Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A BLOCKCHAIN-BASED MULTIMODAL APPROACH TO MALWARE DETECTION IN ANDROID IOT ECOSYSTEMS

BALINGAN SANGAMESHWAR[1], P. CHANDRA MOUNIKA[2], PRAVEENA MANDAPATI[3], J. MANORANJINI[4], TIRUMALASETTI LAKSHMI NARAYANA[5], V. SUJATHA LAKSHMI[6], D. N. V. SATYANARAYANA[7]

[1]Department of CSE (CyS, DS and AI & DS), Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad, Telangana, India
[2]Department of CSE (Cyber Security), Vignana Bharati Institute of technology, Ghatkesar, Hyderabad, Telangana, India
[3]Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
[4]Department of Artificial Intelligence and Data Science, Rajalakshmi Engineering College, Chennai, Tamilnadu, India
[5]Department of Electrical and Electronics Engineering, Aditya University, Surampalem, Andhra Pradesh, India
[6]Department of Computer Applications, R V R & J C College of Engineering, Guntur, Andhra Pradesh, India
[7]Department of Chemical Engineering, R V R & J C College of Engineering, Guntur, Andhra Pradesh, India

E-mail: balingan.sangameshwar@gmail.com, mounika803@gmail.com, praveena.conf@gmail.com, drmanoranjinicse@gmail.com, tlaxman17@gmail.com, sujathavdmpudi@gmail.com, dnvsatya2001@gmail.com

ABSTRACT

As the Internet of Things (IoT) continues to proliferate, the security challenges associated with interconnected devices have become increasingly complex. Malicious actors exploit vulnerabilities in IoT networks, leading to the need for robust solutions in malware detection and classification. This research proposes a novel approach by integrating block chain technology into the IoT security framework to enhance the efficiency and reliability of malware detection. The study investigates the limitations of traditional malware detection methods in IoT environments and explores the potential of block chain to address these challenges. Block chain's decentralized and tamper-resistant nature provides a secure and transparent platform for recording and validating data transactions within the IoT ecosystem. By leveraging block chain, the research aims to establish a trustworthy and resilient infrastructure for detecting and classifying malware in real-time. Furthermore, the paper discusses the implementation of a block chain-based consensus mechanism to validate the integrity of data collected from IoT devices. This consensus model ensures the authenticity of information, reducing the risk of false positives or negatives in malware detection. Additionally, the study explores the use of smart contracts to automate and enforce security policies, enhancing the overall responsiveness of the system. The proposed approach not only contributes to the advancement of IoT security but also lays the foundation for a more collaborative and secure IoT ecosystem. The findings of this research have significant implications for industries relying on IoT technologies, emphasizing the importance of proactive measures to safeguard interconnected devices from evolving cyber threats.

Keywords: *Internet of Things, malware detection, classification, block chain, IoT security*

1. INTRODUCTION

The advent of the Internet of Things (IoT) has ushered in a new era of connectivity, enabling seamless communication and interaction between devices, sensors, and systems. IoT networks encompass a wide array of devices, ranging from consumer electronics like smart thermostats and wearable fitness trackers to industrial machinery and infrastructure monitoring sensors. These interconnected devices collect and exchange vast amounts of data, driving efficiency gains, automation, and innovative services across various sectors, including healthcare, transportation, manufacturing, and agriculture [1]. The significance of IoT networks lies in their ability to enhance productivity, streamline processes, and improve quality of life. In healthcare, for instance, IoT-enabled medical devices can monitor patient vital signs remotely, enabling timely interventions and reducing hospital readmissions. In smart cities, IoT sensors can optimize traffic flow, reduce energy consumption, and enhance public safety through real-time monitoring and data analytics. However, alongside these transformative benefits, the rapid proliferation of IoT devices has also brought about unprecedented security challenges [2]. The decentralized and heterogeneous nature of IoT ecosystems presents a complex security landscape, characterized by numerous entry points for potential cyberattacks. IoT devices often have limited computational resources and may lack robust security mechanisms, making them vulnerable to exploitation by malicious actors. Moreover, the sheer scale and diversity of IoT deployments make it challenging to enforce consistent security measures across all devices and networks [3]. Recent years have seen a surge in cyberattacks targeting IoT devices, ranging from relatively simple exploits, such as default password attacks and firmware vulnerabilities, to more sophisticated threats, including botnets, ransomware, and supply chain attacks. These attacks can have far-reaching consequences, compromising sensitive data, disrupting critical services, and even posing physical safety risks in certain contexts [4].

