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

***Taoufik Elmissaoui1*, *Obayi Adaora Angela* 2, Uzo Izuchukwu Uchenna3.**

***Onyedeke Obinna Cyril 4,* Olayiwola Abisola Ayomide 5, *Famuyiwa, Kolawole Samuel A*6,**

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)

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

*4Department of Computer Science, University of Nigeria, Nsukka, Nigeria*[*Obinna046@gmail.com*](mailto:Obinna046@gmail.com)*,*

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

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

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

*5Department of polytechnic, Itori.computer science, D.S Adegbenro ICT*

[***famuyiwakola@gmaill.coom***](mailto:famuyiwakola@gmaill.coom)

**Abstract**

An increase in the number and 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 behavior of the application in a run time environment and monitors the application’s dynamic behavior and system 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 the controlling applications. As a result of high predominance, interruption location frameworks (IDS) are given to checkmate interruptions. IDS is a kind of safety programming planned to thusly alert heads when someone or something is endeavoring to deal information structure through malignant activities or through security approach encroachment [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 Internet to check for any of the most recent risks which could achieve attack. There are different IDS like static approaches, 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 toward the finish 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 environment and screens the application's dynamic approach to acting and structure responses.

**2.0 Detection Approach**

Intrusion detection systems are mentioned by the area approach used to perceive meddling exercises [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 effects 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 dim assaults or combinations of known ones [5].

**2.1Table 1: Essential features of a good (anomaly based and signature based) IDS.**

|  |  |  |
| --- | --- | --- |
| 1. | Confidentiality | An effective intrusion detection system ensures that the data is hidden from unapproved parties, procedures, or systems. |
| 2. | Integrity | It ensures that the information is safeguarded in terms of its significance, fulfillment, consistency, planned use, and connection to its representation. |
| 3. | Availability | Guaranteeing that the data and system are open and usable to supported individuals or possibly shapes. |
| 4. | Accountability | Guaranteeing that trades are recorded with the objective that occasions may be imitated and followed to clients or strategies. |

**2.1.1 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.

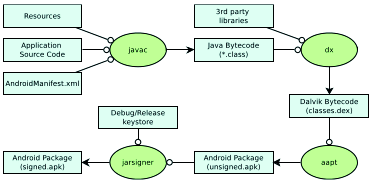
****

Figure 1: Build process of an Android application (Adapted from [9])

**2.1.2 Android Malware**

A malevolent application or malware alludes to an application that can be utilized to think twice about activity of a gadget, take information, sidestep access controls or in any case cause harm on the host terminal [9]. This part presents the Android malware danger and development.

**2.1.3 Malware**

Aggressors need to get to a device by presenting malware on it. The goal is to steal information 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 and move this information to the aggressor is arranged. Spyware can be business and malignant. Business spyware are applications presented on the client's handset genuinely by another person 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. Incidentally, they furthermore assemble information from the system, for instance, the client's area book or his examining history.

**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 sending a few premium-rated SMS messages.

**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 true applications, which are then modified 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, as the application can speculatively kill the root respects from the client. Like most Trojans, the harmful application pretends to be normal until it is installed on the client's device. It tries, when presented, to use no less than one root exploits to obtain root permission to the device. With root access, an application can replace, modify, and introduce applications as it sees fit.

**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 and get directions from at least one Order and Control (C&C) waiter. The developers of malware muddle their code and use encryption to hide fundamental data 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 application's record without executing the application to recognize dangerous models. From the application's source code, many features are isolated, for instance, assents, broadcast recipients, APIs, purposes, data stream, control stream, gear parts, etc. Consent 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 environment and screens the application's dynamic approach to acting and system responses. It executes the questionable application inside a controlled environment habitually called sandbox. Network associations, capability calls, asset utilization, framework calls, and so on 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 situation has been undermined by a malware, an attacker would then have the choice to dispatch their assault through several devices like gathering sniffer, port scanner, weakness 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 in light of the fact that they rely upon static examination of usage approval and system 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 diminishes the readiness and testing time from 113.53 and 2.93 to 44.78 and 2.06, accomplishes the most elevated F-extents of 0.998, has the least fake issue rate, and wipes out unimportant highlights.

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.

