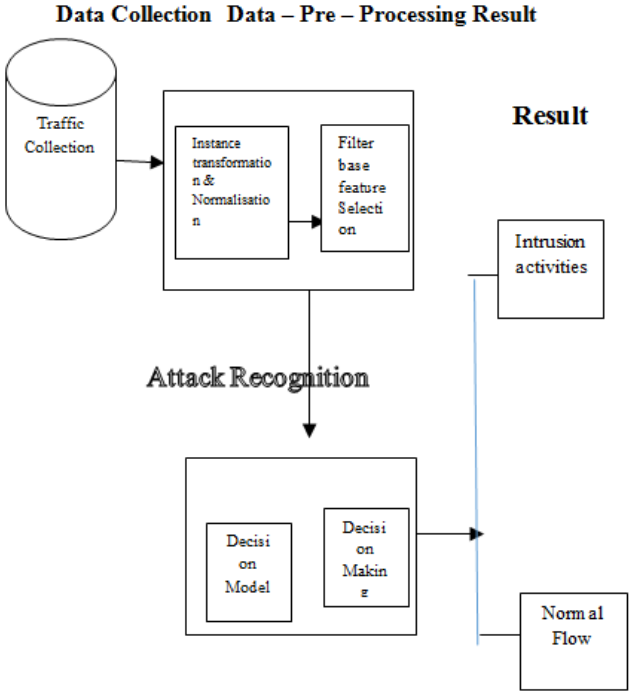

Fig 3. The Structure of the Proposed System (SIDS).

IV. System Implementation

The system implementation is the development of the new system or application following the laid plans from analysis and design stage. This chapter depicts how the plan from the previous section is executed with the aim of providing a proficient system to detection of intrusion on Android phone. Apparatuses and techniques used to actualize are presented in this section.

A. Choice of Development Environment

The integrated development environment (IDE) used in the development of this work is the Android studio 3.5.3, JRE 1.8.0_202-release-1483-b03 amd64, JVM: OpenJDK 64-Bit Server VM by JetBrains s.r.o on which the source codes are written, compiled and uploaded on Google Play Store. Android Studio offers numerous features that improves profitability when building Android applications, for example, Gradle-based system which is use to manage all dependencies (to build, test, run and package your app), Android Virtual Device (Emulator) also helps run and debug apps in the Android studio. The programming languages employed in this project are Java while Shared Preferences integrated database management system was used.

B. Implementation Architecture

The implementation architecture of the SIDS is represented in Fig. 4 below. It is made up of the various components of the software modules and their linkages. Fig. 4 illustrates the Implementation Architecture of the system.

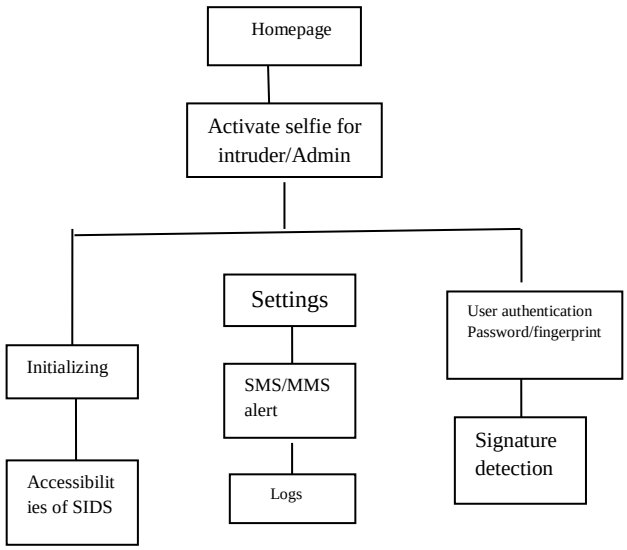

Fig 4. The Implementation Architecture.

V. Result and Discussions

Smart intrusion detection system (SIDS) is a mobile application developed using Java. After the application has been downloaded and installed, then activation of selfie for intruder and the Admin, also the user will configure SMS and location alert, number of attempts, SMS number. If an intrusion is detected, immediately the alert agent sends an SMS and MMS (that contains a statement indicating an intrusion and also the location of the phone), while a selfie of the intruder will be kept in the app log for the users view. The problem of false alarm is avoided because the proposed system major alert agent is through SMS and not only email that requires ICMP (which sends error messages to email indicating service is not available or not reachable).