1.1 Need for Effective Malware Detection and Classification Mechanisms

In light of these security concerns, there is an urgent need for effective malware detection and classification mechanisms tailored to the unique characteristics of IoT networks. Traditional security solutions, such as signature-based antivirus software and network intrusion detection systems (IDS), may prove inadequate in detecting zero-day exploits and polymorphic malware variants prevalent in IoT environments. Moreover, the resource constraints of IoT devices necessitate lightweight and efficient detection methods that minimize computational overhead and power consumption [5]. Block chain technology, originally devised as the underlying framework for cryptocurrencies like Bitcoin, has garnered significant attention for its potential applications beyond financial transactions. At its core, a block chain is a decentralized and distributed ledger that records transactions in a secure and immutable manner. Each block in the block chain contains a cryptographic hash of the previous block, creating a chain of blocks that are resistant to tampering and modification. In the realm of cybersecurity, block chain technology holds promise as a means of enhancing data integrity, transparency, and trust in digital transactions and communications. By decentralizing control and eliminating single points of failure, block chain can mitigate the risk of data breaches and unauthorized access [6]. Moreover, the use of cryptographic techniques ensures the confidentiality and authenticity of transactions, bolstering security across various applications. In the context of IoT security, block chain technology offers several potential benefits, including:

Immutable Recordkeeping: The immutable nature of block chain ensures that once data is recorded on the ledger, it cannot be altered or deleted without consensus from the network participants. This property can enhance the integrity and auditability of IoT data, reducing the risk of data manipulation and tampering. Decentralized Trust: By distributing trust among network participants and eliminating the need for centralized intermediaries, block chain can enhance the resilience of IoT networks against single points of failure and malicious attacks. Smart contracts, self-executing contracts coded on the block chain, enable automated and tamper-proof enforcement of agreements and policies in IoT deployments. Secure Identity Management: Block chain-based identity management systems can provide a secure and verifiable means of authentication and access

control for IoT devices and users. Decentralized identity solutions empower individuals to maintain control over their personal data and selectively disclose information to authorized parties [7].

Transparent Auditing and Compliance: The transparent and auditable nature of block chain transactions facilitates regulatory compliance and accountability in IoT deployments. Organizations can leverage block chain to track the provenance and lifecycle of IoT devices, ensuring adherence to industry standards and data protection regulations. In this paper, we propose leveraging block chain technology as a novel approach for malware detection and classification in IoT networks. By harnessing the decentralized, transparent, and immutable properties of block chain, along with learning algorithms, we aim to develop a robust framework for detecting and mitigating malware threats in real-time. Through the integration of block chain-based security mechanisms, we seek to enhance the resilience and trustworthiness of IoT ecosystems, safeguarding critical infrastructure and sensitive data from malicious actors [8].

2. MALWARE THREATS IN IOT NETWORKS

The proliferation of Internet of Things (IoT) devices has exposed these interconnected networks to a wide array of malware threats, posing significant challenges to the security and integrity of IoT ecosystems. Malicious actors leverage various techniques to exploit vulnerabilities in IoT devices, compromising their functionality, stealing sensitive data, and orchestrating large-scale cyberattacks. Understanding the types of malware targeting IoT devices, the challenges posed by these threats, and the limitations of traditional security measures is crucial for devising effective countermeasures to mitigate the risks [9].

2.1 Types of Malware Targeting IoT Devices

Botnets: Botnets are networks of compromised devices, often referred to as bots or zombies, that are controlled by a central command-and-control (C&C) server. Malicious actors use botnets to launch coordinated attacks, such as distributed denial-of-service (DDoS) attacks, spam campaigns, and cryptocurrency mining. IoT devices, with their ubiquity and diverse capabilities, are prime targets for botnet recruitment due to their often insufficient security measures and always-on connectivity.

Ransomware: Ransomware is a type of malware that encrypts files or locks users out of their devices, demanding a ransom payment in exchange for decryption or restoration of access. IoT devices, including network-attached storage (NAS) devices, surveillance cameras, and smart appliances, are increasingly targeted by ransomware operators seeking to extort money from individuals and organizations. The proliferation of IoT ransomware poses not only financial risks but also threats to privacy and data integrity.

Spyware: Spyware is malicious software designed to secretly monitor and collect information about users' activities without their consent. In the context of IoT devices, spyware can compromise privacy and expose sensitive data, such as audio and video recordings from smart home devices, location tracking data from wearables, and confidential business information from industrial sensors. Malicious actors may exploit spyware to conduct surveillance, espionage, or identity theft attacks.

Malware, as defined by various researchers, is code that is intentionally introduced into a system with the intention of causing damage or bypassing the intended functionality of the system. Illustrated in Figure 1 are the numerous types of malware: Trojan horses, viruses, worms, and so forth.

