CYBER SECURITY SYSTEM FOR MOBILE DEVICES USING ARTIFICIAL INTELLIGENCE

[1]Dr. R. Rambabu, [2]G. Swarnalatha, [3]Dr. D. Naga Purnima

[1]Professor & HOD, Department of Computer Science & Engineering, Rajamahendri Institute of Engineering & Technology, Rajamahendravaram, A.P, India
[2]Associate Professor, Department of Computer Science & Engineering, Rajamahendri Institute of Engineering & Technology, Rajamahendravaram, A.P, India
[3]Professor& HOD, Department of Mathematics, Rajamahendri Institute of Engineering & Technology, Rajamahendravaram, A.P, India

ABSTRACT: The fast rise in smartphone usage has coincided with an upsurge in malicious attacks targeting Android mobile devices. Android systems provide several significant methods, such as banking apps; as a result, malware that takes advantage of security flaws in systems targets them. Throughout the last ten years, the cyber threat has increased dramatically. The skills of cybercriminals have advanced significantly. The networks were not sufficiently protected by the security regulators in place against the growing number of highly adept cybercriminals. High levels of innovation and automation have resulted from the most recent developments in Artificial Intelligence (AI) techniques. Even while AI approaches have many benefits, they might also be used maliciously. Modern Artificial Intelligence (AI)-assisted approaches are being used by the most recent generation of cyber threats to undertake multi-level, powerful, and possibly deadly attacks. Different issues arise while trying to defend against new and developing threats with current cyber defense technologies. Therefore, an artificial intelligence-based cyber-threat protection system for Android-powered mobile devices is provided in this study.

KEYWORDS: Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Cybercriminals

I. 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

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.

II. LITERATURE SURVEY

jun 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 intrusionidentification 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 semisupervised 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 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.

III. METHODOLOGY

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.

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. 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.

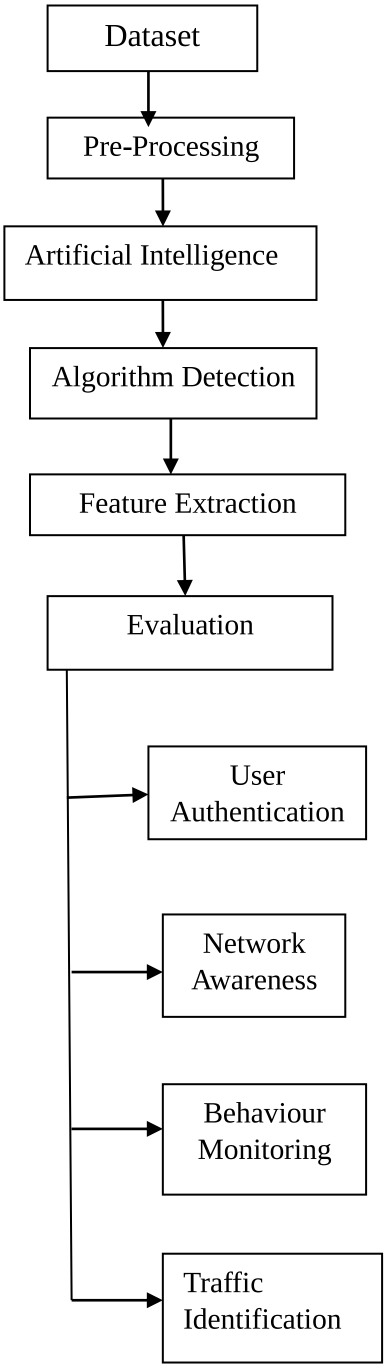

Fig.1: Block diagram Of Presented System

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 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. 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 and precision.

IV. 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.

Table.1: Performance Analysis

Parameters	Traditional Methods	AI
Threats detection	82.4	90
Time	9727	7546

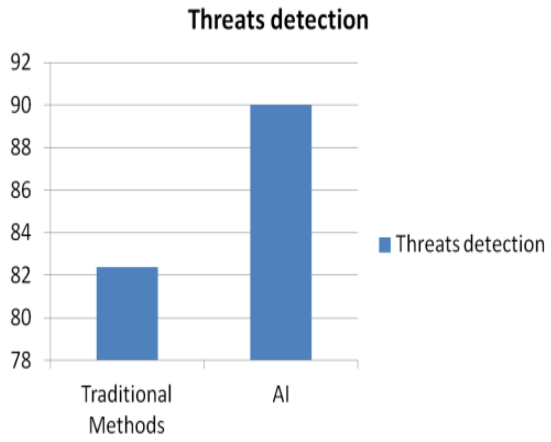

Fig.2: Threats Detection Comparison Graph

In Fig.2 threats detection comparison graph is observed between traditional methods and AI.

In Fig.3 time comparison graph is observed between traditional methods and AI.

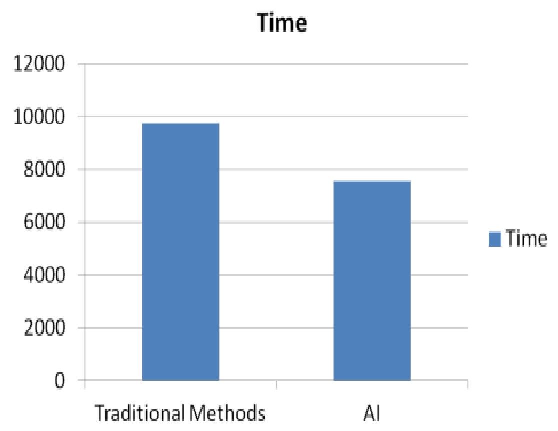

Fig.3: Time Comparison Graph

V. CONCLUSION

In this study, an artificial intelligence-based cyber-threat security solution for Android-powered mobile devices is provided. Several machine learning and deep learning techniques are applied in this method to compute and validate the system's operation. The Drebin and CICAndMal2017 datasets are used in this strategy. High execution accuracy was attained by the SVM and traditional neural network long short-term memory algorithms for the purpose of building an accurate cyber threat security system that can help shield Android-operated mobile devices from attacks. In terms of user authentication, network state comprehension, dangerous nature observation, and abnormal traffic detection for Android-operated mobile devices, the provided system performs better than traditional mobile devices.

VI. REFERENCES

[1] E. Hodo, X. Bellekens, A. Hamilton and P. L. Dubouilh, "Threat analysis of IoT networks using artificial neural network intrusion detection system", *Proceedings of the International Symposium on Networks Computers and Communications (ISNCC)*, pp. 1-6, 2017.

[2] O. Vermesan, P. Friess and P. Guillemin, "Internet of things strategic research roadmap", *Global Technological and Societal Trends*, vol. 1, pp. 9-52, 2012.

[3] L. Cao, "Data science: a comprehensive overview", *ACM. Computing Surveys (CSUR)*, vol. 50, no. 3, pp. 43, 2017.

[4] J. Kivimaa, A. Ojamaa and E. Tyugu, "Graded security expert system", *International Workshop on Critical Information Infrastructures Security*, pp. 279-286, 2010.

[5] Murat Yesilyurt and Yildiray Yalman, "Security Threats on Mobile Devices and their Effects: Estimations for the Future", *International Journal of Security and Its Applications*, vol. 10, no. 2, pp. 13-26, 2016.

[6] C. Panchev, P. Dobrev and J. Nicholson, "Detecting port scans against mobile devices with neural networks and decision trees", *International Conference on Engineering Applications of Neural Networks*, pp. 175-182, 2014.

[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