Fig 5. Home Page of User Phone of SIDS.

The figure's below is an illustration of the output (result) displayed of an intrusion attempt. Fig. 5, 6, 7, 8, 9 and 10 presents the screenshots of the output for the proposed system (SIDS).

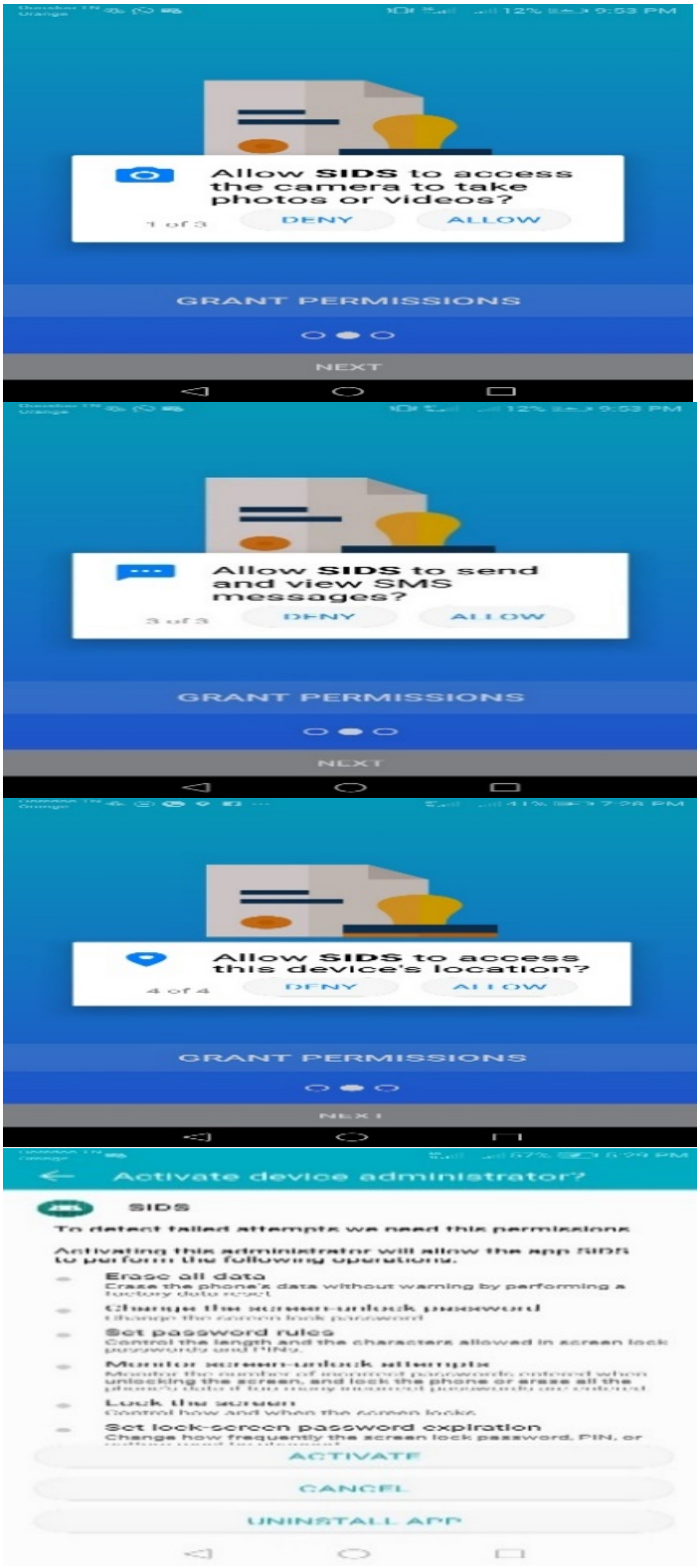

Fig 6. Activating Intruder Selfie and Admin of SIDS.