2.2 Challenges Posed by Malware in IoT Environments

Heterogeneity and Scale: IoT ecosystems encompass a wide range of devices with diverse hardware architectures, operating systems, and communication protocols. Managing security across this heterogeneous landscape is challenging, as each device may have unique vulnerabilities and requirements. Additionally, the scale of IoT deployments, spanning millions of interconnected devices, amplifies the complexity of securing these networks and detecting malicious activities [10]. Resource Constraints: Many IoT devices are resource-constrained in terms of processing power, memory, and energy consumption. Traditional security solutions, such as antivirus software and

intrusion detection systems, may impose significant overhead on IoT devices, impairing their performance and battery life. Designing lightweight and efficient malware detection mechanisms that operate within the resource constraints of IoT devices is essential for maintaining their functionality and usability [11]. Lack of Security by Design: IoT devices are often designed with functionality and connectivity as primary considerations, with security taking a backseat. As a result, many IoT devices lack basic security features, such as secure boot mechanisms, firmware validation, and over-the-air (OTA) update capabilities. Vulnerabilities in IoT devices, combined with the absence of security updates and patches, create opportunities for malware infections and exploitation by malicious actors.

Signature-based Detection: Traditional security measures, such as signature-based antivirus software, rely on known patterns or signatures of malware to detect and block malicious activities. However, signature-based detection is ineffective against zero-day exploits and polymorphic malware variants that continuously evolve to evade detection. IoT environments, with their diverse and rapidly evolving threat landscape, require more adaptive and proactive detection mechanisms. Centralized Security Architectures: Many traditional security solutions rely on centralized architectures, where security controls and monitoring are concentrated in a single location or device. In IoT networks, centralized security architectures may introduce single points of failure and bottlenecks, making them vulnerable to targeted attacks and exploitation. Decentralized and distributed approaches that distribute security functions across IoT devices and networks can enhance resilience and mitigate the impact of security breaches. Manual Security Management: Traditional security measures often require manual configuration, management, and updates, which can be cumbersome and error-prone, particularly in large-scale IoT deployments. IoT devices deployed in remote or inaccessible locations may be challenging to monitor and maintain, increasing the risk of security misconfigurations and vulnerabilities going unnoticed. Automated security solutions that leverage machine learning, artificial intelligence, and orchestration can streamline security management and response workflows in IoT environments.

Figure 1. Various types of malware

In light of these challenges and limitations, there is a pressing need for innovative approaches to malware detection and classification tailored to the unique characteristics of IoT networks. In the subsequent sections of this paper, we explore the potential of blockchain technology as a novel approach for enhancing the security posture of IoT ecosystems, particularly in the context of malware detection and mitigation. By leveraging the decentralized, transparent, and immutable properties of blockchain, along with machine learning algorithms, we aim to develop a robust framework for detecting, classifying, and mitigating malware threats in real-time, while addressing the inherent challenges and limitations of traditional security measures in IoT environments [12].

3. BLOCK CHAIN TECHNOLOGY IN IOT SECURITY

Figures should be labeled with "Figure" and tables with "Table" and should be numbered sequentially, for example, Figure 1, Figure 2 and so on (refer to table 1 and figure 1). The figure numbers and titles should be placed below the figures, and the table numbers and titles should be placed on top of the tables. The title should be placed in the middle of the page between the left

and right margins. Tables, illustrations and the corresponding text should be placed on the same page as far as possible if too large they can be placed in singly column format after text. Otherwise they may be placed on the immediate following page. If its size should be smaller than the type area they can be placed after references in singly column format and referenced in text

Block chain technology, originally conceived as the underlying architecture for cryptocurrencies like Bitcoin, has evolved into a powerful tool with far-reaching applications beyond the realm of finance. In the field of cybersecurity, blockchain holds immense potential for enhancing data integrity, ensuring secure transactions, and strengthening identity management practices. In this section, we delve into the fundamentals of blockchain technology, explore its applications in cybersecurity, and discuss the advantages of leveraging block chain for securing Internet of Things (IoT) networks [13].

3.1 Fundamentals of Block Chain Technology

At its core, a block chain is a decentralized and distributed ledger that records transactions in a secure, transparent, and immutable manner. The key principles underpinning block chain technology include: Unlike traditional centralized systems where data is stored and managed by a single entity or authority, block chain operates on a decentralized network of nodes. Each node maintains a copy of the block chain, ensuring redundancy, fault tolerance, and resilience against single points of failure. Once data is recorded on the block chain, it becomes immutable and tamper-proof. Each block in the block chain contains a cryptographic hash of the previous block, creating a chain of blocks that are linked together in a chronological order. Any attempt to alter the data within a block would require altering all subsequent blocks in the chain, making tampering with the block chain computationally infeasible. The transparent nature of block chain enables all network participants to view and verify transactions recorded on the ledger. Transactions are broadcasted to the entire network and validated through a consensus mechanism, such as proof-of-work or proof-of-stake, ensuring transparency and trust among network participants [14].

