International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 5, Issue 3, 202-210, 2024
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V5I3P120

Original Article

Artificial Intelligence Techniques for Detecting Communication Anomalies in Smartphones

Harsha Vardhan Reddy Kavuluri[1], Akhil Kumar Pathani[2], Ajay Dasari[3], Venkata Kishore Chilakapati[4], Srikanth Reddy Keshireddy[5], Venkata Teja Nagumotu[6]
[1]Lead database administrator, Wissen infotech Inc.
[2]Network Engineer, Ebay.
[3]Senior Support Engineer, Microsoft.
[4]Support Escalation Engineer, Microsoft.
[5]Senior Software Engineer, Keen Info Tek Inc.
[6]Sr Network Engineer, Techno-bytes Inc.

Abstract *- Nowadays, everybody desires to possess their personal mobile device, and this has led to an increase in the number of Android users worldwide. Every device connected to the internet communicates with a multitude of applications and thus ends up having many malware attacks or threats in a mobile home. This paper takes a comparative design of predictive models based on smartphone detecting communication anomalies through AndroVul. In this paper, a framework is proposed to be developed to detect cases of communication abnormality using the AndroVul data set with the help of an Artificial Neural Network (ANN). The methodology consists of the preprocessing, feature selection and model training to do a good differentiation of the benign and malicious communication behavior. The evaluation conducted on the experiment indicates that ANN performs with 99.33% accuracy (ACC) , 99.71% precision (PRE), 99.65% recall (REC) and an F1-score (F1) of 99 which is superior to the classical models: MLP (84.31%), Random Forest (93.6%), PCA-based classifiers (89.3%), and SVM (98.2%). Such results indicate the efficiency of AI-based solutions to increase the security of communication in smartphones, and can be applied on a large scale to identify potential abnormalities of communication in the mobile environment. In general, the most important contribution is the introduction of a strong AI-based framework that improves the security of mobile communication by providing reliable, scalable, and high-performance anomaly detection.*

Keywords *- Smartphone, Android Security, Machine Learning, Mobile Security, Mobile Computing, Deep Learning.*

1. Introduction

The increasing number of mobile Internet of Things (IoT) devices has revolutionized the digital landscape in numerous sectors, including smart cities, industrial systems, and healthcare infrastructure. These devices include anything from smartphones and tablets to smart TVs and wearable systems. From banking to education to gaming, and many more besides, the widespread use of mobile applications has simplified, accelerated, or otherwise improved a great deal of previously laborious tasks. The official store for Android apps contains a significant number of free apps, which helps explain Android's dominance in the mobile OS space [1]. Many of these devices run on the Android operating system, which is popular due to its open-source nature and extensive customization options. Nonetheless, there is also a significant growth in the amount and sensitivity of communication data that is being generated, transmitted and stored all due to the rapid expansion of mobile devices. This encompasses network communication, messaging communication patterns, application-to-server communication, and background service communication. Consequently, smartphones have been the best targets of numerous security threats, particularly those attacks that exploit or manipulate these communication devices. The current mobile applications are open and programmable [2], and as such have become very susceptible to communication-based malicious activities like Trojan horses, worms, spyware, and mobile botnets [3][4].

Although built-in mobile security measures, such as access control, authentication and permission management measures, exist, they are in most cases not adequate enough to identify unknown or emerging communication anomalies in real time [5]. Moreover, mobile devices have very low computational capabilities in comparison with traditional computing systems and effective yet lightweight detection methods are needed. As machine learning (ML) is still in its infancy, the research of anomaly detection, particularly, in the case of smartphone communication behavior, is a more important and more complex area that demands an in-depth understanding of both detection methods and the issue thereof [6][7]. AI techniques, in this instance, are relevant in identifying the abnormal patterns of communication and enhancing ACC efficiency and flexibility in detecting anomalies. DL models can learn more complicated communication patterns, detect minor anomalies, and run large amounts of communication logs much faster than traditional ML models, which is why they are particularly suited to the protection of modern smartphone ecosystems.

2. Motivation and Contribution

Smartphone usage has risen at an alarming rate, and communication anomalies have caused numerous security vulnerabilities, including malware-infected calls and data breaches, which are grave threats to the privacy and integrity of the device. Conventional security systems are not usually adequate to identify such advanced and dynamic threats as they happen. This drives the desire to use smart object-driven solutions that can effectively detect dysfunctional communication patterns. The use of high-level ML, especially ANN, is a potential solution to improving the security of smartphones by autonomously and efficiently detecting anomalies. The purpose of this study is to come up with an effective model that is proactive in protecting users from malicious communication practices. The current study contributes to the literature of Detecting Anomalies in Smartphones in a number of ways:

- Utilized the AndroVul dataset, comprising 18,780 Android apps, to ensure a realistic and diverse data foundation.
- Standardization, handling of missing values, and removal of outliers are all part of the extensive data pre-treatment methods that were included.
- Enhanced model performance by concentrating on most relevant features through the application of Chi-Squared feature selection.
- Presented powerful graphics to visualize malware distribution and types of apps to aid in data interpretation.
- A very precise model of ANN to identify communication abnormalities in smartphones.
- Evaluated the performance of the model through a variety of evaluation measures, including ACC, PRE, REC, and F1, to have a comprehensive and confident analysis of the model.

