International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-9, Issue-12, 2022 Regular Edition E-ISSN: 2349-7084

Cyber Threat Security System Using Artificial Intelligence for Android-Operated Mobile Devices

[1]K Thejeswari , [2]K Sreenivasulu ,[3]B Sowjanya

[1]M.Tech Student , G.Pullaiah College of Engineering and Technology , Kurnool
[2]Professor of CSE , G.Pullaiah College of Engineering and Technology , Kurnool
[3]Assistant Professor of CSE , G.Pullaiah College of Engineering and Technology , Kurnool

Corresponding author : ***K Thejeswari***

Available online at: http://www.ijcert.org

Received: 18/10/2022, Revised: 02/11/2022, Accepted: 23/12/2022, Published: 08/01/2023

Abstract: Malicious attacks on Android mobile devices have increased as smartphone usage has grown rapidly. The Android systems accommodate a variety of important approaches, like banking applications; hence, they become the target of malware that uses security system vulnerabilities. The cyber threat has grown exponentially over the past decade. Cybercriminals have become highly experienced. Current security regulators were insufficient to protect networks from an increasing number of highly skilled cybercriminals. The latest advances in Artificial Intelligence (AI) methods have led to a high level of innovation and automation. While the AI techniques provide important advantages, they could be utilized maliciously. The latest creation of cyber threats leverages modern AI (artificial intelligence)-aided techniques that are efficient for launching multi-level, potent, and potentially devastating attacks. Present cyber defence systems face different problems in protecting against recent and emerging risks. Hence, in this work, a cyber-threat security system using artificial intelligence for Android-operated mobile devices is presented. The machine learning (ML) and deep learning (DL) algorithms can conveniently identify threats on Android mobile devices.

Keywords: Android Mobile devices, Artificial Intelligence, Cyber threats, Cyber security, Machine Learning and Deep Learning

---

1. Introduction

In present time, admiration for Android-operated cellular devices has allured the attention of malware developers, and this particular task is increasing quickly [1]. With the rapid development of technologies, the utilisation of smart phones with the latest specifications enhances the connected Android applications. In general, security is built into Android systems, with sandboxing techniques and authorization systems programmed to reduce the threat of Android applications. The former is implemented by utilising the Linux environment to run Android applications, which enables the user to grant permissions to install any applications. Anyhow, while updating or upgrading cellular applications, security and privacy parameters like time permission, background location, memory, etc. are modified, this gives a time frame for malware attacks. Customers could exploit Android vulnerabilities during application development because Google Play Store didn't detect malicious attacks until applications were published.

Artificial intelligence is accelerating both economic and social development. It has also become one of the key technologies of digitalization, creating both opportunities and risks [2].

The majority of malware development focuses on cellular devices, which hackers hack and turn into bots.That enables hackers to approach affected devices with another associated device and create botnets. Botnets were utilised to implement various malicious attacks like distributed denial-of-service (DDoS), spam forwarding, stealing information, etc. Malicious botnet attacks were implemented by modern methods (e.g., multi-stage payload or self-defense), producing hard-to-detect malware. As a result, it causes the primary risks, necessitating the programme for beneficial policies to detect these attacks.As a result, developing high potential

and capability cyber security resolutions was a current priority [3].

Cybersecurity is the design of protective plans that protect computing resources, networks, programs, and information from unlicensed approaches, alteration, and smashing. Because of further considerations in data and communication technologies, recent cyber security threats emerged and were modified quickly. It was important for the automatic detection of stages in a cyberattack on a host. This facilitates automated forensics that leads to quick attack discovery, risk evaluation, and eventually remediation. This indicates an important level of knowledge about the attacker's target [4]. A robust cyber defence system must be able to protect against the latest cyber threats [5].

However, cybercriminals adopted the latest and most advanced methods to increase the power and scale of their attacks. However, there was a requirement for simple, adaptive, and strong cyber defence systems that were efficient at identifying multiple damages in real time. Adoption of AI technologies has increased recently, and it now plays an important role in the detection and prevention of cyber threats [6].

In a positive sense, AI can be utilised for defence against cyber threats or protection in general (defensive AI). By means of AI, malware, spam, and phishing emails can be detected more accurately. This can significantly increase the level of IT protection. At the same time, AI can make cyber-attacks much more efficient and scalable. The usage of AI as a disruptive force is often referred to as "offensive AI."

It also complicates the investigation and development of the protection process used by these applications, as a result of recent difficulties and vulnerabilities in Android applications that attackers can exploit immediately. The view of Android applications of digital e-commerce, e-business, savings, and online banking was combined with confidential and valued data communicated over cellular networks, which was significant to calculate the application’s information regarding optimal protection. To ensure that no protection access occurred in this network, ML and DL models were detected by utilising identification of malicious attacks against Android applications.

In recent times, the ML and DL classifiers have gained a lot of attention due to their accurate and reliable results. Several machine learning algorithms and the DL algorithm are used to classify normal and abnormal botnet attacks. ML and DL models are used to detect Android botnets. In this paper, a cyber-threat security system using AI for Android-operated mobile devices is presented. In this approach, various ML and DL models were used to investigate the performance of the presented approach.

2. Literature Survey

Jonghoon Lee, Jonghyun Kim, Ikkyun Kim, and Kijun Han et al. [7] present cyber threat detection based on ANN using event profiles. The suggested technology changes the collected multiple protection events into separate event profiles and utilises DL-based identification techniques for better cyber-risk identification. Accordingly, the examiner outcomes of this investigation confirm that suggested techniques can utilise learning-based algorithms for network intrusion-identification and even present actual time utilization; implementation performs better than traditional ML techniques.

A.M.S.N. Amarasinghe, W.A.C.H. Wijesinghe, D.L.A. Nirmana, Anuradha Jayakody, A.M.S. Priyankara et al. [8] present an AI-based cyber threat and vulnerability identification, prevention, and prediction model. The suggested application was an automatic system that includes a process to enforce vulnerabilities and a large database of familiar vulnerabilities. CNN detects vulnerabilities, and AI-based generative algorithms perform the remediation method and enhance the accuracy.

Ozan Veranyurt et al. [9] discussed the usage of artificial intelligence in DOS/DDOS attack detection. In this work, the author aimed to examine the detection of denial-of-service attacks through different machine learning algorithms and artificial neural networks (ANNs). The evaluation will be done with the Knowledge Discovery and Data Mining Tools Competition (KDD 99) dataset and the data collected in lab tests. The focus of the study will be the assessment of the ML and ANN models' success in the identification of network layer DOS attacks.

Ricardo Calderon et al. [10] discussed the advantages of AI in cyber security. The approach of AI can enhance the identification rate of IDPS systems, and machine learning methods can mine the data to identify the sources of botnets. Anyhow, the execution of artificial intelligence might show different damages, and cyber security professionals must notice stability among threats and advantages.

Vishal Dineshkumar Soni et al. [11] discussed the role of AI in combating cyberthreats in banking. Exact mode is produced by artificial intelligence for the banking sector; thereby, it can detect fraud in transactions. Artificial intelligence was clearly linked to the domain of cyber security. Different types of cybercrimes can be blocked and detected by artificial intelligence-based fraud detection models.

Nitika Khurana, Sudip Mittal, Aritran Piplai, Anupam Joshi, et al. [12] have discussed the prevention of poisoning attacks on AI-based threat intelligence systems. In this analysis, it utilises an ensemble of semi-supervised applications to assure the validity of information obtained by AI systems by assessing the trustworthiness of Reddit posts, and the security analysts use these systems to describe available risk by examining data spread on social media websites, forums, blogs, etc.

Gregory Falco, Arun Viswanathan, Carlos Caldera, Howard Shrobe, et al. [13] present A Master Attack Methodology for an AI-Based Automated Attack Planner

 https://doi.org/10.22362/ijcert/2022/v9/i12/v9i1207

for Smart Cities. This implementation can protect both novices and experts in detecting attacks.They suggest and produce a trail for automated attack generation techniques that could provide clear, adjustable, and consistent attack trees in the initial phase of protection, which is a difficult framework for cyber-attack.

Amaan Anwar & Syed Imtiyaz Hassan et al. [14] Applied AI Methods to Prevent Cyber Assaults In order to enhance the expansion of cyber security, a comprehensive view of the cyber environment of associations where AI is integrated with human knowledge is necessary, as neither humans nor artificial intelligence can prove complete achievement in this field.

Nadine Wirkuttis and Hadas Klein et al. [15] discussed AI in cyber security. Artificial intelligence methods will enhance their complete protection implementation and produce the best security against increasingly sophisticated cyber threats. Along with the increased chances of artificial intelligence in cyber security, there are valid risks and analyses associated with its use. Socially managed use of AI methods is necessary for advanced reduction of the associated risks and concerns.

3. Cyber threat Security System Using AI

In this work, cyber threat security system using Artificial Intelligence for android-operated mobile devices is presented. The block diagram of presented system is shown in Fig. 1.

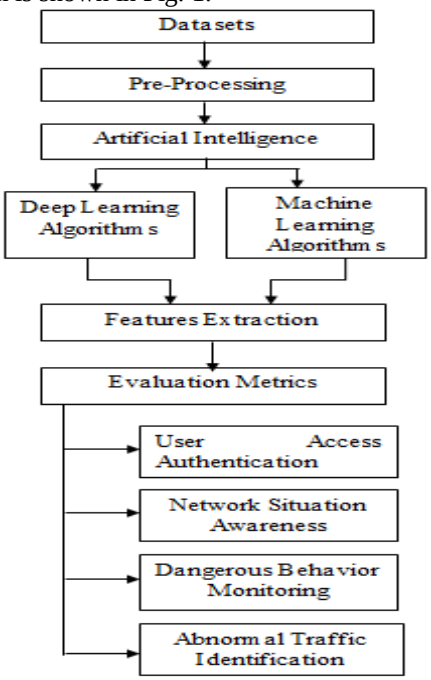

Figure 1. The Block diagram Of Presented System

Examinations were implemented with two standard datasets: Canadian Institute for Cyber Security (CICAndMal2017) and Drebin datasets. The Cyber Security Datasets was standard mobile malware dataset that includes both constant and modern specifications of record files. The datasets are formed from different network runs utilizing CICFlowMeter-V1 and CICFlowMeter- V3. The Drebin dataset is obtained from 15,037 approaches of Drebin program that includes two hundred and fifteen specifications and injections of 5560 malware and 9476 common approaches.

The Android datasets had various formats and features; hence, preprocessing was most significant for controlling the dataset.

Minimum–Maximum Normalization Method: Normalization was calculating application for shift as well as rescales dataset outcomes. The minimum–maximum normalization technique is implemented to calculate information in the range of 0 and 1. The normalization technique is implemented for overlap of complete datasets utilizing following equation:

$$V' = \frac{V - x_{min}}{\max(A) - \min(A)} (new_{\max(A)} - new_{\min(A)} + new_{\min(A)} \dots (1)$$

where, min(A) and max(A) were the minimum and max information, respectively, new_min(A) and new_max(A) were recent outcomes of min and max utilized for calculation of information, as well as 'V' is normalized information.

AI can quickly operate a large amount of information and has a best detection impact for particular situations. However it might be disrupted and may not confirm the recent condition accurately. Interactive ML utilized in AI is also incorporated in cyber security.

The Support Vector Machine (SVM) was a supervised ML model implemented to rectify linear and nonlinear approaches difficult issues. That was utilized to sketch hyper plane among data points which were close to hyperplane as well as evaluate impact of position and situation of hyperplane, known as Support Vector (SV). A best execution of Support Vector can be obtained if data points distance was near to hyperplane. SVM has several functions, both linear and non-linear; RBF (Radial Basis Function) was suitable for separate models due to network information have a difficult structure. Linear Regression (LR) could examine as one of the best conventional ML model in which the better fit line/hyper plane for the accessible training data was described utilizing the minimum mean squared error function.

A Multilayer perceptron (MLP) was a feed forward ANN which makes pair of results provides pair of inputs. An MLP is characterized by many layers of input nodes connected as a directed graph between the input nodes and outcome layers. A MLP having only three layers of nodes: input, hidden, and output layer.

CNN-LSTM (Convolutional Neural Network- Long Short-Term Memory) was a combination design generated with fusion of Convolutional Neural Network and Long Short-Term Memory; both were DL AI algorithms. The Convolutional Neural Network is having invisible neurons with trainable mass and bias features. That was widely implemented to examine information in

 https://doi.org/10.22362/ijcert/2022/v9/i12/v9i1207

grid layout, forming dissimilar from remaining framework. That was known as feed-forward network due to input data stream in single path, from input to production layer.

Feature extraction was an important element of the ML workflow that means that the developer would have to provide only related data to the models; hence it can describe the exact answer and enhances the capability of the algorithm. Feature extraction indicates the method for transforming raw information into numerical parameters which could operate during saving the data in actual data set. Feature Extraction goal that decreases features count in dataset by forming recent attributes from presented (and get rid of actual attributes). The recent decreased set of attributes shall able to conclude better for data contained in actual features set.

The datasets are classified into 80% training and 20% testing data. The random operation for dividing the training and testing was showed. The training level is implemented to suit the model utilizing the Android malware datasets. The test level is programmed to check available programs utilizing recent information. The most effective execution of ML and DL algorithms guarantees protection of Android-operated mobile device applications.

In this approach, the ML models including Linear regression, SVM and DL, MLP algorithms and CNN-LSTM (Convolution Neural Network-Long Short-Term Memory) are used to validate the performance of presented system in order to provide greater user authentication, network situation awareness, harmful nature observation and anomalous traffic detection.

User authentication is checking of a user's detection by utilization of mobile device and single or many authentication techniques for security access. User authentication checks the detection of a user attempting to get approach to a network or mobile by permitting the change of credentials from a human to a machine at the time of interactions on the network to ensure user authenticity. Network situation awareness is a platform for analyzing and displaying customers' current network performance and security status based on threat intelligence, big data, visualization and other technologies. Network situational understanding was about the design and content of the network that might not match what they think. So what tools are available to produce the important data and how do they do it?

Dangerous nature observation is recent applications for inner side risk obstruction and identification. Anomalous network traffic was traffic caused by malicious reasons along with traffic by different dangerous attacks, Internet worm and scan. The identification segment obtains data run from observation systems or routers.

The performance of presented ML and DL algorithm is calculated with respective to accuracy, precision and sensitivity.

4. Result Analysis

In this part the output examination of cyber threat security system using Artificial intelligence for android-operated mobile devices is discussed. The performance evaluation of presented algorithms on standard Android malware dataset is regulated using the Python programming language. The statistical investigation evaluates output of presented algorithms.

The performance metrics are evaluated depends on the following values. The True Positive (TP) indicates the number of examples that were achieved and divided as positive sentiment, False Positive (FP) was number of examples which were not exactly divided as negative sentiments, True Negative (TN) indicates number of examples which were divided as negative sentiment, and False Negative (FN) indicates number of examples which were not exactly divided as positive sentiments.

Accuracy: It is ratio of exactly divided samples to complete classified samples and it is expressed as

$$Accuracy = \frac{TP}{TP + TN + FP + FN} \quad (1)$$

Sensitivity: It is called as recall. It is described as ratio of exactly classified positive samples to complete number of positive samples (i.e. TP+ FN).

$$Sensitivity = \frac{TP}{TP + FN} .. \quad (2)$$

Precision: The precision can be described as number of TPs to total positive predictions (i.e. TP+FP).

$$Precision = \frac{TP}{(TP + FP)} ... \quad .(3)$$

The performance of various ML and DL algorithms is shown in Table 1.

Table 1: Performance Evaluation of Different Ml and Dl Algorithms

Algorithms	Accuracy (%)	Precision (%)	Sensitivity (%)
LR	82.4	84.3	80.6
MLP	91.7	90	92.7
SVM	94	95.2	93.4
CNN-LSTM	95.4	97	96.5

In ML algorithms, the SVM algorithm has better performance than LR algorithm whereas in DL algorithms the CNN-LSTM has better results compared to MLP. The CNN-LSTM has better results than SVM, MLP and LR. The comparison between these four algorithms is shown in Fig. 2.

 https://doi.org/10.22362/ijcert/2022/v9/i12/v9i1207

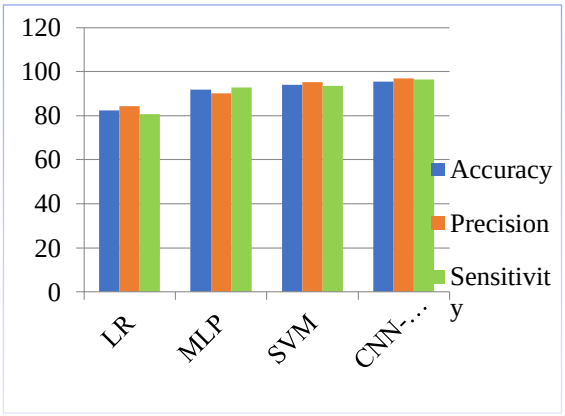

Fig. 2: Performance Comparison of Different Ml and Dl Algorithms

Compared to traditional mobile devices, presented cyber threat security system has better results in terms of user authentication, understanding of network condition, and harmful nature observation and abnormal traffic detection for Android-operated mobile devices. The Fig. 3 shows the performance comparison between traditional approaches and presented cyber threat security system using AI for android operated mobile devices.

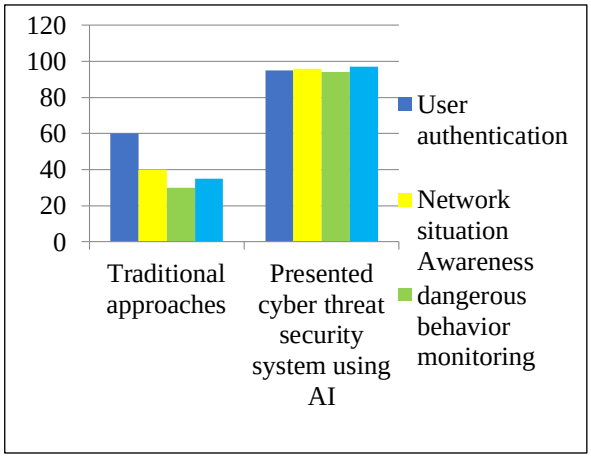

Figure 3. Performance Comparison Graph

Therefore, presented cyber threat security system using AI effectively monitors the dangerous behavior, identifies the abnormal traffic and provides user authentication as well as awareness about network situation. This system has greater results for Android-operated Mobile devices in order to detect and monitor the abnormalities and threats.

5.Concussions

In this work, a cyber-threat security system using artificial intelligence for Android-operated mobile devices is presented. In this approach, different ML and DL algorithms are utilized to calculate and verify the execution of the presented system. There are different types of ML and DL algorithms like LR, SVM, Multilayer Perceptron, and CNN-LSTM-Memory. This method makes use of the CICAndMal2017 and Drebin datasets. The SVM and conventional neural network long short-term memory algorithms achieved high execution accuracy for implementing an accurate cyber threat security system that can aid in the protection of android-operated mobile devices against threats. Compared to traditional mobile devices, the presented system has better results in terms of user authentication, understanding of network conditions, harmful nature observation, and abnormal traffic detection for Android-operated mobile devices.

References

[1] Hasan Alkahtani and Theyazn H. H. Aldhyani, “Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices”, Sensors 2022, 22, 2268, doi.org/10.3390/s22062268

[2] Daniel Kant, Andreas Johannsen, “Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)”, 2022, Society for Imaging Science and Technology, doi.org/10.2352/EI.2022.34.3.MOBMU-38

[3] Zhimin Zhang, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang, Kim‐Kwang Raymond Choo, “Artificial intelligence in cyber security: research advances, challenges, and opportunities”, 2021 Springer, doi.org/10.1007/s10462-021-09976-0

[4] Muhammed AbuOdeh, Christian Adkins, Omid Setayeshfar, Prashant Doshi, Kyu H. Lee, “A Novel AI-based Methodology for Identifying Cyber Attacks in Honey Pots”, The Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI-21), 2021, Association for the Advancement of Artificial Intelligence

[5] Hooman Alavizadeh, Julian Jang-Jaccard, Tansu Alpcan and Seyit A. Camtepe, “A Markov Game Model for AI-based Cyber Security Attack Mitigation”, arXiv:2107.09258v1 [cs.GT] 20 Jul 2021

[6] Thanh Cong Truong, Quoc Bao Diep and Ivan Zelinka, “Artificial Intelligence in the Cyber Domain: Offense and Defense”, Symmetry 2020, 12, 410; doi:10.3390/sym12030410

[7] Jonghoon Lee, Jonghyun Kim, Ikkyun Kim, And Kijun Han, “Cyber Threat Detection based on Artificial Neural Networks using Event Profiles”, VOLUME 7, 2019, DOI 10.1109/ACCESS.2019.2953095, IEEE Access

[8] A.M.S.N. Amarasinghe, W.A.C.H. Wijesinghe, D.L.A. Nirmana, Anuradha Jayakody, A.M.S. Priyankara, “AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System”, 2019 International Conference on Advancements in Computing (ICAC), December 5-6, 2019. Malabe, Sri Lanka

[9] Ozan Veranyurt, “Usage of Artificial Intelligence in DOS/DDOS Attack Detection”, International Journal of

Basic and Clinical Studies (IJBCS) 2019; 8(1): 23-36, ISSN:2147-1428

[10] Ricardo Calderon, "The Benefits of Artificial Intelligence in Cyber security", Economic Crime Forensics Capstones, 2019, doi: digitalcommons.lasalle.edu/ecf_capstones

[11] Vishal Dineshkumar Soni, "Role Of Artificial Intelligence in Combating Cyber Threats in Banking", International Engineering Journal For Research & Development, 4(1), 7, 2019, doi.org/10.17605/OSF.IO/JYPGX

[12] Nitika Khurana, Sudip Mittal, Aritran Piplai, Anupam Joshi, "Preventing Poisoning Attacks on AI Based Threat Intelligence Systems", 2019 IEEE, 978-1-7281-0824-7/19

[13] Gregory Falco, Arun Viswanathan, Carlos Caldera, And Howard Shrobe, "A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities", 2018 IEEE ACCESS, doi:1 0.1109/ACCESS.2018.2867556

[14] Amaan Anwar & Syed Imtiyaz Hassan, "Applying Artificial Intelligence Techniques to Prevent Cyber Assaults", International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 5 (2017), pp. 883-889

[15] Nadine Wirkuttis and Hadas Klein, "Artificial Intelligence in Cyber security", Volume 1, No. 1, 2017, Academia

 https://doi.org/10.22362/ijcert/2022/v9/i12/v9i1207