Data Integrity and Tamper Resistance: By leveraging block chain for data storage and verification, IoT devices can maintain the integrity of sensor data, event logs, and transactions. Any attempt to tamper with the data recorded on the block chain would be immediately detected, mitigating the risk of data manipulation and unauthorized access. Decentralized Trust: Block chain enables decentralized trust among IoT devices, eliminating the need for centralized intermediaries or trusted third parties. Through consensus mechanisms and cryptographic algorithms, IoT devices can securely exchange data and execute transactions without relying on a central authority, reducing the risk of single points of failure and malicious attacks. Secure Device Authentication: Block chain-based identity management systems can provide a secure and verifiable means of authenticating IoT devices and establishing trust relationships. By leveraging cryptographic keys and digital signatures, IoT devices can securely communicate with each other and validate the authenticity of data sources, mitigating the risk of spoofing and unauthorized access. Immutable Audit Trail: Block chain maintains an immutable audit trail of all transactions and interactions within the IoT network, enabling transparent auditing and forensic analysis. In the event of a security breach or anomaly detection, organizations can trace the origin of the incident, identify compromised devices, and take appropriate remedial actions to mitigate the impact.

Resilience Against Malicious Attacks: Block chain enhances the resilience of IoT networks against malicious attacks by distributing trust and control among network participants. Even if a subset of IoT devices is compromised or compromised, the integrity of the block chain remains intact, enabling unaffected devices to continue operating securely and autonomously. Block chain technology offers a compelling solution for enhancing the security posture of IoT networks by providing data integrity, secure transactions, identity management, and resilience against malicious attacks. By leveraging the decentralized, immutable, and transparent nature of block chain, organizations can strengthen the security and trustworthiness of IoT ecosystems, safeguarding critical infrastructure and sensitive data from cyber threats [15].

4. PROPOSED APPROACH: MALWARE DETECTION AND CLASSIFICATION USING BLOCK CHAIN

In this section, we present a comprehensive framework for malware detection and classification in IoT networks using block chain technology. The proposed approach combines the decentralized, immutable nature of block chain with machine learning algorithms to create a robust and adaptive system for identifying and mitigating malware threats in real-time.

i. IoT Devices: These are the endpoints within the IoT network, including sensors, actuators, and other connected devices. Each IoT device collects data from its environment and communicates with other devices and the block chain network.
ii. Block chain Network: The block chain network serves as the decentralized ledger for recording transactions and storing metadata related to malware detection and classification. It consists of a distributed network of nodes, each maintaining a copy of the block chain ledger.
iii. Malware Detection and Classification Module: This module is responsible for analyzing incoming data from IoT devices, detecting potential malware threats, and classifying them into predefined categories. It leverages machine learning algorithms for predictive analysis and anomaly detection.

This research paper provides an introduction to a standard machine learning workflow utilized for malware detection and classification, encompassing an examination of its challenges and limitations. Additionally, it evaluates the latest advancements and developments in the domain, focusing on deep learning methodologies. In order to enhance comprehension of the proposed machine learning approach for malware detection, the comprehensive workflow process is depicted in Figure 2 and Figure 3.

4.1 Integration of Block chain for Malware Detection

The integration of block chain enables a synergistic approach to malware detection and classification: Block chain for Data Integrity, IoT devices submit data to the block chain network, where it is recorded in a tamper-proof and immutable manner. This ensures the integrity and authenticity of the data, preventing unauthorized modifications or tampering. The malware detection and classification module utilizes algorithms to analyse the incoming data for signs of malicious activity. These algorithms are trained on labelled datasets to recognize patterns and anomalies indicative of malware infections. Smart Contracts for Automated Analysis, Smart contracts, self-executing contracts deployed on the block chain, can automate the analysis and classification of incoming data. Smart contracts define rules and criteria for identifying malware threats, enabling real-time detection and response [16].

4.2 Data Collection and Pre-processing Techniques

Data collection and pre-processing are crucial steps in preparing the data for analysis:

i. Data Collection: IoT devices collect data from various sensors and sources, including network traffic, system logs, and device telemetry. This data is transmitted securely to the block chain network for analysis.
ii. Data Pre-processing: Before analysis, the incoming data undergoes pre-processing to clean, normalize, and transform it into a suitable format for machine learning. This may involve removing outliers, scaling features, and encoding categorical variables.