2.1. Justification and Novelty

This research is justified by the rising complexity of smartphone-based attacks and the weakness of the current detection systems in detecting subtle communication abnormalities. Although it is not the first study to discuss different ML models, this study presents a new method to the existing research by combining the advanced pre-processing methods, i.e. Chi-Squared feature selection and data normalization, with a very accurate ANN model based on the full AndroVul dataset. This study is novel as it has excellent performance and is capable of differentiating benign and malicious communications successfully. This study is a notable addition to the field of intelligent mobile security because it combines strong predictive modelling with robust feature engineering.

2.2. Paper structure

The Structure of the paper is as follows: Section II delves into the topic of mobile device communication anomalies. Detailed in Section III are the approach's architecture and design. Section IV presents the results and comparisons, while Section V discusses the last remarks and further investigation.

3. Literature Review

This study has been informed and strengthened by a comprehensive examination and analysis of relevant research on smartphone communication anomaly detection. Prakash, Sankaran and Jithish (2019) offer a fresh method for identifying smartphone malware threats by combining aspects of statistics and information theory. In order to identify unusual patterns of smartphone use, they use the Kullback-Leibler divergence measure to parameterize CPU consumption, RAM utilization, and network data. The suggested approach has a dual benefit. When compared to ML techniques, it has fewer computational requirements, allowing it to function well on devices with limited capacity. Second, the model may be used to detect malicious behavior on a wide variety of smartphone usage patterns, making the suggested approach generic. The suggested method detects malicious activities in Android cellphones with an ACC of 86.24%, according to the evaluation [8].

Talab *et al.* (2019) explore an approach to cardiac abnormality diagnosis that is both reliable and inexpensive, utilizing mobile phones that are presently usually accessible to the ordinary user. Using data from a digital stethoscope or a recorded heartbeat from the phone's microphone, an app is created to identify irregularities in the heart's electrical activity. First, use wavelet transforms to denoise the signal. Then, classify the recorded heart sounds using ML techniques, namely CNNs. This is how the raw heart sound data is processed. The neural network is trained using a database that contains recorded human heart sounds along with their accompanying diagnoses. Adam and other neural network fine-tuning methods to make predictions more easily, regularization is applied. On the validation set, the suggested method achieved a performance level of 94.2% when tested on 5- to 8-second heart sound data [9].

Zulkefli *et al.* (2017) analyze the strategies that can be employed by the assailant to carry out an effective social engineering assault. The authors then used the prior discussion to inform their use of a ML algorithm that can identify phishing attempts. Last but not least, the authors have demonstrated over 90% ACC in their ML evaluations of the proposed method. This demonstrates that the suggested technique could assist in reducing APT attacks by spear phishing in smartphones [10]. Mirsky *et al.* (2017) utilize pcStream, a method well-suited for identifying clusters in real-world data streams, and propose enhancements to the PCstream algorithm to capture point, contextual, and collective anomalies. Evaluation is the most detailed one and covers the problem of mobile security through the lenses of a distinct set of volunteers, who participated in the study

during eight months. Research has shown that PCStream extensions may effectively detect malicious program context abnormalities and data leaks (point anomalies). And with just one false positive every two days, the system can detect a group anomaly the existence of an unauthorized user—in just 30 seconds [11].

Da Costa *et al.* (2017) provide a system for detecting mobile botnets that relies on anomalies and hosts. The proposed approach uses statistical data retrieved from system calls in conjunction with ML methods to identify unusual behavior. It could put the method through its paces in a realistic setting using a dataset that it had created itself, which included thirteen families of mobile botnets and two sets of legal apps. The suggested method achieved several noteworthy results, including low false positive rates and high true detection rates [12].

Huang *et al.* (2016) suggest a method that detects irregular sleep nights without supervised learning by analyzing patterns and identifying changes in context. The outcomes of the experiments validate the effectiveness of the suggested strategy in identifying nights with disrupted sleep patterns. Research is the first of its kind to employ unrestricted smartphone sensing to identify shifts in sleep patterns, a feat that has the dual advantages of requiring less training and being more resilient to behavioral variability [13].

