International Journal of Safety and Security Engineering
Vol. 15, No. 1, January, 2025, pp. 13-20
Journal homepage: http://iieta.org/journals/ijsse

A Blockchain-Based Malware Detection Model for IoT Devices

Doaa Abdelrahman[1,2], Mohamed Rasslan[1,3*], Nashwa Abdelbaki[2]

[1] EG-Cert, National Telecommunication Regulatory Authority, Giza 12577, Egypt
[2] Center of Informatics Science, Faculty of Information Technology and Computer Science, Nile University, Giza 12588, Egypt
[3] Electronics Research Institute, Ministry of Higher Education and Scientific Research, Cairo 12622, Egypt

Corresponding Author Email: mohamed@eri.sci.eg

https://doi.org/10.18280/ijsse.150102

Received: 12 March 2024
Revised: 6 November 2024
Accepted: 6 December 2024
Available online: 31 January 2025

Keywords:
blockchain-based malware detection, malware detection for IoT, decentralized malware detection model

ABSTRACT

Malware is malicious software designed to cause destructive actions that damage information systems and networks. Malware infections have increased rapidly, and malware types have become more sophisticated, making malware detection more difficult. However, the IoT technology is vulnerable to malware attacks, since such devices have a permanent internet connection and no security. This makes it easier for the hackers to access them. These malware attacks are becoming go-to attacks on hackers. Thus, new malware detection techniques are required to address this challenge. Building a blockchain solution that allows IoT devices to download files from the Internet and verify whether they are malicious is an urgent need. The recent emergence of blockchain technology represents a solution because of its features, such as decentralization, persistence, and anonymity. Blockchain can be used instead of ordinary databases in signature-based malware detection solutions to provide decentralization and integrity. Another vital usage for blockchain networks, especially for Android devices, is that they can offer heuristic malware detection techniques for low-resource devices. Moreover, using blockchain technology overcomes some difficulties in malware detection and improves the detection ratio compared with strategies that do not utilize blockchain technology. This study examined different malware detection models based on blockchain technology. Furthermore, blockchain technology's effects on malware detection are elaborated on, particularly in an Android environment.

1. INTRODUCTION

The number of malware files is increasing annually, and malware writers use different platforms and evading techniques to bypass security systems. Thus, security researchers must continue using new methods to detect malware. Moreover, malware has become increasingly destructive. Ransomware is a perfect example of how malware infection could be damaging. When ransomware infects a computer, data encryption occurs until the ransom is paid. Wannacry ransomware infected many computers in 2017, causing extreme damage worldwide. According to Cyber Security Ventures [1], in 2021, ransomware will attack new businesses every 40 s, and every 11 s by 2022. This has created a global annual cost of $20 billion. Moreover, they estimated that by 2031, victims' losses will be approximately $265 billion because of ransomware, and a new attack will occur every two seconds. Over time, malware writers have improved their malware payloads and related force activities.

Currently, IoT devices are widely used in various businesses and industries. As is, and are perfect for data analysis. However, IoT devices can gather large amounts of sensitive data. They include chips, cameras, sensors, and many other components. Moreover, IoT devices are the least secure, as linked security recently attracted significant attention to linked security and organization security. IoT devices are not regularly fine-tested and secured from cyber-attacks. Careless behaviors, such as weak passwords or unencrypted network services, complicate this problem. Due to its low computational power, the use of advanced security solutions is not easy. Therefore, malicious software can be quickly injected into IoT devices to access valuable data. In Palo Alto Networks [2], 135,000 security cameras were scanned in March 2022. They found one vulnerability in at least 54% of the scanned cameras. Attackers can use these vulnerabilities to attack cameras and later use them to attack an organization's network. Unfortunately, according to IoT Analytics, there is a predicted increase of 9% in terms of the total number of IoT devices that will reach 27 billion by 2025. Despite the increase in IoT use, 57% of the entities included in the survey were worried about security attacks and data leaks when deploying IoT devices. Moreover, according to Gartner, 20% of organizations have detected cyberattacks on IoT devices in the past three years.