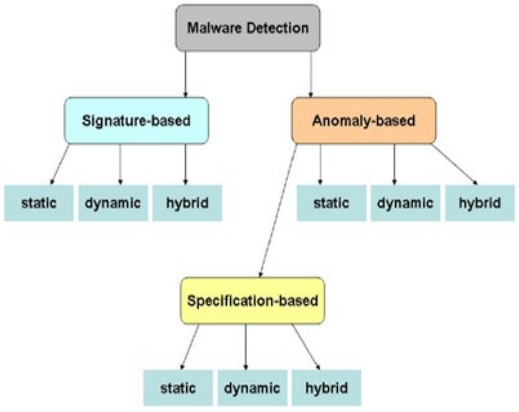

Figure 2. Method proposed for detecting malware

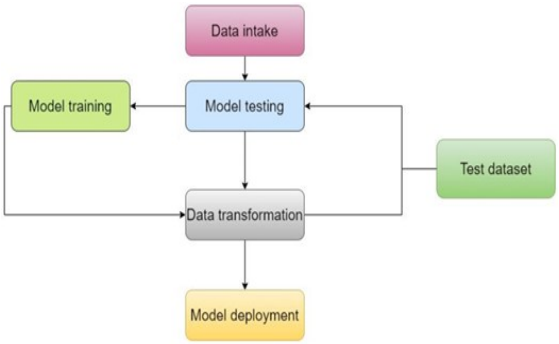

Figure 3. Represents a workflow procedure

4.3 Feature Extraction and Selection for Effective Classification

Feature extraction and selection are essential for identifying informative patterns and reducing dimensionality:

Feature Extraction: Relevant features are extracted from the pre-processed data to capture the characteristics indicative of malware infections. This may include statistical measures, frequency domain analysis, and time-series features extracted from the raw data.

Feature Selection: Dimensionality reduction techniques, such as principal component analysis (PCA) or feature importance ranking, are employed to select the most discriminative features for classification. This helps improve model performance and reduce computational overhead.

By integrating block chain technology with machine learning algorithms and employing effective data collection, pre-processing, feature extraction, and selection techniques, the proposed approach provides a robust and adaptive solution for malware detection and classification in IoT networks. The decentralized, immutable nature of block chain ensures data integrity and transparency, while machine learning enables predictive analysis and real-time detection of malware threats. This framework can significantly enhance the security posture of IoT ecosystems, safeguarding critical infrastructure and sensitive data from cyber threats.

5. RESULTS AND DISCUSSION

Daily Internet use has perks and cons. Internet crime is increasing faster than real-world crime due to cyber-attacks and new viruses that may overcome security measures. Today, malware detection is more complex and challenging than in the past. The signature-based strategy for malware identification is outdated and ineffective for complex current malware detection [30]. While new methods for malware detection exist, it is still challenging to detect all new infections. Detecting malware comprises three steps: analysing, extracting features, and classifying as malicious or benign. Recent cybersecurity research focuses on threat hunting, intelligence, digital forensics, malware detection, and intrusion detection.

Recently, blockchain technology has gained popularity. Consensus-based technologies like fault-tolerant distributed computing systems are essential. IoT data analysts aim to understand blockchain-based IoT data, which is based on DPOS, PoW, PBFT, PoS, and others. Thus, to solve the multi-feature malware detection problem, we adopt a permissioned block-chain structure to store malware feature information. Four layers make to the architecture: 1) Network, 2) Storage, 3) Support 4) IoT devices can afford the Application Layer design. Figure 10 depicts the blockchain architecture for IoT malware detection. Figure 4 shows the blockchain layer's network, support, and storage layers.

There is substantial evidence that the proposed framework outperforms the results of the acquired experiments. Here, we go over the essentials of conducting experiments, such as data sources and statistics, evaluation tools for learning about the performance requirements of the machine learning algorithm we used, and the results that prove our model is worth pursuing.

If the suggested framework's extracted features are important, then the experimental results will show that. Figure 5 displays the clustering findings, which are optimized for the high-dimensional and noisy dataset. Over the two axes following feature reduction, red indicates harmful samples and blue indicates benign samples in clustered data. Figure 6 (a) demonstrates inefficient means-widespread clustering, while Figure 6 (b) demonstrates efficient clustering. Even though two distinct clusters are shown, the depiction of the subspace area of features is obviously predominating. Nevertheless, when looking at the distribution of scores, it's not easy to tell the two groups apart. Hyperplane placement becomes much easier when two clusters are visualized using projections over data points. Drawing such a data

projection is difficult since it requires in-depth analysis of data points during the separation process. Visualizations of various sample data projections in Figures 6 and 7 demonstrate the efficacy of our suggested method in differentiating between malware and benign samples.

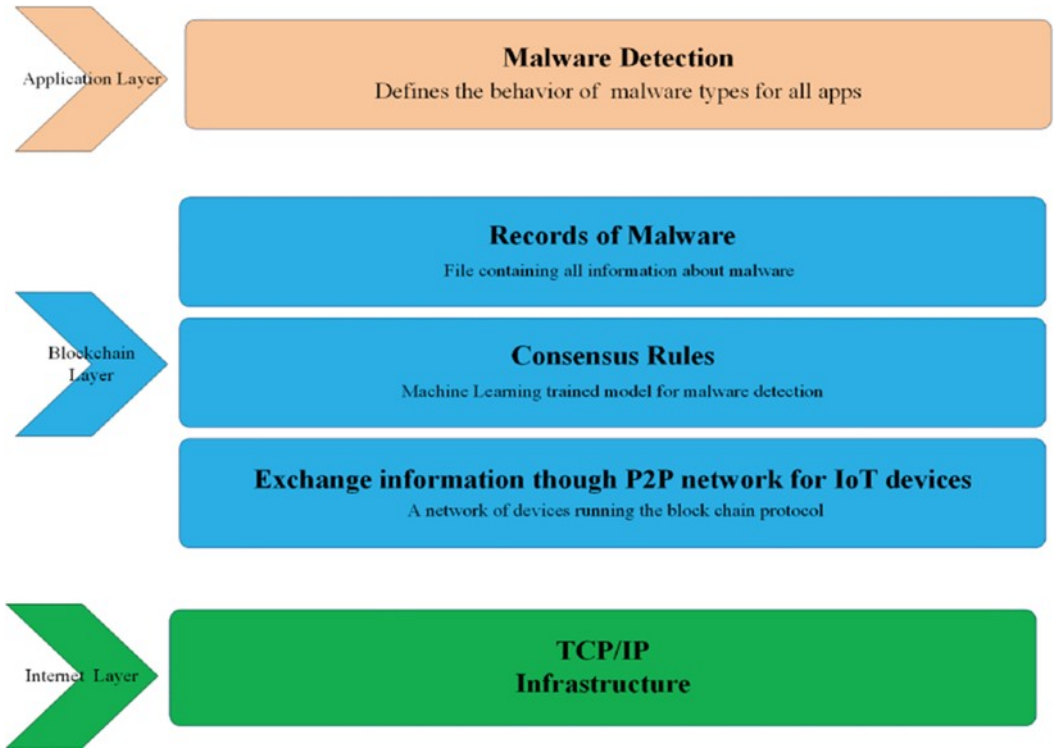

Figure 4. IoT device malware detection using block chain

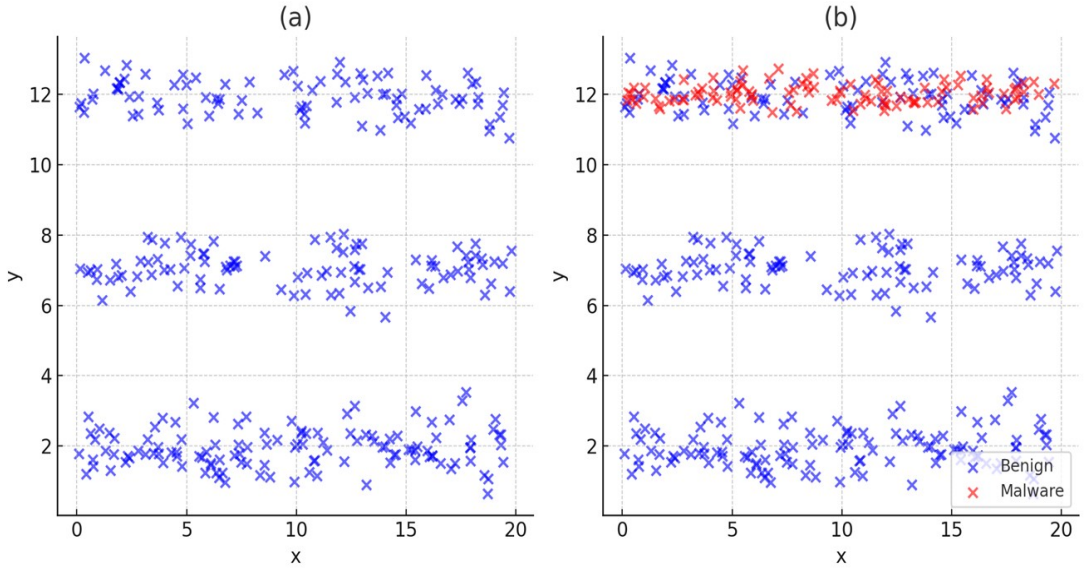

Figure 5. Grouping of malware and safe programs

Journal of Theoretical and Applied Information Technology
15th April 2025. Vol.103. No.7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

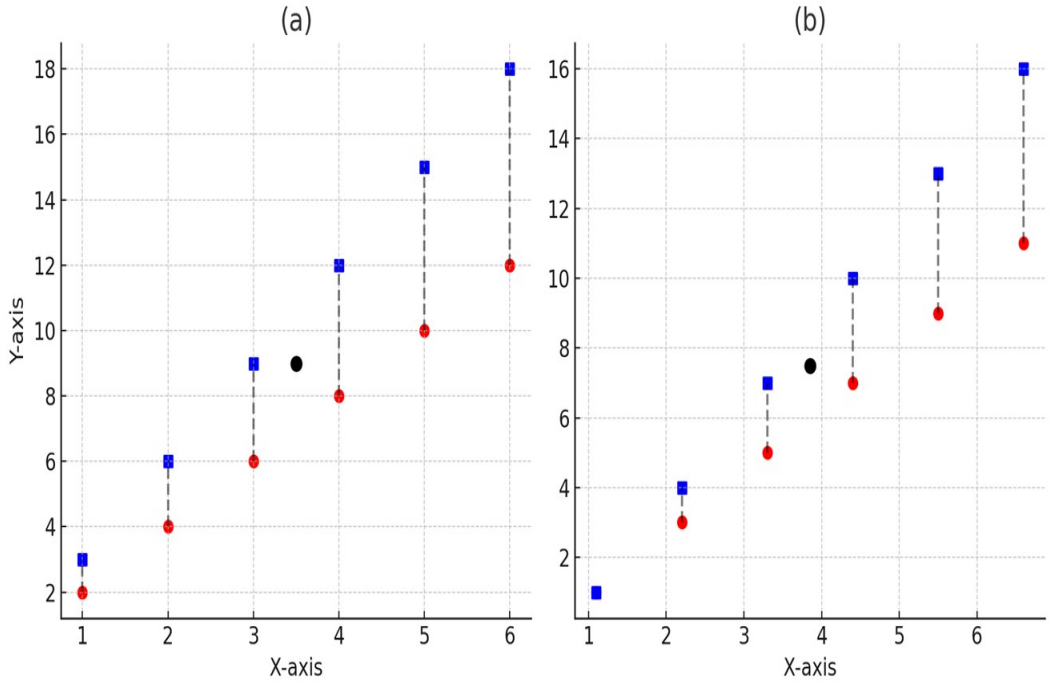

Figure 6. Effective feature analysis based on clustering (a) Widely dispersed means (b) Denotes a closer proximity

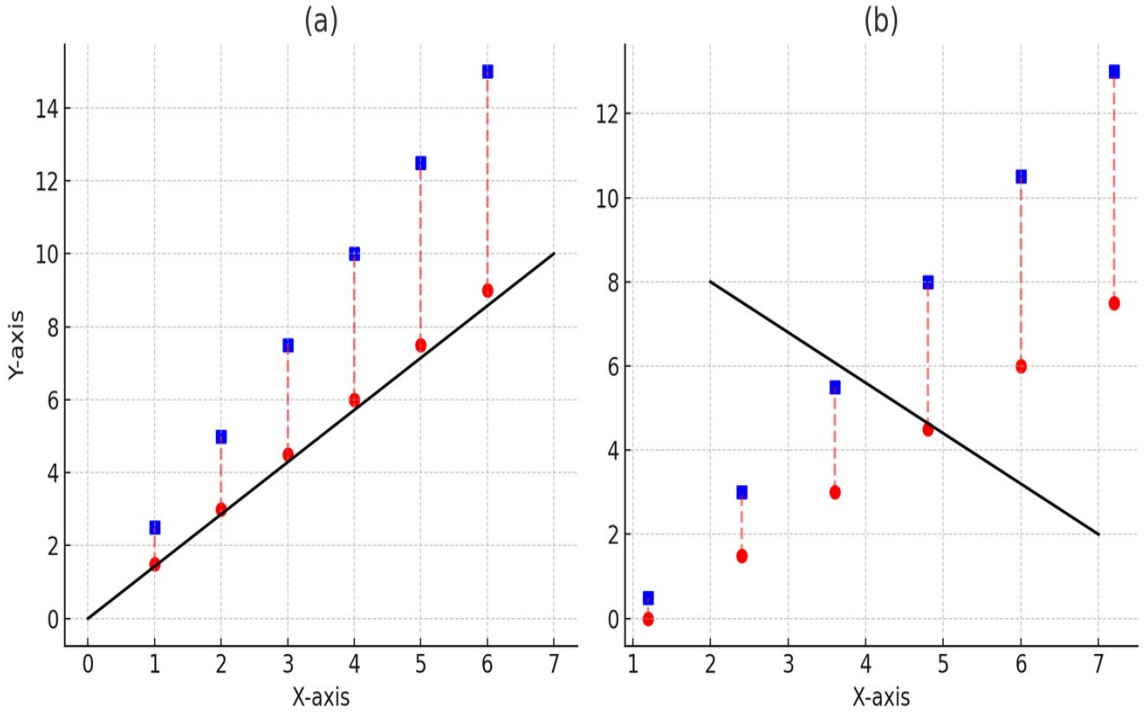

Figure 7. Analysis of projection features with efficiency (a) A forecast. (b) improved forecast

6. CONCLUSION

Devices connected to the Internet of Things are bringing about a paradigm shift in the world by enabling a variety of fascinating applications, including sensing, intelligent healthcare, remote monitoring, intelligent agriculture, and many others. Internet of Things (IoT) devices and applications that are based on the Android platform are working together to make IoT aspirations come true. Therefore, the purpose of this research effort is to provide a system that is capable of detecting malware on Android Internet of Things devices effectively. The information regarding the malware was retrieved, clustered, and classified, and then this information was also placed in the blockchain. In this way, all of the malware information that is recorded in the blockchain history may be sent over the network, and as a result, any infection that is most recent can be efficiently recognized. The proposed clustering method that we have developed calculates the weights of each feature set and iteratively reduces the elements that are not necessary. This method has the potential to be very effective in distinguishing between malware and benign programs, despite the fact that malware has many of the same characteristics as benign applications. In conclusion, the permissioned blockchain that is utilized in our framework offers genuine information that is stored in a distributed malware database. This information will help to improve the efficiency with which malware is detected during runtime.

REFERENCES:

[1] Author No.1, Author No 2 Onward, "Paper Title Here", *Proceedings of xxx Conference or Journal (ABCD)*, Institution name (Country), February 21-23, year, pp. 626-632.

[2] B.N. Singh, Bhim Singh, Ambrish Chandra, and Kamal Al-Haddad, "Digital Implementation of an Advanced Static VAR Compensator for Voltage Profile Improvement, Power Factor Correction and Balancing of Unbalanced Reactive Loads", *Electric Power Energy Research*, Vol. 54, No. 2, 2000, pp. 101-111.

[3] URL Date Stamp Time Stamp GMT and dd/mm/yyyy

[1] Allioui, H., & Mourdi, Y. (2022). Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. Sensors, 23(19), 8015. https://doi.org/10.3390/s23198015

[2] Frimpong, Bismark Atta & Barbosa, Claudia & Alhameed, Raed. (2023). The Impact of the Internet of Things (IoT) on Healthcare Delivery: A Systematic Literature Review. Journal of Techniques. 5. 84-91. 10.51173/jt. v5i3.1433.

[3] Alajlan, R., Alhumam, N., & Frikha, M. (2022). Cybersecurity for Blockchain-Based IoT Systems: A Review. Applied Sciences, 13(13), 7432. https://doi.org/10.3390/app13137432

[4] Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). IoT Vulnerabilities and Attacks: SILEX Malware Case Study. Symmetry, 15(11), 1978. https://doi.org/10.3390/sym15111978

[5] Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

[6] Chen, Guang & Xu, Bing & Lu, Manli & Chen, Nian-Shing. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments. 5. 10.1186/s40561-017-0050-x.

[7] Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., & Miranda, F. P. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. Journal of Risk and Financial Management, 16(8), 360. https://doi.org/10.3390/jrfm16080360

[8] Bakhshi, Taimur & Ghita, B.V.. (2021). Perspectives on Auditing and Regulatory Compliance in Blockchain Transactions. 10.1007/978-3-030-75107-4_2.

[9] Potter, Kaledio & Oloyede, Joy & f, olaoye. (2024). Securing the Internet of Things (IoT) Ecosystem: Challenges and Solutions in Cybersecurity. Journal on Internet of Things.

[10] Potter, Kaledio & Oloyede, Joy & f, olaoye. (2024). Securing the Internet of Things (IoT) Ecosystem: Challenges and Solutions in Cybersecurity. Journal on Internet of Things.

[11] Srivastava, Astha & Gupta, Shashank & Quamara, Megha & Chaudhary, Pooja & Aski, Vidyadhar. (2020). Future IoT-Enabled Threats and Vulnerabilities: State of the Art, Challenges and Future Prospects. International Journal of Communication Systems. 33. 10.1002/dac.4443.

[12] arshad, syed & Nasralla, Moustafa & Khattak, Sohaib & Ahmed, Taqwa & Rehman, Ikram.

(2023). Malware Analysis for IoT and Smart AI-Based Applications. 10.1007/978-3-031-34969-0_7.

[13] Perera, Srinath & Nanayakkara, Samudaya & Rodrigo, M.N.N. & Senaratne, Sepani & Weinand, Ralf. (2020). Blockchain Technology: Is it Hype or Real in the Construction Industry. 17. 100125. 10.1016/j.jii.2020.100125.

[14] Gautami Tripathi, Mohd Abdul Ahad, Gabriella Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," Decision Analytics Journal, Volume 9, 2023.

[15] Channivally, Siddhartha. (2023). Blockchain in Internet of Things (IOT) Security. 10.13140/RG.2.2.18730.59841.

[16] Alajlan, R., Alhumam, N., & Frikha, M. (2022). Cybersecurity for Blockchain-Based IoT Systems: A Review. Applied Sciences, 13(13), 7432. https://doi.org/10.3390/app13137432