Most of the existing studies, though they do investigate a variety of anomaly detection methods of smartphones, appear to concentrate on small sets of features, particular types of attacks, or a small set of applications. Most of the approaches used are small or artificial data, do not have real-time flexibility, or are not capable of capturing the complexity of changing patterns of communication behavior on smartphones today. Moreover, some of the approaches are computationally intensive and cannot be deployed to devices, and some cannot be generalized to different users and changing network conditions. Thus, although the improvement in Table I has been evident, it is still possible to conclude that there is a significant gap in the research to come up with a robust, scalable, and AI-based model that can accurately identify the communication anomalies based on rich and real-world data and retain high ACC, efficiency, and generalizability.

Table 1: Overview of Recent Studies on Predictive Modelling of Detecting Communication Anomalies in Smartphones

Author	Proposed Work	Dataset	Key Findings	Challenges/recommendations
Prakash, Sankaran & Jithish (2019)	Malware detection using statistical & information-theoretic approaches	Smartphone usage data (CPU, RAM, network)	86.24% accuracy; efficient on low-power devices	Less accurate than ML models, but efficient
Talab et al. (2019)	CNN-based heart anomaly detection via smartphone microphones	Heart sound recordings dataset	94.2% accuracy using CNN and ADAM Regularization	Accuracy relies on clean input signals
Zulkefli et al. (2017)	Machine learning classifier to detect phishing URLs for smartphone protection.	URL dataset labeled as phishing or legitimate.	Achieved >90% accuracy for phishing detection.	Limited to URL-based attacks; recommend multi-feature models including behavior-based analysis.
Mirsky et al. (2017)	Extensions of pcStream algorithm for detecting point, contextual, and collective anomalies in smartphone data streams.	Dataset from 30 volunteers over 8 months.	Detected data leakage, malicious behavior, and unauthorized device use within 30 seconds with very low false positives.	High computational demand; recommend optimization for real-time on-device processing.
Da Costa et al. (2017)	Host-based mobile botnet detection using ML on system call features.	Self-generated dataset with 13 botnet families + benign apps.	High detection rate with low false positives in realistic scenarios.	Dataset limited to synthetic scenarios; recommend testing on real-world botnet samples.
Huang et al. (2016)	Unsupervised model for detecting irregular sleep patterns using smartphone sensing data.	Smartphone sensor data (accelerometer, microphone, etc.).	Effective detection of irregular sleep nights without supervised training.	Performance varies with user behavior diversity; recommend adaptive learning mechanisms.

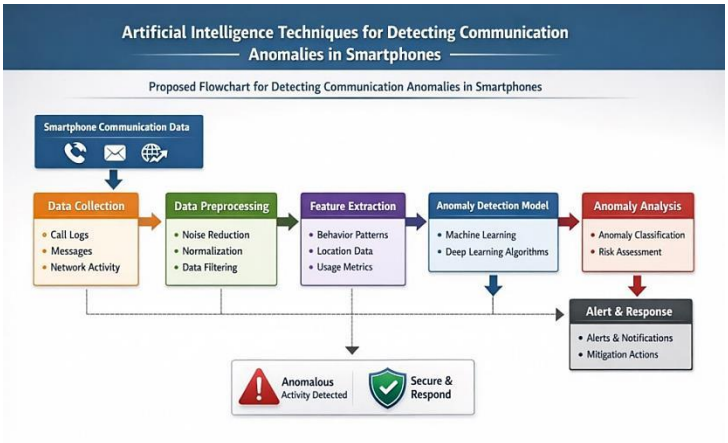

Fig 1: Proposed Flowchart for Detecting Communication Anomalies in Smartphones

4. Research Methodology

The proposed methodology for detecting communication anomalies in smartphones using the AndroVul dataset involves a structured pipeline shown in Figure 1. consisting of data collection, pre-processing, and model. This data collection After cleaning the data by dealing with missing values and outliers, the data was normalized using Standard Scaler to standardize feature distributions as part of the pre-processing. In order to keep the most important features for classification, the Chi-squared test was used for feature selection. The next step was to split the dataset in half, making one half for testing and the other for training. Using this processed data, the ANN model was trained to classify communication activities. The model's performance was evaluated using standard measures like ACC, PRE, REC, and F1 to ensure reliable prediction and efficient anomaly detection classification.

A full description of each step in the suggested flowchart for finding strange phone calls is given below.

4.1. Data collection

The AndroVul dataset, culled from the AndroZoo repository, has 18,780 Android apps. It is utilized in this experiment. Metadata that provides the number of antivirus engines from the VirusTotal website which compiles a large range of antivirus programs and web-based virus scanners is proposed by the Androzoo project to be included with applications' APKs. that detected malware in the program. Data distribution in three categories is shown in Figure 2:

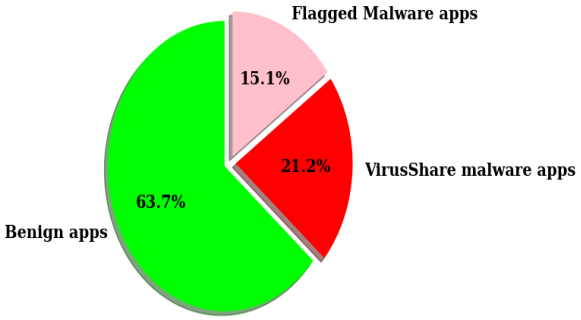

Fig 2: Pie chart for Dataset distribution

Figure 2 illustrates the distribution of app categories within the dataset. A majority, 63.7%, are classified as benign apps, indicating that they exhibit no signs of malicious behaviour. 21.2% of the dataset consists of VirusShare malware apps, which are confirmed malicious samples obtained from a trusted malware repository. The remaining 15.1% are flagged malware apps, identified as potentially malicious based on antivirus flagging, but not yet confirmed. This dissection shows that there are more benign uses, and a large part of it is isolated into confirmed and suspected malware, which are more appropriate to strike the balance in the study of malware classification.

4.2. Data Pre-Processing

The data preparation was done by collecting the AndroVul dataset, cleaning and extraction of features of interest. Pre-processing involved processing of missing values, outliers and data transformation and normalisation. The pre-processing steps are vital and the major steps are as follows:

- Remove missing value: Removing missing values, also known as handling missing data, involves strategies to address incomplete data within a dataset. The adopted methodology varies according to the type and minor extent of missingness, and the objectives of analysis.
- Remove Outliers: ACC and reliability of data analysis and ML models can be advanced by removing the outliers, which are distinctly separate data points as compared to others.

4.3. Feature Selection using Chi-Squared

Feature selection refers to the process of extracting useful characteristics from a dataset's initial collection of features in order to improve model performance and interpretability. It is an extremely important step in ML and data mining, which can assist in creating more efficient and accurate models that decrease the number of dimensions, remove noise, and target the most informative variables. Chi-squared is a statistical test that is applicable in the selection of features, especially where the data is categorical. It finds the features with the highest correlation to the target variable and checks if they are independent of the target variable.

4.4. Data Normalization using StandardScaler

To standardize the data, the StandardScaler() technique was applied to standardize the data to make the mean of the resulting distribution equal to zero and the standard deviation equal to one. It is implemented through deriving the mean value of each observation and dividing it by the standard deviation as expressed in Equation (1) below:

$$z = \frac{x-\mu}{\sigma} \qquad (1)$$

z stands for the feature's converted value, x for the original values of the descriptors, μ for the feature's mean, and ϖ for its standard deviation in the data.

4.5. Data Splitting

Data splitting refers to the process of splitting a dataset into separate subsets, usually used to train, validate, and test ML models. The whole dataset was partitioned into training and testing sets so that the model's efficiency could be evaluated. To be more specific, testing and performance evaluation received 20% of the data, whereas 80% went toward model construction and parameter estimate.

4.6. Proposed Artificial Neural Networks (ANN) Model

An ANN model is a kind of computational network that attempts to discover intricate relationships and patterns in data by mimicking the way the human brain works. Between the input and output layers, there may be one or more hidden layers in this network of interconnected nodes (neurons) [14]. To enable the network to learn from data using training algorithms such as back propagation, the neurons process the incoming data using activation functions and weighted connections. One well-liked model is the ANN, which mimics the way the human brain stores and retrieves information through synapses, as well as how it performs generalized computations and tasks like pattern recognition and classification. It is possible to express the neuron k output (y) using Equation 2.

$$y_k = \varphi(u_k + b_k) \text{And } u_k = \sum_{j=0}^{m} w_{kj} x_j \qquad (2)$$

in which bk is the bias that affects the input of the activation function φ and w_{kj}Is the synaptic weight from input x_jTo k. A multilayer perceptron's strength lies in its hidden neurons, which are highly connected to one another through synapses. This allows the network to recognize patterns, which is essential for solving difficult issues. Iterative algorithms can train biases and weights using an error function described in Equation (3) for the n-th iteration on neuron i.

$$e_i = d_i(n) - y_i(n) \qquad (3)$$

The neuron's output is denoted by y, while the desired output is represented by d. Equation (4) shows how to refine this error function into an error energy function for an O-sized output layer:

$$E_{avg} = \frac{1}{N}\sum_{n=1}^{N} E(n) \text{where } E(n) = \frac{1}{2}\sum_{i=1}^{o} e_i^2(n) \qquad \square\square\square$$

The data set size is denoted by N. The goal of optimization is to minimize the error energy function as much as feasible as it propagates backward through the network, layer by layer.

4.7. Evaluation Metrics

A variety of performance indicators were used to evaluate the suggested design. TP, FP, TN, and FN were calculated by comparing the actual values with the predicted values of the trained models. Below, describe the calculation and analysis of ACC, PRE, REC, and F1 using these data:

- Accuracy: The percentage of correct predictions generated by the trained model as a whole compared to all of the input samples in the dataset. It is given as Equation (5)-

$$Accuracy = \frac{TP+TN}{TP+Fp+TN+FN} \quad (5)$$

- Precision: Precision is the ratio of those instances that the model successfully predicted to the instances that were predicted as positive. Precision is expressed as Equation (6)

$$Precision = \frac{TP}{TP+FP} \quad (6)$$

- Recall: This metric is the ratio of the number of positive events that were actually expected to occur to the number of positive events that should have occurred. It has a mathematical expression in Equation (7).-

$$Recall = \frac{TP}{TP+FN} \quad (7)$$

- F1 score: It is the harmonic mean of ACC and REC, which means it helps keep ACC and memory in balance. It might be anything from zero to one. The mathematical expression for it is Equation (8)-

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (8)$$

The model's performance and comparison analysis are shown in this assessment matrix.

5. Results and Discussion

This section details the experimental process and evaluates the suggested model's performance throughout the training and testing phases. A Windows 10 (64-bit) PC with an Intel(R) Core(TM) i7-2600 CPU running at 3.40 GHz and 16 GB of RAM is used for the experiments. Table II shows the results of training the proposed model on the AndroVul dataset and then evaluating it using the KPIs of REC, ACC, PRE, and F1. A remarkable ACC of 99.33 was achieved by the suggested ANN model, indicating that the model produced very accurate predictions. Additionally, it has a REC score of 99.65 and a PRE of 99.71, both of which show that it can accurately identify true abnormalities and that it can misread false positives. Furthermore, the F1 of 99 demonstrates a superb equilibrium between memory and PRE. All of these results demonstrate how powerful and efficient the ANN model is for spotting communication outliers in smartphone data.

Table 2: Experiment Results of Proposed Model for Detecting Anomalies

Performance matrix	Artificial Neural Network (ANN) model
Accuracy	99.33
Precision	99.71
Recall	99.65
F1-score	99

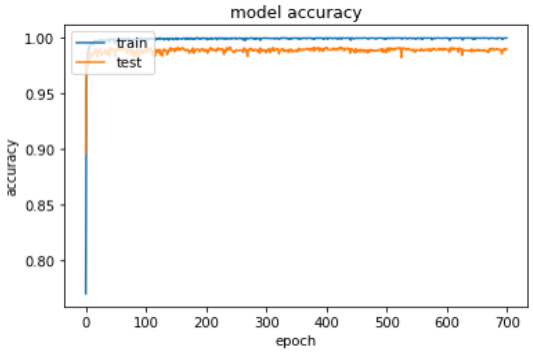

Fig 3: Plot Accuracy Curves for the ANN Model

The model ACC is shown in Figure 3, both during training and testing in the proposed model across training epochs. The ACC of the training (blue line) is increasing steadily and it reaches almost 100 percent, which is high learning of the model. The testing ACC (orange line) also increases at a high rate and reaches a steady point of around 98% and this performance is consistent throughout the training process. The near correspondence between the ACC of training and testing implies that the model is well generalized and there is a low rate of overfitting. On the whole, the chart shows that the model is robust and reliable in revealing time-related communication anomalies.

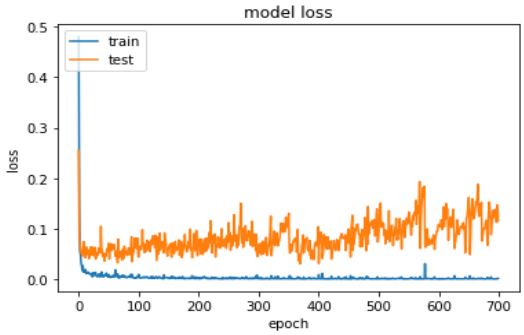

Fig 4: Plot Loss curves for the ANN Model

Figure 4 shows the model loss broken down by training period for both the testing and training phases. The training loss (blue line) reduces drastically and levels off towards zero which is an indication that the model is well-trained by the training data with minimal error. But it can be observed that testing loss (orange line) has more changes and it is slowly decreasing with time, which is possibly an indication of overfitting wherein the model is good at predicting the training data, but less reliable with the unseen data. Despite these variations, the overall test loss remains relatively low, demonstrating that the model still maintains reasonable generalization while detecting communication anomalies.

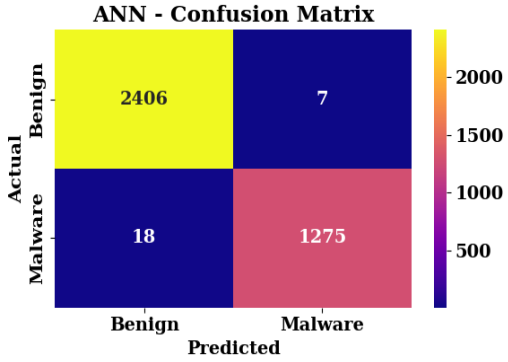

Fig 5: Plot Confusion Matrix For ANN

Figure 5 displays the ANN model's confusion matrix, which demonstrates the model's strong classification capabilities when it comes to distinguishing between legitimate and malicious instances. The model also identifies malware and benign samples with 1275 TP and 2406 TN respectively. The small number of FP (7) and FN (18) implies that it is a highly precise and effective in recalling the information, implying that the ANN can be trusted to detect anomalies in the domain of cybersecurity. Such equilibrium of sensitivity and specificity demonstrates the strength of the model in site reliability engineering in reality.

5.1. Comparative Analysis

Table 3 indicates that there is a performance hierarchy between the various models that were tested in terms of anomaly detection. Classical machine-learning classifiers like the Multilayer Perceptron (84.31%), the Random Forest (93.6%), and the Principal Component Machine with PCA features (89.3%) show fairly good results though they are still unable to capture more non-linear associations inside complex smartphone communication patterns. The Support Vector Machine (98.2) proves to be more accurate because of its great generalization in high-dimensional feature space. However, the provided ANN model demonstrates the highest ACC of 99.33, implying that it is more likely to be able to learn complex behavior patterns and sensitive anomaly patterns. This significant improvement indicates the robust character of the model, the reflection of features, and the capability to apply in the real-time detection of anomalies in communication systems based on smartphones.

Table 3: Accuracy Comparison Of Different Models For Detecting Anomalies

Models	Accuracy
Multilayer Perceptron [15]	84.31
Random Forest[16]	93.6
Support Vector Machine[17]	98.2
Principal Component Analysis[18]	89.3
Propose ANN	99.33

The suggested model of ANN has considerable benefits in identifying anomalies in communication in smartphones. The fact that it can learn the complex and non-linear patterns in the data allows it to have high ACC as shown by its excellent

performance in comparison to the other models. With an high ACC the ANN model demonstrates exceptional PRE in distinguishing normal and abnormal communication behaviours. Additionally, its adaptability and robust learning capabilities make it highly effective in handling large and diverse datasets like AndroVul, resulting in reliable and consistent anomaly detection. This makes the ANN model a powerful and efficient solution for real-time smartphone communication monitoring.

6. Conclusion and Future Study

The real-time movement behavior of people at a certain time is an important sign for sudden events. Since the distribution of mobile phones is almost the same as that of the population, the mobile network might function as a sensor network to track user locations and the distribution of the population at large without incurring any additional costs. The paper is effective in proving the usefulness of the Artificial Intelligence methods, specifically an ANN to identify communication anomalies in smartphones based on the dataset AndroVul. The systematic preprocessing, feature selection and the strict model training that are in favor of the proposed methodology result in a high ACC in the detection of abnormal communication behaviors. The validation of the ANN can be confirmed by the experiments with a high ACC of 99.33 and high PRE, REC, and F1. Such results indicate that the model has high competence to distinguish benign and malicious patterns of communication accurately and with low rate of misclassification. An additional comparative study also supports the idea that ANN performs better than the traditional machine-learning models, including Multilayer Perceptron, Random Forest, PCA-based classifiers, and Support Vector Machine, as it is better able to learn diverse and subtle forms of communication. The model demonstrates high outcomes, yet there could be a limitation in generalization based on the limitations of the dataset and some overfitting. More varied communication data should be employed in future work, more sophisticated temporal models put to use, and more lightweight understandable AI solutions constructed in real time smartphone anomaly detection.

References

[1] P. Pathak, A. Shrivastava, and S. Gupta, “A survey on various security issues in delay tolerant networks,” *J Adv Shell Progr.*, vol. 2, no. 2, pp. 12–18, 2015.

[2] M. Louk, H. Lim, and H. Lee, “An Analysis of Security System for Intrusion in Smartphone Environment,” *Sci. World J.*, 2014, doi: 10.1155/2014/983901.

[3] B. Amro, “Malware Detection Techniques for Mobile Devices,” *Int. J. Mob. Netw. Commun. Telemat.*, vol. 7, no. 4/5/6, pp. 01–10, Dec. 2017, doi: 10.5121/ijmnct . 2017.7601.

[4] S. Achouche, U. B. Yalamanchi, and N. Raveendran, “Method, apparatus, and computer-readable medium for performing a data exchange on a data exchange framework,” 2019

[5] R. A. Ariyaluran Habeeb, F. Nasaruddin, A. Gani, I. A. Targio Hashem, E. Ahmed, and M. Imran, “Real-time big data processing for anomaly detection: A Survey,” *Int. J. Inf. Manage.*, vol. 45, pp. 289–307, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.08.006.

[6] Y. Bhomia, S. Sahu, and S. Sing, “Machine learning for anomaly detection approaches, challenges, and applications,” *Pharma Innov.*, vol. 8, no. 3S, pp. 24–27, Jan. 2019, doi: 10.22271/tpi.2019.v8.i3Sa.25252.

[7] V. M. L. G. Nerella, “Automated cross-platform database migration and high availability implementation,” *Turkish J. Comput. Math. Educ.*, vol. 9, no. 2, pp. 823–835, 2018.

[8] J. Prakash, S. Sankaran, and J. Jithish, “Attack detection based on statistical analysis of smartphone resource utilization,” in *2019 IEEE 16th India Council International Conference, INDICON 2019 - Symposium Proceedings*, 2019. doi: 10.1109/INDICON47234.2019.9030310.

[9] E. Talab, O. Mohamed, L. Begum, F. Aloul, and A. Sagahyroon, “Detecting heart anomalies using mobile phones and machine learning,” in *Proceedings - 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering, BIBE 2019*, 2019. doi: 10.1109/BIBE.2019.00083.

[10] Z. Zulkefli, M. M. Singh, A. R. Mohd Shariff, and A. Samsudin, “Typosquat Cyber Crime Attack Detection via Smartphone,” in *Procedia Computer Science*, 2017. doi: 10.1016/j.procs.2017.12.203.

[11] Y. Mirsky, A. Shabtai, B. Shapira, Y. Elovici, and L. Rokach, “Anomaly detection for smartphone data streams,” *Pervasive Mob. Comput.*, vol. 35, pp. 83–107, Feb. 2017, doi: 10.1016/j.pmcj.2016.07.006.

[12] V. G. T. Da Costa, S. Barbon, R. S. Miani, J. J. P. C. Rodrigues, and B. B. Zarpelao, “Detecting mobile botnets through machine learning and system calls analysis,” in *IEEE International Conference on Communications*, 2017. doi: 10.1109/ICC.2017.7997390.

[13] K. Huang, X. Ding, J. Xu, G. Chen, and W. Ding, “Monitoring sleep and detecting irregular nights through unconstrained smartphone sensing,” in *Proceedings - 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing*, 2016. doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.30.

[14] S. Garg, “AI/ML Driven Proactive Performance Monitoring, Resource Allocation and Effective Cost Management in SaaS Operations,” *Int. J. Core Eng. Manag.*, vol. 6, no. 6, pp. 263–273, 2019.

[15] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “Flow anomaly-based intrusion detection system for Android mobile devices,” in *2017 6th International Conference on Modern Circuits and Systems Technologies, MOCAST 2017*, 2017. doi: 10.1109/MOCAST.2017.7937625.

[16] T. Salman, D. Bhamare, A. Erbad, R. Jain, and M. Samaka, “Machine Learning for Anomaly Detection and Categorization in Multi-Cloud Environments,” in *2017 IEEE 4th International Conference on Cyber Security and Cloud*

Computing (CSCloud), IEEE, Jun. 2017, pp. 97–103. doi: 10.1109/CSCloud . 2017.15.

[17] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, Sep. 2019, doi: 10.1016/j.iot.2019.100059.

[18] L. Wen and H. Yu, "An Android malware detection system based on machine learning," in *AIP Conference Proceedings*, 2017. doi: 10.1063/1.4992953.

[19] Mamidala, J. V., Enokkaren, S. J., Attipalli, A., Bitkuri, V., Kendyala, R., & Kurma, J. (2023). Machine Learning Models Powered by Big Data for Health Insurance Expense Forecasting. *International Research Journal of Economics and Management Studies IRJEMS*, *2*(1).

[20] Nadella, V. M. (2023). Zero Trust Architecture for Telecom Operations. *International Journal of Emerging Research in Engineering and Technology*, *4*(3), 115-129.

[21] Bitkuri, V., Kendyala, R., Kurma, J., Enokkaren, S. J., & Mamidala, J. V. (2023). Forecasting Stock Price Movements With Deep Learning Models for time Series Data Analysis. *Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-531. DOI: doi. org/10.47363/JAICC/2023 (2)*, *489*, 2-9.

[22] Nadella, V. M. (2023). Anomaly Detection and Fault Prediction using ML in Telecom Operations. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(3), 134-143.

[23] Kosaraju, P., & Nadella, V. M. (2022). Security and Privacy in IoT Ecosystems. *Universal Library of Engineering Technology*, (Issue).

[24] Singh, A. A. S. S., Mania, V., Kothamaram, R. R., Rajendran, D., Namburi, V. D. N., & Tamilmani, V. (2023). Exploration of Java-Based Big Data Frameworks: Architecture, Challenges, and Opportunities. Journal of Artificial Intelligence & Cloud Computing, 2(4), 1-8.

[25] Routhu, K. K. (2023). AI-driven succession planning in Oracle HCM Cloud: Building resilient leadership pipelines through predictive analytics. *International Journal of Science, Engineering and Technology*, *11*(5).

[26] Tamilmani, V., Namburi, V. D., Singh Singh, A. A., Maniar, V., Kothamaram, R. R., & Rajendran, D. (2023). Real-Time Identification of Phishing Websites Using Advanced Machine Learning Methods. *Available at SSRN 5837142*.

[27] Routhu, K. K. (2023). AI-driven succession planning in Oracle HCM Cloud: Building resilient leadership pipelines through predictive analytics. International Journal of Science, Engineering and Technology, 11(5). https://doi.org/10.5281/zenodo.17292018

[28] From Fragmentation to Focus: The Benefits of Centralizing Procurement. (2023). International Journal of Research and Applied Innovations, 6(6), 9820-9833. https://doi.org/10.15662/

[29] Routhu, K. K. (2023). Embedding fairness into the digital enterprise, data driven DEI strategies with Oracle HCM Analytics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *9*(8), 266-274.

[30] Routhu, K. K. (2023). AI-driven skills forecasting in Oracle HCM Cloud: From static competencies to predictive workforce design. *International Journal of Science, Engineering and Technology*, *11*(1).

[31] Padur, S. K. R. (2023). AI-Augmented Enterprise ERP Modernization: Zero-Downtime Strategies for Oracle E-Business Suite R12. 2 and Beyond. *Available at SSRN 5605510*.

[32] Routhu, K. K. (2022). From Case Management to Conversational HR: Redefining Help Desks with Oracle's AI and NLP Framework. *International Journal of Science, Engineering and Technology*, *10*(6).

[33] Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., & Patchipulusu, H. H. S. (2022). Blockchain Technology in Supply Chain and Logistics: A Comprehensive Review of Applications, Challenges, and Innovations. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(3), 72-80.

[34] Attipalli, A., BITKURI, V., Mamidala, J. V., Kendyala, R., & KURMA, J. (2022). Empowering Cloud Security with Artificial Intelligence: Detecting Threats Using Advanced Machine learning Technologies. *Available at SSRN 5741263*.

[35] Padur, S. K. R. (2022). Intelligent resource management: AI methods for predictive workload forecasting in cloud data centers. *J. Artif. Intell. Mach. Learn. & Data Sci*, *1*(1), 2936-2941.

[36] Nadella, V. M. (2022). Digital Twins for Predictive Network Management and System Simulation. *International Journal of AI, BigData, Computational and Management Studies*, *3*(3), 100-111.

[37] Routhu, K. K. (2022). From RFID to Geofencing: IoT-Enabled Smart Time Tracking in Oracle HCM Cloud. *International Journal of Science, Engineering and Technology*, *10*(4).

[38] Nadella, V. (2019). Extracting road traffic data through video analysis using automatic camera calibration and deep neural networks.

[39] Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Vangala, S. R. (2022). Data Security in Cloud Computing: Encryption, Zero Trust, and Homomorphic Encryption. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 31-41.

[40] Padur, S. K. R. (2022). AI augmented platform engineering, transforming developer experience through intelligent automation and self optimizing internal platforms. *International Journal of Science, Engineering and Technology*, *10*(5), 10-5281.

[41] Kosaraju, P. , & Nadella, V. M. (2021). Quality of Experience (QoE) and Network Performance Modelling for Multimedia Traffic. Journal of Artificial Intelligence and Big Data, 1(1), 1-13. https://doi.org/10.31586/jaibd.2021.135