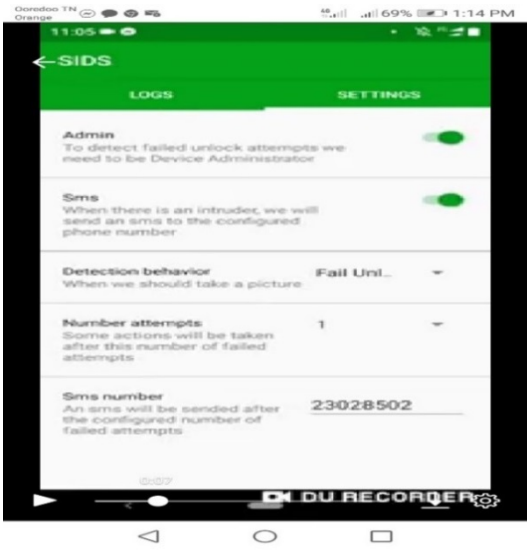

Fig 7. User Configuration Settings of SIDS.

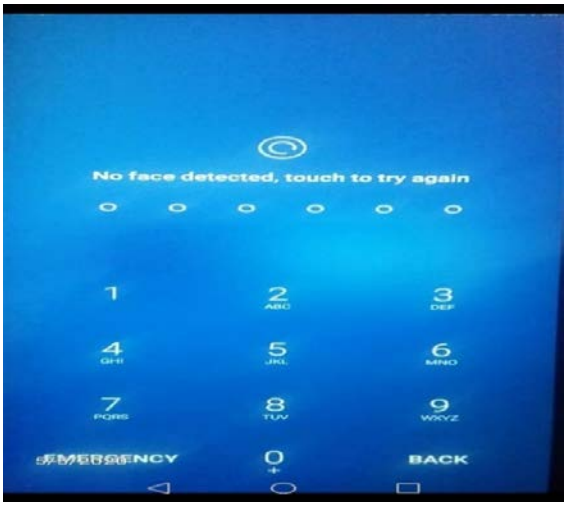

Fig 8. User Login Password of SIDS.

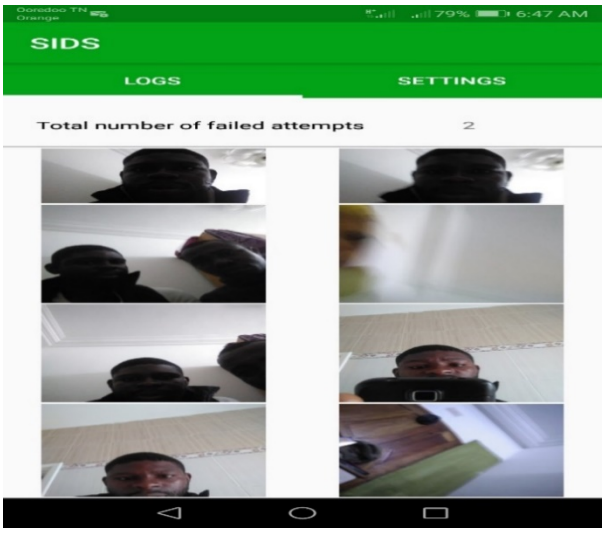

Fig 9. Intruder Selfie of SIDS.

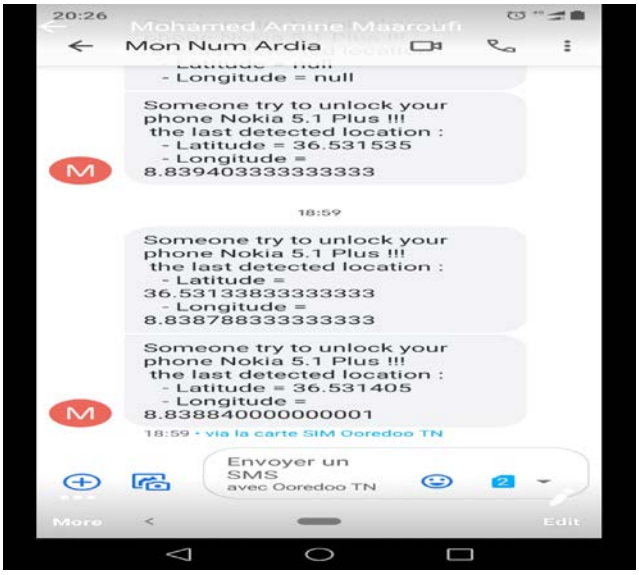

Fig 10. SMS Alert of an Intrusion with Location of the Phone of SIDS.

A. Conclusion and Future Work

In conclusion, Smart IDS is introduced in order to detect intrusions when other defensive measures fall flat, by inactively observing system events and searching for security related issues. This paper gives a successful and productive procedure to detect noxious activities (attempt of authentication, selfie records of intruder) in the Phone. We have had the option to plan and build up an application named SIDS that can detect intrusion on Android Phone. SIDS was developed using Android Studio, Android SDK (software development kit) written with Java. The Object Oriented Analysis and Design Methodology (OOADM) were used for the analysis, design and development of the system and Unified Modeling Language (UML) to model the system.

The future work will involve the detection and screenshot of all activities of the intruder on the android phone. These activities will be sent to the email of the user and also kept on the log for the user's view with finger print required for access.

ACKNOWLEDGMENT

We thank all the authors for their huge contributions in this paper. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

[1] Drake Bear. "How many people own smartphones around the world - Business Insider," *Available: http://www.businessinsider.com/*how-many-people-own-smartphones-saround-the-world. 2017,

[2] Okoronkwo M.C and Onyedeke O.C. "An intrusion detection system(IDS) on android phones using a filter base feature selection algorithm," *Int. journal of innovative research and developmenyt.*, vol.8, issue 11, pp. 101. 2019.

[3] Robert Moskowitz. "Network Intrusion: methods of Attack". *RVS Conference*. 2020.

[4] Ansam Khraisat, Igbal Gondal, Peter Vamplew & Joarder Kamruzzaman. "Survey of intrusion detection systems: techniques, datasets and challenges". *Scientific Data*. Vol 20, 2019.

[5] Dr. S. Vijayaram and Ms. Maria."Intrusion Detection System – A Study", *International Journal of security, Privacy and Trust Management (IJSPTM).* Vol 4, issue 1. 2015.

[6] Martin Borek. "Intrusion Detection System for Android: Linux Kernel System calls Analysis". *School Of Information and Communication Technology, Sweden. 2017.*

[7] D. Ashok Kumar, S. T. Venugopalan. "Intrusion Detection Systems: A Review". *International Journal of Advance Research in computer science.* Vol 8, issue 8. 2017.

[8] V. Grampurohit. "Android App Malware Detection," *International Institute of Information Technology, India.* 2016.

[9] P. Garcı´a-Teodoroa, *, J. Dı´az-Verdejoa , G. Macia´-Ferna´ndeza , E. Va´zquezb. "Anomaly-based network intrusion detection: Techniques, systems and challenges". Journal homepage: *www.elsevier.com/locate/cose,* computers & security. Vol 28, Pp 18–28. 2009.

[10] Yubin Kuang. "A Comparative Study on Feature Selection Methods and Their Applications in Causal Inference". Department of Computer Science, Faculty of Science, *Lund University*, pp. 1-3. 2009.

[11] Yuyang Zhou, Guang Cheng, Shanqing Jiang, and Mian Dai. "An Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier". *School of cyber Science and Engineering*. 2019.

[12] Khurram Majeed1, DrYanguo Jing2, DrDusica Novakovic3, and Prof Karim Ouazzane4. "Behaviour based anomaly detection for smart phones using machine learning Algorithm". *International conference on Computer Science and Information Systems (ICSIS)* Oct 17-18. 2014.

[13] Muhamed Halilovic, AbdulhamitSubasi. "Intrusion Detection on Smartphones". *International Burch University Faculty of Engineering and Information Technologies*, Department of Information Technologies, Sarajevo, Bosnia and Herzegovina. 2014.

[14] Alessandri, D. "Using Rule-Based Activity Descriptions to Evaluate Intrusion Detection Systems". *Recent Advances in Intrusion Detection, Third International Workshop.* 2017.

[15] Adetunmbi A.Olusola, AdeolaS. Oladele, DaramolaO,.Abosede. "Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features". *Proceedings of the World Congress on Engineering and Computer Science*, Vol 1, Pp 2663-2664. 2010.

[16] A.A. Waskita, H. Suhartantoy, P.D. Persadhazy, L.T. Handoko. "A simple statistical analysis approach for Intrusion Detection System". *Center for Development of Nuclear Informatics-National Nuclear Energy Agency*, Pp 1.2014.

[17] Yousef Farhaoui, Ahmed Asimi. "Creating a Complete Model of an Intrusion Detection System effective on the LAN". *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 3, No. 5, Pp 1-2. 2012.

[18] Mr. Akash J Wadate, Prof. N. R Chopde, Prof. D. R. Datar. "Malware Detection System for Android Mobile Applications". *International Journal of Engineering Research and General Science*, Vol 4, Issue 1, Pp 21-22. 2016.

[19] Abdulla Amin Aburomman, Mamun Bin IbneReaz. "Evolution of Intrusion Detection Systems Based on Machine Learning Methods". *Australian Journal of Basic and Applied Sciences*, Vol 7, no 7, Pp 46. 2013.

[20] Mehrnaz Mazini[a], Babak Shirazi[b], Iraj Mahdavi[b]. "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and Ada Boost algorithms". *Journal of King Saud University*, Pp 799-806, 2018.

[21] Mohammed A, Ambusaidi, Xiangjian He, Priyadarsi Nanda, Zhiyuan Tan. "Building an intrusion detection system using a filter-based feature selection algorithm". *IEEE transactions on computers*, vol 1, no 1 Pp 1-3. 2014.

[22] P. Kaushik and A. Jain. "Malware Detection Techniques in Android," *Internationnal Journal. Comput. Appl.*, vol. 122, no. 17. 2015.

ONYEDEKE OBINNA CYRIL received his B.Sc. degree in computer science from Renaissance University, Nigeria (2011), M.Sc. degree in computer science from University of Nigeria, Nsukka (2020). His current address is Department of Computer Science, university of Kairouan, Tunisia. He has published over nine international journals and counting. He is a nominated Africom Scholar. He also has certification of award of achievement in project management from University of California, Berkeley. His current research interest includes: Network Security, Cryptology, information system. 0binna046@gmail.com

PROF. TAOUFIK ELMISSAOUI is an associate professor in the higher institute of Applied Mathematics and computer science, university of Kairouan, Tunisia since 2014. He is actually member of ELIVES project, point of contact of AFRICOM project and coordinator of the TNIS master in the higher institute of Applied mathematics and computer science. From 2006 to 2007 he was a staff engineer with Norkatech, Tunisia. From 2007 to 2013 he was an assistance professor in the Sousse University, Tunisia. He received his PhD, master's degree and engineering degree in telecommunications form National Engineering School of Tunisia ENIT). His research focuses on medical radar system and behind wall localization. elmissaoui.enit@gmail.com,

Dr. Okoronkwo, M. C (MSc, PhD), Senior lecturer, Department of Computer Science at University of Nigeria, Nsukka (UNN), MNCS, MCPN. Research interest is in ICT in Governance, Big Data, Artificial Intelligence and Networking. matthew.okoronkwo@unn.edu.ng.

Ihedioha Uchechi Michael is an Academic member of University of Nigeria Nsukka. My Current address is Department of computer Science, University of Kairuoan, Tunisia. I have participated in the publication of five journal articles till date and counting. I am also an Africom nominated Scholar. I hold a bachelor's degree in Computer science from the University of Nigeria Nsukka and an MSc in Information Technology from the National Open University of Nigeria and currently rounding off a second MSc in System Engineering in an Africom scholarship exchange program between the Universities of Nigeria Nsukka and the University of Kairuoan, Tunisia. mikeuche2002@gmail.com

Dr. Chikodili H.Ugwuishiwu is a lecturer and research fellow in the Department of Computer Science, University of Nigeria, Nsukka. She holds different degrees including BSc. (2004), MSc. (2009) and Ph.D (2018), all from Computer Science Department in University of Nigeria Nsukka. Her areas of research interest are on Information System (IS), Computer modeling and Simulation and Data mining. She has published many articles in journals and conferences, both local and international. She has also attended many local and international workshops. She is a member of professional bodies including Computer Professionals Registration Council of Nigeria (CPN), Nigeria Computer Society (NCS), Nigeria Women in Information Technology (NIWIIT), Organisation for Women in Science for the developing world (OWSD) and Association of Information System (AIS). chikodili.ugwuishiwu@unn.edu.ng

Okwume Benedette Onyebuchi, a staff of University of Nigeria Nsukka. She holds a BSc, MSc in computer science and currently running her PHD in the computer science department, University of Nigeria Nsukka. Areas of interest include Artificial Intelligence, Data Mining, and Queuing Theory and information system. okwumebenedette@gmail.com