By facing cybersecurity attacks, companies can benefit from IoT opportunities; however, they undertake different vulnerabilities, constituting a portion of the newest regulatory guidance. Global government organizations understand the dangers and threats of connected devices that are not manufactured with appropriate security in mind and react to various variables in blockchain, which changes companies will be required to meet. Different organizations have started to undergo digital transformation, making IoT attacks a worrisome trend. IoT devices convert "dumb" items into "smart.” It has sensors to collect data and access the Internet to share different data types, allowing new business models and opportunities.

Within a network, transparent information sharing via blockchain technology represents an innovative database mechanism. Data are stored by blockchain in blocks linked to each other in a chain. Once the blockchain records the data, it can’t be modified or deleted, making it a trusted, unalterable, or immutable ledger for malware signatures. Moreover, blockchain adds decentralization to malware detection solutions. Besides that, IoT devices that have low resources can benefit from blockchain networks without running heuristic malware detection techniques on them directly.

In this paper, we study recent malware detection approaches, especially those that use blockchain technology to achieve a high detection rate, decrease the false positive rate, or address a lack of resources to benefit from previous approaches in providing a hybrid malware detection framework based on blockchain for IoT devices, which addresses the limitations of existing techniques. In terms of the remainder of this paper, in Section 2, different malware detection techniques are presented, and in Section 3, blockchain technology is introduced. Different malware detection approaches are discussed and compared in Section 4. The Android malware detection methods are described and compared in Section 5.

2. MALWARE DETECTION

Modern society experience a severe adverse impact from malware that affects computers and the internet. For a reduction in the resulting damage, quick detection is necessary. It is possible to categorize malware detection techniques [3] into behavior- and signature-based, as well as heuristic methods. Signature-based is the most common detection method, whereby a signature is extracted from files and stored in a database. A signature can be a byte sequence with features collected from known malware files. The signature database was then scanned to test each new file. Thus, signature-based methods can successfully detect known malware; unfortunately, they cannot detect new or unknown malware. In Behavior-based methods, a suspicious file is executed in a monitored environment to observe its behavior and determine if it is malware. Unknown malware can be detected using this method, but the problem is the high false-positive rate. Machine-learning algorithms are used in heuristic methods. Different features can be extracted using various analytical techniques. Subsequently, machine-learning algorithms are used to classify suspicious files into malicious or benign classes. Heuristic-based methods can detect unknown malware like behavioral-based methods but suffer high false-positive rates.

3. BLOCKCHAIN TECHNOLOGY

Nakamoto developed blockchain technology in 2008. It is the primary technology for various virtual currencies, including Bitcoin, and it has attracted significant attention in recent years.

A blockchain consists of sequential blocks. Every block features a transaction record list. A successive number of blocks form a public ledger. A previous block hash is contained in each block header. The initial blockchain block that lacks any parent is the Genesis block [4, 5].

The block header comprises a block version that designates the block validation rules, Merkle tree root hash, which includes all block transactions' hash values, and timestamp to record the present time in universal time from January 1, 1970; n bits that mark a valid block hash threshold; once starts by zero and increases in each hash calculation, and the parent block hash is a 256-bit hash value that points to the previous block.

The block body is comprised of transactions and a counter. Transactions and block sizes determine the maximum number of transactions in a block. The authentication of transactions is verified using an asymmetric cryptography mechanism. Each user had a pair of private and public keys. The user uses a private key to sign the transition. The signed transactions are then broadcast over the entire network. Other users use public keys to verify each transaction signature. The elliptic curve digital signature algorithm (ECDSA) is used in the digital signature, signing, and verification phases. Consensus algorithms are used to secure blockchain transactions. It is a protocol to ensure that all network nodes agree on the ledger's current state, making blockchain reliable. There are different types of consensus algorithms based on other principles. Proof of Work (PoW) is one of the oldest consensus algorithms. Many blockchain platforms use it, such as Bitcoin, Ethereum, and others. It is the most reliable and secure consensus algorithm, but its main problem is scalability. In POW, network nodes that work as miners have to prove their work to have the right to add new transactions to the ledger. Thus, miners must solve mathematical puzzles before adding every new block to the ledger. Then, the validators verify the answer before recording the new block. After that, no one can modify ledger records after every node in the network approves the block. As mentioned before, there are different consensus algorithms based on other ideas, such as Proof of Authority, Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Importance (PoI), and others.

Thus, every user who wants to transact uses their private key to sign and broadcast it into the network. Every node on the network uses the sender's public key to check new transactions by checking their UTXO to find if the transaction is valid or discard it. Each node collects several transactions to create the block if the transaction is valid. To save any block on the ledger, the POW steps start. Every miner tries to solve the mathematical challenge, and the correct and fast answer will be rewarded after validators approve the answer. Finally, the block will be recorded and can’t be modified.

Blockchain has been used in different fields other than virtual currencies because of its vital characteristics, as follows:

Decentralization: In original transaction-based systems, the central trusted entity must verify every transaction reflected in the cost and performance. Unlike a blockchain, there is no need for a third party. Blockchain consensus algorithms were used to conserve data stability in a distributed network.

Persistency: Transactions can be verified quickly. Honest miners admit only valid transactions. Once transactions are included in a blockchain, they are difficult to edit or delete.

Blocks containing invalid transactions were also revealed.

Anonymity: In a blockchain, users handle their generated addresses. Thus, their identities cannot be revealed.

Auditability: The Bitcoin blockchain records Users' balance data using the Unspent Transaction Output (UTXO) model. There is a reference for every transaction to previous unspent transactions. Moreover, the unspent time consumed changes a spent transaction once the current transaction is stored in the blockchain. Thus, every transaction can be confirmed and tracked.

Blockchain has three architectural types with different features, as shown in Table 1.

Public blockchain: A permission-less distributed ledger system in which anybody can read, send transactions, and store valid transactions in the blockchain, and anybody can contribute to the consensus process.

Private blockchain: A restrictive or permission blockchain in which a specific organization has permission to write on the blockchain, although permission to read can be restricted or public.

Consortium blockchain: More than one organization manages a blockchain network. A preselected set of nodes is used to control the consensus process. Before users join, they must ask for permission as a permissioned blockchain. Consortium blockchain shares some characteristics with both private and public blockchains.

Figure 1 shows the different blockchain architecture types used in malware detection approaches. Table 1 explains the reason for using hybrid architecture from blockchain in the majority of malware detection approaches. Using public blockchain provides complete decentralization and persistence to malware detection approaches, making blockchain more suitable for them.

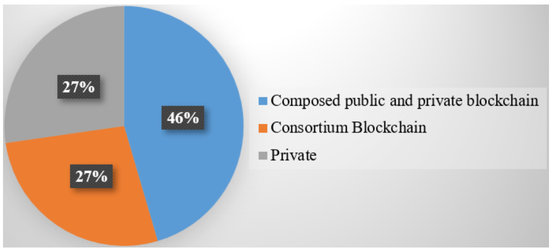

Figure 1. Blockchain architecture

4. MALWARE DETECTION USING BLOCKCHAIN TECHNOLOGY

Cyberattacks have become increasingly complex. It is becoming a customized multivector that can be performed in multiple phases. Mobile networks and IoT devices were also targeted. The attackers attempt different entry points and plugins to compromise their targets. In addition, different evasion and obfuscation techniques have been used. Anti-analysis techniques are deployed to make the malware analysis process more difficult and time-consuming. However, security researchers are trying to use innovative and different approaches to win the race with malware writers and reveal malicious indicators and abnormalities, addressing the limitations of traditional anti-antiviral techniques. In this section, we propose a study of recent malware detection approaches based on blockchain, considering different reasons to benefit from blockchain technology, such as a lack of resources, decreasing signature distribution time, improving the detection rate, and decreasing the false positive rate. A summary of different approaches can be found in Table 2.

Table 1. Blockchain types

Basis of Comparison	Public	Private	Consortium
Access	anyone has the right to read, write, and share in a consensus process	managed by a single organization, read and write is done upon invitation	managed by several organizations, read and write is done upon permission
Permission	permission-less	permissions	permissions
Speed	slow	fast	fast
Decentralization	true decentralized	centralized	balance between decentralization and control
Consensus algorithms	proof of work, proof of stake, proof of burn, proof of space etc.	Proof of Elapsed Time (PoET), Raft	proof-of-work, proof-of-stake
Energy consumption	more power and energy consuming than private	least power and energy-consuming	less power and energy than the public
Examples	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar	R3 (Banks), EWF (Energy), B3i (Insurance), Corda	R3, Hyperledger, Enterprise Ethereum Alliance (EEA), TradeLens
Cost	less expensive	more expensive	less expensive than private
Security	more secure due to decentralization	prone to hacks, risks, and data breaches	more secure than private
Data privacy	less than private	full privacy	greater data privacy than the public

Table 2. Blockchain-based malware detection approaches

Ref.	Methodology	Achievements	Limitations
[5]	Signature and behavior-based detection are used, Blockchain is used in signature sharing.	Decentralization increase signature sharing speed.	N/A
[6, 7]	Used to detect malicious PE files using signatures, heuristic, and behavior-based methods. The Ethereum blockchain platform comprises a public blockchain and a consortium blockchain.	Improved the false negative rate by about 4% and the false positive rate by about 2.5%. Improve response speed using different detection techniques.	The experiment evaluation reveals that the proposed system improves accuracy and false positives but also reveals that the system effectiveness decreases when the cover rate decreases.

[8, 9]	Used signature-based and multiple AV techniques used to detect malicious PE files. A network comprises several general-purpose computers or nodes, either low- or high-end resource types. Whenever a conveyable executable file reaches a node, it is broadcast on the network, and all active nodes begin scanning each file individually. If the file is assessed as malign or malicious, its file hash is added to the blockchain as a transaction.	Enhanced efficiency for a low-end system that can't run a heuristic-based scan due to a lack of resources. Faster response.	Scalability needs to be enhanced.
[10]	Used to detect malicious PE files, used 10,000 files for training & 4,000 files for validation, used Ethereum blockchain platform, used public blockchain, used static based detection then belief neural network (DBN) as the detection engine, used to detect malicious PE files.	Presented novel detection engine provides complete security over a variably sized network.	No insight into the behavior.
[11, 12]	Used pattern matching, behavioral and heuristic-based detection design, and implementation of a novel anti-malware environment called BitAV.	BitAV allows for the de-centralization of the update and maintenance mechanisms. The software reported that their proposed methodology was 1,400% faster in the field scanning process than in other industrial antimalware solutions network maintenance mechanism lowered the average update propagation speed by 500% and is far less susceptible to targeted denial-of-service attacks. Improve scalability and fast scanning speed with less memory usage.	The blockchain-based consensus scheme is the only one that works for unvalidatable data across an anonymous network.
[13]	Used to detect malicious Android applications using static-based detection, deep learning, and natural language processing techniques dataset collected from the applications in the APK format.	Better and accurate predictions based on blockchain reliability by ensuring data integrity detection accuracy of 95.44%.	No insight into the behavior.
[14]	Used to detect malicious Android applications. Internal blockchain is used in feature extraction. An external blockchain is used to provide feedback on different machine-learning feature algorithms to complete the task.	System error-free and more accurate.	N/A
[15]	Used to detect malware in IOT devices. The BCMPB-RIDMPL approach used five layers in malware detection (one input layer, three hidden layers, and one output layer) and used point biserial correlative features in feature-selecting malware hash verification using the Ruzicka similarity index. The dataset contains 129,013 application packages, among which 123,453 are benign application packages (.APK), and 5560 are malware and droid application packages.	Time consumption minimization by twelve percentage points. