**ANOMALY BASED INTRUSION DETECTION SYSTEM (IDS) USING HYBRID TECHNIQUES ON ANDROID.**

***Taoufik Elmissaoui1*, *Obayi Adaora Angela* 2, Uzo Izuchukwu Uchenna2.**

***Onyedeke Obinna Cyril2,* Olayiwola Abisola Ayomide 3, *Famuyiwa, Kolawole Samuel A*4,**

1*Innov’Com , SUP’COM,University of Chartage && Higher institute of Applied Mathematics and computer science, university of Kairouan, Tunisia.;* [*elmissaoui.enit@gmail.com*](mailto:elmissaoui.enit@gmail.com)*.*

2*Department of Computer Science, University of Nigeria, Nsukka, Nigeria*   
[cyril002@yahoo.com](mailto:cyril002@yahoo.com)

2*Department of Computer Science, University of Nigeria, Nsukka, Nigeria*   
[cyril002@yahoo.com](mailto:cyril002@yahoo.com)

*2Department of Computer Science, University of Nigeria, Nsukka, Nigeria*[*Obinna046@gmail.com*](mailto:Obinna046@gmail.com)*,*

 ORCID iD: <https://orcid.org/0000-0003-4571-3031>

*3Department of Computer engineering, Olabisi Onabanjo University, Ago-iwoye, Nigeria*

[cyril8216*@gmail.com*](mailto:cyril8216@gmail.com)

*4Department of Computer engineering, OlabisiOnabanjo University, Ago-iwoye, Nigeria*

[cyril8216*@gmail.com*](mailto:cyril8216@gmail.com)

**Abstract**

A rise in the variety and level of sophistication of intrusion detection systems (IDS) targeting popular platforms occurred simultaneously with the rapid development of Android technologies and their widespread acceptance by users. Android phones' intrusion detection systems are based on the same principles as those found in other systems like personal computers and computer networks. The fundamentals of attack defense remain the same, even though the systems differ in type and architecture. The point of this paper is to raise client's attention to the high pace of interruptions or vindictive exercises on Android telephones and to give counter measure framework to additional got activities. This examination gives a fruitful and useful technique to recognize poisonous activities (endeavor of validation, selfie records of gatecrasher) in the phone.. Hybrid techniques was adopted in this research for detection of intrusions. These techniques has a high rate of detecting malicious patterns and it also inspects the behaviour of the app in a runtime environment and display the app's dynamic behavior and framework responses.

***Keywords:*** malware activities, intrusion detection system, android phone, hybrid techniques.

**1.0 Introduction**

Intrusion is any activity that undertakings to settle the secretly, accessibility or trustworthiness of an asset or on the other hand the controlling applications. Because of high predominance, interruption location frameworks are given to checkmate interferences. IDS is a sort of wellbeing programming intended to hence caution heads when a person or thing is trying to bargain data structure through harmful exercises or through security approach infringement [1]. An IDS works by looking at framework rehearses through checking at shortcomings in the construction, the unwavering quality of records and organizing assessments of models subject to known assaults. It likewise screens the Web to check for any of the latest dangers which could accomplish assault. There are various IDS like static methodologies, dynamic procedure among others. This undertaking embraced the hybrid methodology on android application. Android was shipped off by Google and Open Handset Partnership in September 23, 2008. Android has experience a colossal improvement since its beginning stage in light of its comfort, open source, ease of making and flowing applications. With an expected 81% offer in 2015, Android has turned into the most generally utilized working framework on current cell phones. As per the report, 432 million high level mobile phones were sold, with the Android working framework representing 81.7 percent of the market and Apple's iOS representing 17.9 percent. The expansion of adaptable application markets has been ignited by the far reaching utilization of the Android working framework. Google Play is the best application store followed by Apples Application store. From 16 thousand applications close to the completion of 2009 to around 2.8 million at Walk, 2017, Google Play has encountered fast development. Android applications can be downloaded from the Google Play Store and from outside specialists [2]. To identify, prevent, and reduce IDS on Android phones, a few methods have been proposed and implemented. There are three types of strategies used to distinguish Android IDS: static, dynamic, and half breed. While static methods don't run an application, they do evaluate it and decompile its code. Mark confirmation, network addresses, Programming interface calls, consent examination, and other boundaries can all be checked using static methods. Dynamic systems which incorporates area of IDS at run-time, screens application effectively during their execution. A few aspects of an application, such as framework calls and Programming interface following, are separated during dynamic procedures to determine whether the application is benign or malicious. Hybrid systems has a high speed of perceiving malignant models and it moreover surveys the approach to acting of the application in a run time climate and screens the application's dynamic way to deal with acting and design reactions.

**2.0 Detection Approach**

Interruption discovery frameworks are referenced by the area approach used to see intruding activities [4]. The most all around disclosure frameworks are anomaly and abuse region. Peculiarity discovery is planned to recognize noxious exercises through perceiving deviations from a common profile direct. Notwithstanding the despite their superior ability to distinguish novel attacks, these IDSs typically suffer from the negative impacts of a high FP rate. [5]. Signature identification is the area method that uses known checks or examples to distinguish valid events from dangerous ones. It is effective at recognizing known attacks with a low FP rate without the drawback of irregularity recognition. Nevertheless, this sort of IDSs can't see faint attacks or mixes of known ones [5].

**2.1 Android Application Development**

The Java source code is compiled into Dalvik Virtual Machine (DVM) executable byte code and stored in a DEX file for Android applications. Local libraries for Android applications are written in C. A ZIP archive file with the suffix "APK" contains the application's DEX file, manifest, all assets, certificates, and own libraries. Customers can download this APK file from Google Play. While unloading an APK file, the Android application's source code cannot be viewed in plain text.

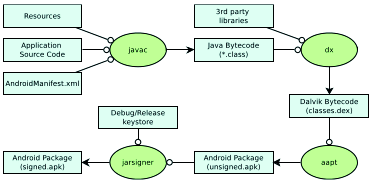
****

Figure 1: Construct interaction of an Android application (Adjusted from [9])

**2.1.2 Android Malware**

A malignant application or malware implies an application that can be used to mull over movement of a contraption, take data, and evade access controls or regardless reason hurt on the terminal of the host [9]. This part presents the Android malware risk and improvement.

**2.1.3 Malware**

Aggressors need to get to a device by installing malware on it. The objective is to take data or damage the device. Malware is spread by tricking the user into installing an application that looks real or by taking advantage of a device's weakness, such as a security hole in the browser.

**2.1.4 Spyware**

Spyware is uncommonly typical in the Android stage, getting fragile information from a setback's system also, transfer this data to the attacker's organized system. Spyware can be business and unsafe. Business spyware is software that is installed on a customer's phone by someone else specifically to watch out for the client, while dangerous spyware surreptitiously take data and impart it to a pariah.

**2.1.5 Gray-ware**

The primary objective of dim product is to monitor customers who introduced the product on their own because they believed it to be genuine programming. This is part of the way right because the creators include actual utility as advertised.

**2.1.6 Fraud-ware**

In order to introduce a fraud-ware-based application, the client is deceived into believing that it will become fully functional after from the system, for instance, the client's area book or his examining history.

**2.1.7 Trojan**

Trojans are programs that say they are useful but do horrible things behind the scenes, like downloading more malware, changing the settings on the framework, or contaminating other files on it. The majority of Android malware are Trojans. Due to the sandboxing model, malware developers are largely unable to access the attack vectors used by infections and worms. The malignant code is for the most part included into genuine applications, which are then altered as the principal application. The majority of the applications used for this purpose are paid ones that have been repurposed as free ones for use in non-business sectors.

**2.1.8 Root exploit**

Root takes advantage of are possible on Android to supervise the device, but are seen as a cutting edge that cuts the two different ways among the security neighborhood. Establishing can give the user control over a device and any application that accesses the root freedoms in a similar way. Root praises given to a poisonous application can thoroughly mull over device, because the client might think that the application would kill the root cause. The harmful application, like most Trojans, pretends to be normal until it is installed on the client's device. It endeavors, when presented, to use something like one root exploits to get root agree to the contraption. An application can replace, modify, and present other applications as it sees fit with root access.

**2.1.9 Bot**

Bots are a new type of portable malware that gives the malware essayist control over completely tainted devices. They talk to what's more, get headings from somewhere around one Request and Control (C&C) server. The engineers of malware obfuscate their code and use encryption to conceal essential information from detection. A bot can also introduce additional applications without the need for client information or mediation.

**2.2 General Technique for Feature Selection**

The three most common approaches to feature selection are as follows: static, dynamic, and hybrid techniques are all available. Any one of the three element choice systems is used in any component determination calculation [4].

1. Static technique extracts highlights from the app to identify dangerous models, record without executing the application. Many features, such as consents, broadcast beneficiaries, APIs, purposes, information stream, control stream, gear parts, and so on, are removed from the application's source code. Assent and Programming interface calls are the static highlights that are used the most frequently. Because they are distinct from the AndroidManifest.xml application and have a significant impact on the malware recognition rate.

2. Dynamic technique looks at the approach to acting of the application in a run time climate and screens the application's dynamic way to deal with acting and responses in the framework. It runs the rogue application in a controlled environment known as a sandbox. Network affiliations, ability calls, resource use, system calls, etc are among the powerful features analyzed.

3. Hybrid technique: These consolidates highlights decision procedures that are liberated from any pointers, filtering through highlights that have negligible chance to be useful in examination of data. These methodologies has a high pace of distinguishing vindictive examples and it likewise examines the way of behaving of the application in a runtime environment and examines its dynamic behavior and framework responses. Such strategies are typically computationally more reasonable than the other two and compelling in IDS. The flow chart of the system below:

Download and install app

Activate selfie of intruder/ Admin

Settings

Configure (SMS, No of attempt, SMS no, detection behaviour

Input password

Info correct?

No

Yes

View and access your file, app

‘

Send alert with image of intruder

Figure 2: Flowchart diagram to monitor intrusion

**2.3 Review of Related Literature**

In this segment, we concentrate on a piece of the past techniques required by experts for perceiving harmful applications. Static and dynamic investigations can typically be combined from the various methods used to identify malicious applications. We provide a succinct overview of study focuses that have been conducted using both static and dynamic investigation below.

Work was absent because they perceived the malware as one of the most significant threats to a developing PC and correspondence development, according to [5]. It saw the: classification of malware, estimates of malware's appearance, activities, and methods for anticipating and eliminating malware if it actually disrupts structure Right when a circumstance has been subverted by a malware, an aggressor would then have the decision to dispatch their attack through a few gadgets like social event sniffer, port scanner, shortcoming scanner, secret word wafers among others.

In [6], proposed an original stage independent direct based irregularity acknowledgment structure for cell. It can perceive poisonous activities on cell in certified - time by using independent artificial intelligence methodology called K-suggests gathering. The strategies used is limited considering the way that they depend upon static assessment of use endorsement and framework calls.

According to [7] presented a survey of various procedures and techniques in understanding the thoughts of channel based highlight choice. The various kinds of: incorporate decision, classes of regulated highlight choice and relationship of channel and covering. It limits abundance, clears upheaval and expands the meaning of the goal all together. The duplication of colossal data inside spaces presents phenomenal test to data mining.

According to [8], another host-based IDS model for advanced cells was proposed, and an Android stage application was confirmed. The structure approaches depends upon clients' continuous association, different course of action level is applied and disclosure framework is on higher caution out in the open associations. The most significant restriction is the uncertainty surrounding customer experience risks, cost-creating risks, and security-encroaching risks.

In [9], presents a one of a kind man-made knowledge based IDS to develop the precision and practicality of depiction. On the CIC - IDS 2017, the system decreases the preparation and testing time from 113.53 and 2.93 to 44.78 and 2.06, achieves the most raised F-degrees of 0.998, has the most un-counterfeit issue rate, and clears out irrelevant features.

According to [10], Proposed a system that identifies any unlawful/malignant interruptions in android telephones utilizing channel based highlight determination calculation. It assess the reliance among highlights and result classes, likewise output to determine between legitimate/unlawful clients through secret phrase legitimacy. The shortcoming of the framework is that the confirmation level isn't sufficient utilizing pin and it can't follow the area of the client.

As per [12], assessed information in regard to classifiers arrangement, used dataset, highlight extraction, grouping methodologies, precision area gauges, etc. Crafted by various and cross variety classifiers, works on the accuracy of the gathering and empowers grasping inconvenient issues. The insufficiency is that binomial or typical (quantifiable streams) can't portray model affirmation direct, which accumulates that standard designs of parametric strategies may not work.

As per [13], proposed one stronger mutt strategy for a peculiarity framework based IDS (NIDS) using fake honey bee state (ABC) and Versatile Helping computations (ADA Lift) to get a high rate of acknowledgment but a low rate of false positives. The accuracy and ID speed of this methodology has been chipped away at regarding astonishing procedures. The sham alarm report of interference to the framework and interference ID accuracy, both of which are affected by the large volume of framework data, are the deficiencies. KDD-cup 99 is a type of dataset used to evaluate the presentation of an interruption location structure point of reference least square-support vector machine (LSSVM - IDS) in the request for attacks.

According to [14], reviewed computations in data mining using (learning revelation in data set) KDD-cup 99 and broke down their results that were come to. A great deal of evaluation was surveyed on KDD dataset and it was used for seeing the classes of attacks. The inadequacy stems from the fact that the computer-based intelligence estimates that were used as classifiers for the KDD cup educational assortment do not provide much assurance for detecting client-to-root (U2R) and remote-to-local (R2L) attacks.

A clever strategy for handling distinct rough data pertaining to the framework's traffic was proposed in [15]. In order to determine whether the traffic is typical or destructive, the significant measure of unpleasant information of genuine system traffic from the Interference Recognizable proof Structure is explored. Since there are no diminished pursue spaces, the issue is at present being coordinated into the sensor structure to expand the precision acknowledgment rate.

According to [16], proposed a common information based estimation that consistently picks the best component for gathering. The assessment results shows that the component decision assessment contributes consistently key elements for least square help vector with machining based impedance disclosure framework to accomplish better exactness and lower computational expense differentiated and the top tier methodologies. That's what the deficiency is "enormous data" thwart the entire distinguishing proof cycle and may provoke unacceptable gathering accuracy in light of the computational difficulties in dealing with such data.

According to [17], proposed a structure to manage the security of the steady applications which will assess the flexible applications security subject to the circumnavigated figuring stage and information mining. The delayed consequences of the appraisal show that it is sensible to use information mining and passed handling stage on to routinely check all held applications to channel malware applications from adaptable application markets. It's conceivable that not the telephone's all's parts can be imitated in the cloud, and the exchange of safety highlights to the cloud could likewise be unsafe.

[18] Suggested a proactive system for distinguishing zero-day Android malware that didn't depend on malware tests or their scores to recognize potential security gambles presented by untrusted applications. Chance Ranker is a PC structure that scales applications to decide if they display hazardous way of behaving. By isolating the control stream and information stream from the code way, they drove static testing on the figured Dalvik bytecode in each application. In less than four days, they gathered 118,318 applications from various Android platforms. They perceived 3281 hazardous applications thus of their investigation.

**2.3.1Table 2: Comparison of the articles reviewed showing strength/weakness.**

|  |  |  |  |
| --- | --- | --- | --- |
| S/n | **System/Article** | **Weakness** | **Strength** |
| 1. | Malware Detection, Its Classification Schemes, and Supportive Software Agents [6] | Exactly when a design has been undermined by a malware, an aggressor would then have the choice to dispatch their assault through several devices like bundle sniffer, port scanner, defencelessness scanner, secret word wafer among others. | It recognized the sort of malware, its construction, its exercises, and techniques for forestalling and disposing of malware if it at last pollutes a framework. |
| 2. | Intrusion Detection System – A Study [7]. | Unsafe clients or programmers utilize the alliance's inner designs to gather data's and cause shortcomings like Programming bugs, Pass in association, giving designs to default plan. | Its methods, systems and computations help to distinguish attacks used by developers for getting significant information. |
| 3. | Feature Selection Methods and Their Uses in Causal Inference: A Comparative Study [8] | The dissemination P(x,y) doesn't necessarily in every case have a solid exploratory measure from the data, particularly for high-layered genomic information. Surveying P(x,y) is obviously a more troublesome issue than judicious illustrating. | During the time spent building a model, highlight determination assumes an essential part in wiping out unessential factors and working on model execution by lessening commotion and dimensionality. |
| 4. | Filter-based Feature Selection Algorithm-Based Network-Based Intrusion Detection System [9] | System traffic classification is experiencing a long-term problem as a result of redundant and unimportant information features. When it comes to adapting to large amounts of data, these characteristics prevent a classifier from making precise choices and impede the order process. | The proposed shared data-based calculation is able to handle both straight and nonlinearly subordinate information features and scientifically select the ideal element for order. System intrusion identification uses it to determine its viability. |
| 5. | Building an interruption identification framework utilizing a Channel based include determination calculation [10]. | These "immense data" ruin the entire acknowledgment process and may provoke unsatisfactory course of action precision in view of the computational difficulties in managing such data. | The common information based estimation can consistently picks the ideal part for gathering and it exhibits that our part affirmation calculation contributes progressively crucial features for LSSVM-IDS to accomplish better exactness and lower computational expense separated and the top level techniques. |
| 6. | A Look Back at the Channel Based Component Determination [11] | The extension of colossal data inside various region presents remarkable hardships to data mining. | It reduces repetition, suppresses noise, and adds weight to the objective plan. It is a phase that precedes preparation and enhances precision, speed, information quality, and comprehension. Additionally, it reduces computational resources and dimensionality. |
| 7. | Utilizing a machine learning algorithm, behavior-based anomaly detection for smart phones[12] | Utilizing unsupervised machine learning techniques known as K-means clustering, it is able to detect malicious activities on a mobile device in real time. | Because they rely on static analysis of application permissions and system calls, the methods used are limited. |
| 8. | a review at applications-based feature selection methods [13]. | A major problem with feature selection strategies is that too many highlights in a dataset — comparable to or more prominent than the quantity of tests — causes model overfitting, which prompts unfortunate outcomes on endorsement datasets. | Highlight choice (FS) techniques can be utilized in information pre-dealing with to accomplish strong information decline. Finding precise information models is made easier by this. |
| 9. | Using the KDD CUP 99 Data Set, an Analyses of Various Data Mining Techniques [14] | Client-to-root (U2R) and remote-to-local (R2L) attacks can't be reliably distinguished by the AI calculations used in the KDD cup informational index. | A ton of estimation was surveyed on KDD dataset and it was used for distinguishing the orders of attacks. |
| 10. | A straightforward method for Intrusion Detection System statistical analysis [15] | Since there are no reduced pursuit spaces, the issue is presently being changed into the sensor framework to build the precision revelation rate. | Intrusion Detection System's vast amount of crude information on actual system traffic is examined to determine whether the traffic is normal or destructive. |
| 11 | Intrusion Detection on Smartphones [16]. | The framework strategies relies upon clients' ongoing organization, different arrangement level is applied and discovery component is on higher alarm openly networks. | In order to increase the precision of the revelation rate, the issue is currently being integrated into the sensor framework. |
| 13 | Application Malware Detection System for Android [17] | According to the findings of the evaluation, it is sensible to use appropriated processing stage and information mining to consistently verify whether or not set applications are being channeled through malware applications from adaptable application markets. | It's possible that not all parts of the phone can be replicated in the cloud, so moving the security accommodation there could be risky. |

**3.0 System Architecture**

The architectural plan of the Proposed system is of 4 (four) levels as shown in figure 3.9. The framework was organized considering four layers that plan with the exercises on the construction beginning from; Information Mix are sensors liable for data absolute and are as such the information wellsprings of IDS. This information is drawn from various sources, for instance, chose data and log records. Information Consistent of Managing in this stage information gets changed or encoded to pass it on to such an express that the machine can in actuality parse making the pivotal features and are dealt with. Assault Certification, here the model gander at data's in the dataset, coming about to isolating the information it goes with choice in the event that it's a typical stream or an obstruction. Result is the result that tells tolerating an obstruction is seen. It takes the data and detachment and the coordinated dataset, and match if the data is pursued or typical, if the data is attack, by a watchfulness will be conveyed off the telephone number and email of the client (showing obstruction day, month, time and year).

**Data Collection Data – Pre - Processing**

Traffic Collection

**Result**

Filter base feature

Selection

Instance transformation & Normalisation

Intrusion activities

**Attack Recognition**

Decision Model

Decision Making

Normal Flow

Fig 3: **The Structure of the Proposed System (App).**

**3.1 Input Design**

This proposes the course of action of the medium through which all of the information that the arrangement needs can be given to the framework, with an unequivocal assertion of their information types. This plan is essentially a "structure plan," and it contains the client enrollment data necessary for the system to complete selected tasks or exercises. The client enrollment structure's data plan is depicted in Figure 3.1.

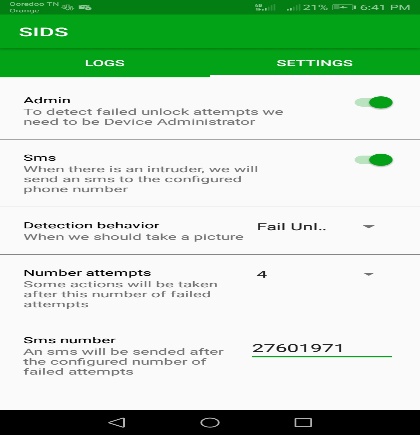
****

Figure 4: Illustration of User Registration

**3.1.1 Output design**

The result arrangement closes how the managed information is to be shown. The plan shows the pre-arranged SMS shipped off the client in sort of a string contains the region of the android telephone. Figure 3.3 representation of the Result Plan of a ready SMS of an endeavor.

**SIDS**

Someone try to unlock your phone AUM-L29!!!

The last detected location:

-Latitude: 35.67035999999999995

-Longitude: 10.110686666666668

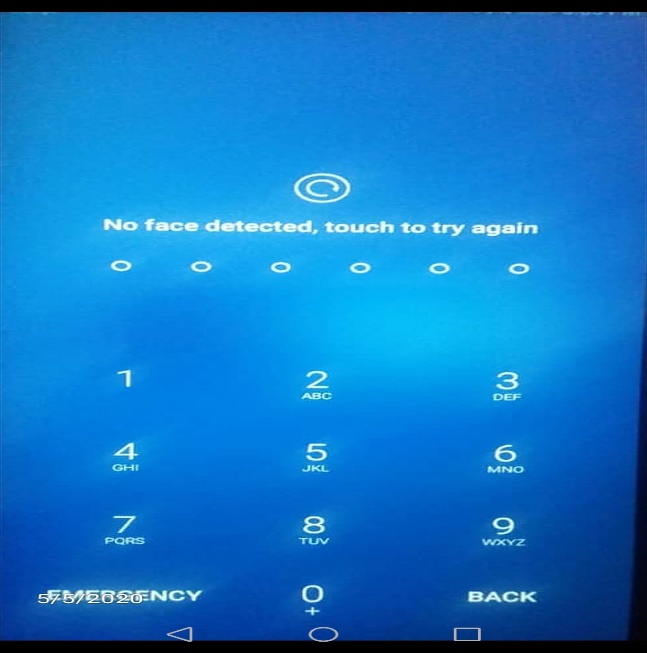
Figure 5: illustration of the Output Design of an alert.

**4.0 Result and documentation**

The proposed system is an android application created utilizing Java. This application gathers information of the clients from the biometric (finger impression and facial acknowledgment) that is utilized the client use in confirmation of his/her telephone, and furthermore information is derived from a variety of sources, such as log and enlisted information chronicles. The application look at data's in the dataset, subsequent to breaking down the information it settles on choice in the event that it's a typical stream or an interruption, and tells assuming an interruption is perceived. After the application has been downloaded and presented, then, at that point, establishment of selfie for gatecrasher and the Director, moreover the client will plan SMS and region prepared, number of tries, SMS number. Expecting an interference is recognized, rapidly the prepared expert sends a SMS and email (that contains a declaration showing an interference and moreover the region of the phone), while a selfie of the intruder will be kept in the application log for the clients view. The issue of fake issue is avoided considering the way that the proposed system critical prepared expert is through SMS and not simply email that requires ICMP (which sends screw up messages to email showing organization isn't available or not reachable). This study supports other previous studies [19, 20, 21] that highlights the need for cybersecurity and user privacy and data security.

****

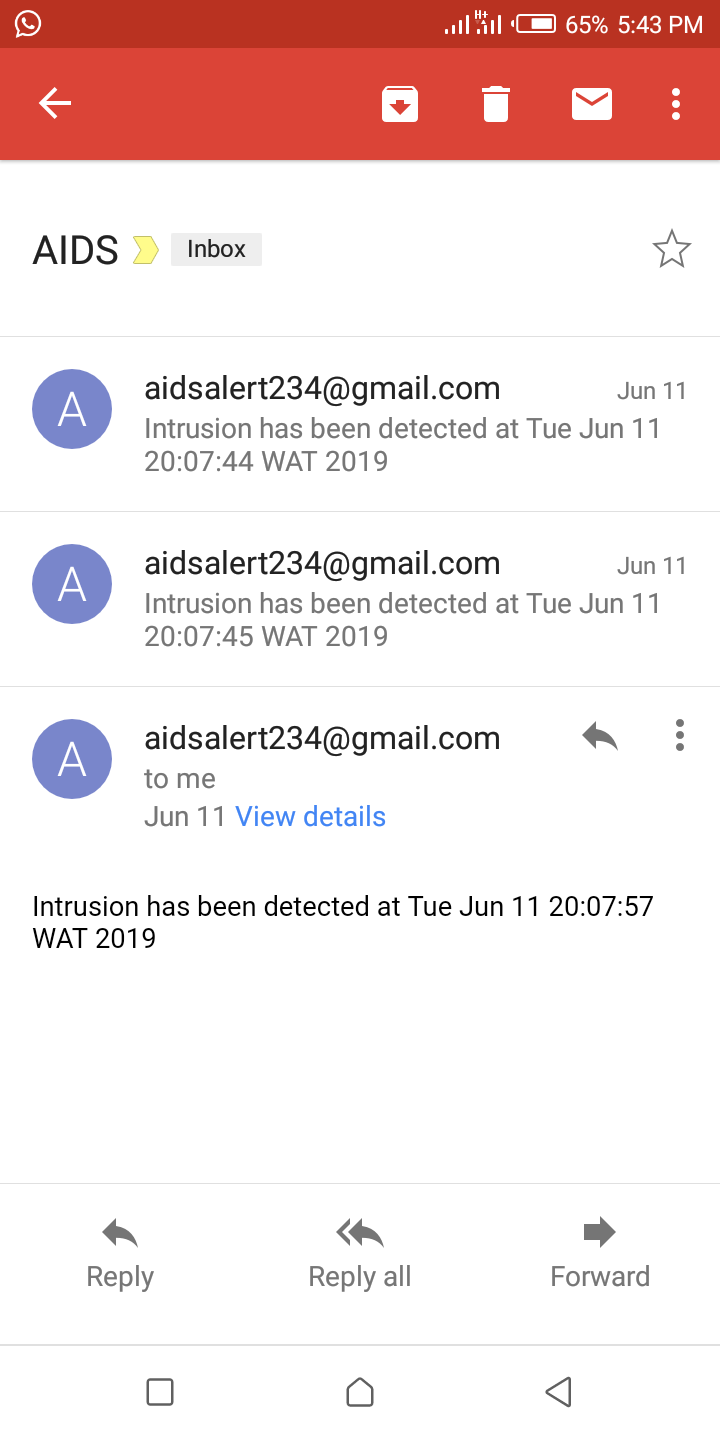
*Figure 6: The screen shot of the* activating biometric

****

*Figure 7: The screen shot of the user Authentication (fingerprint/facial recognition).*

****

*Figure 8: The screen shot Login attempts*



*Figure 9: The screen shot of the email alarm of an interruption*

**5.0 Conclusion**

This framework is acquainted all together with recognize interruptions when other safeguarding efforts crash and burn, by inertly noticing framework occasions and looking for security related issues. This evaluation gives a useful and supportive framework to see horrendous activities (attempt of certification, selfie records of gatecrasher) in the Telephone. We have had the choice to plan and cultivate an application that can perceive impedance on Android Telephone. The proposed structure is a program that continues to run on a working Android system. It also clearly detects harmful presentations, and Android phone users use the application. A few reviews have been done that look at different IDS structures for Android phones.

**Author Contributions:** Conceptualization, ***Taoufik*** E, Onyedeke O. C, ***Obayi A. A*,** Uzo I. U, Olayiwola A. A, *Famuyiwa, K. A*..; Investigation, ***Taoufik*** E, Onyedeke O. C, Uzo I. U,.Olayiwola A. A, *Famuyiwa, K. A*; Project administration, ***Taoufik*** E, ***Obayi A. A*,** Onyedeke O. C; Resources, ***Taoufik*** E; Validation, Onyedeke O. C; Writing—original draft, ***Taoufik*** E, 1, Onyedeke O. C.; Writing—review and editing. All authors have perused and consented to the distributed adaptation of the composition.

**Funding:** This research got no particular award from financing offices in people in general, business, or not-for-benefit areas.

**Acknowledgments:** There is no monetary interest or advantage has emerged from the immediate uses of this research.

**Conflicts of Interest:** The authors proclaim no irreconcilable circumstance. The funders played no part in the plan of the review; in the assortment, examinations, or understanding of information; in the composition of the original copy, or in the choice to distribute the outcomes.

**Availability of Data:** All information are inside the paper. Extra information will be made accessible on demand.

**REFERENCE**

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

[2]. Okoronkwo M.C and Onyedeke O.C, “An Android phone intrusion detection system (IDS) with a filter-based feature selection algorithm” *Int. journal of innovative research and developmenyt.*, vol.8, issue 11, pp. 101, 2019.

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

[4]. AnsamKhraisat, IgbalGondal, Peter Vamplew & Joarder Kamruzzaman. “Study of interruption location frameworks: methods, datasets and challenges”. *Scientific Data*. Vol 20, 2019.

[5]. Khurram Majeed1, DrYanguo Jing2, DrDusica Novakovic3, and Prof Karim Ouazzane4, “Utilizing a machine learning algorithm, behavior-based anomaly detection for smart phones”. International conference on Computer Science and Information Systems (ICSIS’2014) Oct 17-18, 2014 Dubai (UAE).

[6] AdebayoOlawale,Surajudeen, M.A.Mabayoje, Amit Mishra, OshoOluwafemi,“ Malware Discovery, Strong Programming Specialists and Its Grouping Plans”. International Journal of Network Security & Its Applications (IJNSA), Vol.4 no.6,pg 33, 2012

[7] Dr. S. Vijayarani, Ms. Maria Sylviaa.S, “Intrusion Detection System – A Study”.International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 4, No 1, pg 31, 2015.

[8] Yubin Kuang, “A Similar Report on Element Feature Strategies and Their Applications in Causal Surmising”.Department of Computer Science, Faculty of Science, Lund University, pg 1-3, 2009.

[9] Saranya.k1, prabhu.r2, Dr.ramesh kumar.m3,preethi.p4 “Using a filter-based feature selection algorithm, a network-based intrusion detection system”. International Research Journal of Engineering and Technology (IRJET),Volume: 04, no.10,pg 1271, 2017**.**

[10] Mohammed A, Ambusaidi,Xiangjian He, ,Priyadarsi Nanda,Zhiyuan Tan,” Using a filter-based feature selection algorithm, a network-based intrusion detection system”. IEEE transactions on computers, vol 1, no 1pg 1-3, 2014.

[11] K.Mani, P.Kalpama, “A survey on filter based feature choice”. International Journey of Innovation Research in Computer and Communication Engineering, Vol 4, issue 5, pg 9147, 2016.

[12] Jasmina Novakovic, PericaStrbac, Dusan Bulatović, “Toward ideal component determination utilizing positioning techniques and classification Algorithm”. Yagoslav journal of operation Research, pg119 -135, 2011.

[13] A. Jović, K. Brkić, N. Bogunović, " A survey of element choice strategies with applications". Faculty of Electrical Engineering and Computing, University of Zagreb / Department of Electronics, Microelectronics, Computer and Intelligent Systems,pg 3, 2016.

[14] Safaa O, Al- mamory, Firas S. Jassim, “Analyses of Various Data Mining Techniques Using the KDD CUP 99 Data Set”. Journal of Babylon University/Pure and Applied Sciences/ University of Babylon/college of computers and Sciences, Vol 21, No. 8, pg 83, 2013.

[15] A.A. Waskita, H. Suhartantoy, P.D. Persadhazy, L.T. Handoko, “A straightforward factual examination approach for Intrusion Detection Framework”. Center for Development of Nuclear Informatics-National Nuclear Energy Agency,pg 1, 2014.

[16] Muhamed Halilovic, Abdulhamit Subasi, “Intrusion Detection on Smartphones”. International Burch University Faculty of Engineering and Information Technologies, Department of Information Technologies, Sarajevo, Bosnia and Herzegovina. 2017.

[17] Mr. Akash J Wadate, Prof. N. R Chopde, Prof. D. R. Datar, “Malware Identification Framework for Android Versatile Applications“. International Journal of Engineering Research and General Science, Vol 4, Issue 1, pg 21-22, 2016.

[18] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, “RiskRanker : Categories and subject descriptors for zero-day Android malware detection that are scalable and accurate,” *Int. Conf. Mob. Syst. Appl. Serv.*, 2012.

[19] P. Kaushik and A. Jain, “Techniques for Detecting Malware on Android,” *Int. J. Comput. Appl.*, vol. 122, no. 17, pp. 22–26, 2015.

[20] Onyema EM, Kumar MA, Balasubaramanian S, Bharany S, Rehman AU, Eldin ET, Shafiq M. A “Software Defined Network Security Policy Protocol for Internet Control Message Protocol Attack Detection and Prevention”. Sustainability. 2022; 14(19):11950. <https://doi.org/10.3390/su141911950>

[21] Onyema, E.M., Dinar, A.E., Ghouali, S., Merabet, B., Merzougui, R., Feham, M. (2022). Digital Dangers, Assault Procedure, and Moral Hacking in Broadcast communications Frameworks. Blockchain Technologies. Springer, Singapore. pp 25-45

<https://doi.org/10.1007/978-981-19-1960-2_2>