An outfit model that is a combination of C4.5, Order, and Relapse Tree (Truck) was proposed in [11] as a useful classifier for attacks' course of action. In the event that there ought to be an event of two-class and multiclass NSL-KDD educational file independently, the proposed outfit model provides elegant accuracy of 99.67 percent and 99.53%, respectively. A hero among the primary efficiencies in the KDD edifying grouping is the monster number of bleak records, which makes the learning assessments be lopsided towards the constant records, and in this way keep them away from learning unprecedented records which are consistently dynamically shocking to systems, for example, U2R and R2L assaults.

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 inadequacy is that binomial or normal (quantifiable streams) can't depict model confirmation direct, which gathers that standard structures of parametric methodologies 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 lot of assessment was assessed on KDD dataset and it was utilized for seeing the classes of assaults. 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.

According to [15], examines how each component of the KDD 99 interruption acknowledgment dataset affects the disclosure of each class. Their unequivocal outcomes uncovered that several elements (hot Login, number of Compromised conditions, number of record creation tasks, visitor login) have no pertinence in obstruction recognizing verification. The most isolating aspects of each class were concluded using an unforgiving set degree of dependence and the degree of dependence of each class.

A clever strategy for handling distinct rough data pertaining to the framework's traffic was proposed in [16]. In order to determine whether the traffic is normal or harmful, the substantial amount of rough data of actual framework traffic from the Interruption Identification Framework is investigated. Since there are no reduced chase spaces, the issue is currently being integrated into the sensor framework to increase the accuracy recognition rate.

According to [17], proposed a common information based estimation that consistently picks the best component for gathering. The evaluation results shows that the element choice estimation contributes continuously fundamental features for least square assist vector with machining based interference revelation system to achieve better accuracy and lower computational cost 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.

Measures that help with representing the level of abundancy of IDS and the continuous work of guideline and homogenization of IDS are introduced in [18]. The framework connects with us to strengthen the analyzer to track down possible new attacks or assortments of attacks. Their impediments, which are crazy, don't ensure 100 percent security, and the arrangement's blemish is the pace of misdirecting potential gains brought about by clients' uncommon or fascinating way of behaving, which isn't precisely awful.

According to [19], proposed a structure to manage the security of the supportive applications which will evaluate the versatile applications security subject to the circumnavigated figuring stage and data mining. The aftereffects of the assessment show that it is reasonable to utilize 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.

[20] suggested a proactive strategy for identifying zero-day Android malware that did not rely on malware tests or their scores to identify potential security risks posed by untrusted applications. Chance Ranker is a computer framework that scales applications to determine whether they exhibit risky behavior. By separating the control stream and information stream from the code way, they conducted static testing on the figured Dalvik bytecode in each application. They assembled 118,318 applications from various Android promotes and dealt with it in four days or less. They identified 3281 risky applications as a result of their investigation.

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

|  |  |  |  |
| --- | --- | --- | --- |
| S/n | **System/Article** | **Weakness** | **Strength** |
| 1. | Malware Detection, Supportive Software Agents and Its Classification Schemes [6]. | At the point when a structure has been sabotaged by a malware, an assailant would then have the option to dispatch their attack through a couple of gadgets like package sniffer, port scanner, defencelessness scanner, secret word wafer among others. | It identified the type of malware, its structure, its activities, and methods for preventing and eliminating malware in the event that it eventually contaminates a system. |
| 2. | Intrusion Detection System – AStudy [7]. | Harmful clients or software engineers use the affiliation's internal structures to assemble  information's and cause weaknesses like Programming bugs, Pass in organization, passing on structures to default plan. | its procedures, strategies and calculations help to identify assaults utilized by programmers for getting important data. |
| 3. | A Comparative Study on Feature Selection Methods  and Their Applications in Causal Inference [8]. | The circulation P(x,y) does not always have a reliable experimental gauge from the information, especially for high-dimensional genomic data. Assessing P(x,y) is unquestionably a more difficult problem than prescient demonstrating. | In the process of building a model, feature selection plays a crucial role in eliminating irrelevant variables and improving model performance by reducing noise and dimensionality. |
| 4. | Network based Intrusion Detection System using Filter based Feature Selection Algorithm [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 intrusion detection system using a  Filter-based feature selection algorithm [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 component assurance computation contributes dynamically fundamental highlights for LSSVM-IDS to achieve better accuracy and lower computational cost differentiated and the top tier procedures. |
| 6. | A Review on Filter Based Feature Selection [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 arrangement. It is a stage that precedes preparation and enhances precision, speed, information quality, and comprehension. Additionally, it reduces computational resources and dimensionality. |
| 7. | Behaviour based anomaly detection for smart phones using machine learning Algorithm[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 of feature selection methods with  Applications [13]. | A major problem with feature selection strategies is that too many features in a dataset—equivalent to or greater than the number of tests—causes model overfitting, which leads to poor results on approval datasets. | Highlight choice (FS) techniques can be used in data pre-taking care of to achieve powerful data decline. Finding precise information models is made easier by this. |
| 9. | Evaluation of Different Data Mining Algorithms  with KDD CUP 99 Data Set [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. | Analysis of KDD ’99 Intrusion Detection Dataset for  Selection of Relevance Features [15]. | A few features—hot login, number of bargained conditions, number of record creation activities, and visitor login—have no bearing on interruption location, according to observations. | It has a high rate of AI calculation identification on them. |
| 11. | A simple statistical analysis approach for Intrusion  Detection System [16]. | Since there are no reduced pursuit spaces, the issue is currently being transformed into the sensor system to increase the exactness discovery rate. | The Intrusion Detection System's vast amount of crude information on actual system traffic is examined to determine whether the traffic is normal or destructive. |
| 12 | Intrusion Detection on Smartphones [17]. | The framework strategies relies upon clients' ongoing organization, different arrangement level is applied and discovery component is on higher alarm openly networks. | The significant restriction is on client experience dangers, cost creating danger and security encroaching dangers isn't tackled. |
| 13 | Creating a Complete Model of an Intrusion Detection System effective on the LAN [18]. | The system enables us to update the analyser to find conceivable new assaults or varieties of assaults. | Their limitations don't guarantee 100 percent security, ludicrous and the injury of this course of action is the pace of bogus up-sides in view of weird or remarkable direct of clients, who are not exactly frightful. |
| 14 | Malware Detection System for Android Mobile Applications [19]. | The evaluation results exhibit that it is sensible to use appropriated processing stage and data mining to affirm all set aside applications regularly to filter through malware applications from flexible application markets. | The moving of the security helpfulness into the cloud could in like manner be risky, while possibly not all bits of the telephone can be imitated into the cloud. |

**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 plan of the medium through which each of the information that the design needs can be given to the framework, with an unequivocal declaration of their information types. This plan is essentially "structure plan" which contains the clients' enlistment information that could be anticipated for the framework to carryout chose activities or assignments. Figure 3.1is the diagram of the data plan of the client enlistment structure.

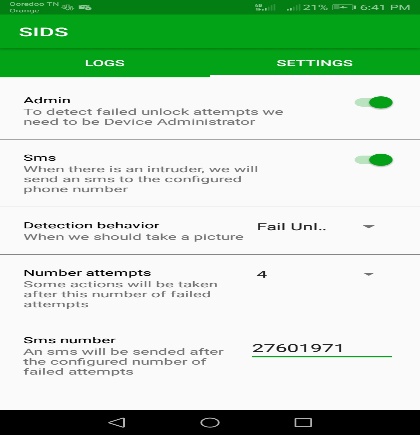
****

Figure 4: Illustration of User Registration

**3.1.1 Output design**

The outcome setup concludes how the dealt with data is to be shown. The arrangement shows the prepared SMS sent off the client in kind 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

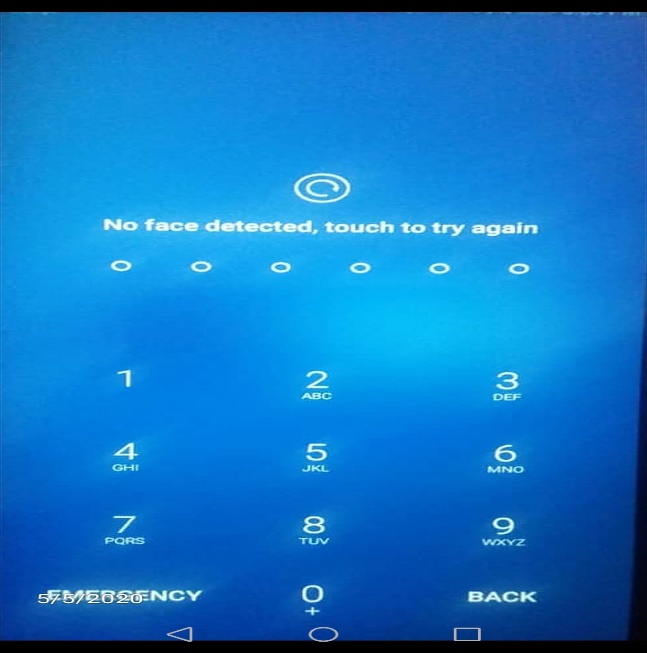
Figure 5: illustration of the Output Design of an alert.

**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 drawn from different sources, for example, enlisted information and log 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 [22, 23, 24] that highlights the need for cybersecurity and user privacy and data security.

****

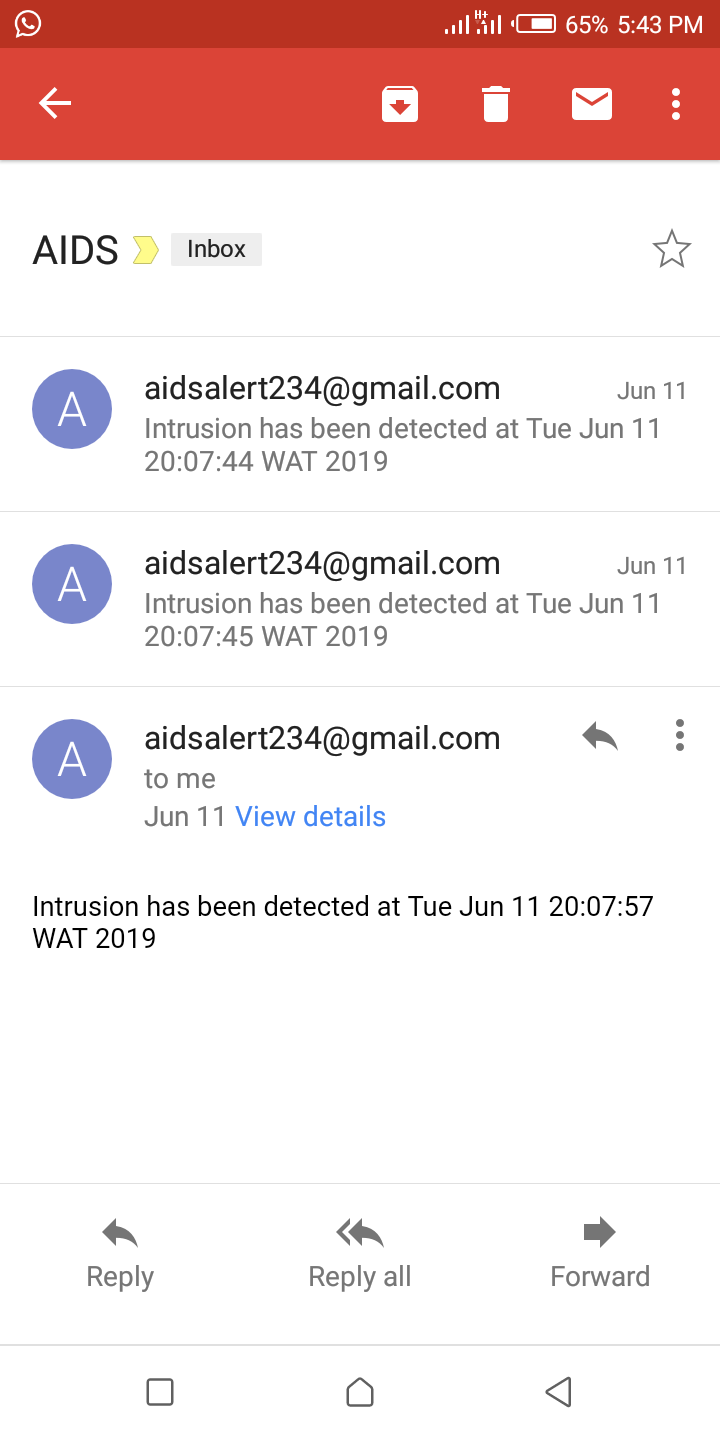
*Figure 6: The screen shot of the* activating biometric

****

*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 alert of an intrusion*

**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 assessment gives a productive and helpful system to perceive destructive exercises (try of affirmation, selfie records of interloper) in the Phone. We have had the decision to design and foster an application that can recognize interference on Android Phone. The proposed structure is an application that keeps on running on an Android working framework. It moreover sees toxic exhibitions unequivocally and the application is utilized by Android phone clients. Several works has been inspected which present various frameworks of IDS on Android phone.

**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 read and agreed to the published version of the manuscript.

**Funding:** This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

**Acknowledgments:** This is to acknowledge that no financial interest or benefit has arisen from the direct applications of this research.

**Conflicts of Interest:** The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

**Availability of Data:** All data are within the paper. Additional data will be made available on request.

**REFERENCE**

[1]. Martin Borek,” Intrusion Detection System for Android: Linux Kernel System calls Analysis”. School Of Information and Communication Technology, *Sweden 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]. 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. “Survey of intrusion detection systems: techniques, datasets and challenges”. *Scientific Data*. Vol 20, 2019.

[5]. 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’2014) Oct 17-18, 2014 Dubai (UAE).

[6] AdebayoOlawale,Surajudeen, M.A.Mabayoje, Amit Mishra, OshoOluwafemi,“Malware Detection, Supportive Software Agents and Its Classification Schemes”. 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 Comparative Study on Feature Selection Methods and Their Applications in Causal Inference”.Department of Computer Science, Faculty of Science, Lund University, pg 1-3, 2009.

[9] Saranya.k1, prabhu.r2, Dr.ramesh kumar.m3,preethi.p4 “Network based Intrusion Detection System using Filter based Feature Selection Algorithm”.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,” Building an intrusion detection system using a filter-based feature selection algorithm”. IEEE transactions on computers, vol 1, no 1pg 1-3, 2014.

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

[12] JasminaNovakovic,PericaStrbac, DusanBulatović, ”Toward optimal feature selection using ranking methods and classification Algorithm”. Yagoslav journal of operation Research,pg119 -135, 2011.

[13] A. Jović, K. Brkić, N. Bogunović, "A review of feature selection methods withapplications". 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, “Evaluation of Different Data Mining Algorithms with 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] AdetunmbiA.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, pg 2663-2664, 2010.

[16] A.A. Waskita, H. Suhartantoy, P.D. Persadhazy, L.T. Handoko, “A simple statistical analysis approach for IntrusionDetection System”. Center for Development of Nuclear Informatics-National Nuclear Energy Agency,pg 1, 2014.

[17] MuhamedHalilovic, AbdulhamitSubasi,” Intrusion Detection on Smartphones”. International Burch University Faculty of Engineering and Information Technologies, Department of Information Technologies, Sarajevo, Bosnia and Herzegovina. 2017.

[18] 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, pg 1-2, 2012.

[19] 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, pg 21-22, 2016.

[20] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, “RiskRanker : Scalable and Accurate Zero-day Android Malware Detection Categories and Subject Descriptors,” *Int. Conf. Mob. Syst. Appl. Serv.*, 2012.

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

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

[23] Onyema, E.M., Dinar, A.E., Ghouali, S., Merabet, B., Merzougui, R., Feham, M. (2022). Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunications Systems. In: Kaiwartya, O., Kaushik, K., Gupta, S.K., Mishra, A., Kumar, M. (eds) Security and Privacy in Cyberspace. Blockchain Technologies. Springer, Singapore. pp 25-45

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

[24] Onyema, E.M., Dalal, S., Romero, C.A.T. *et al.* Design of Intrusion Detection System based on Cyborg intelligence for security of Cloud Network Traffic of Smart Cities.  Springer *J. Cloud Comp* **11,**26 (2022). https://doi.org/10.1186/s13677-022-00305-6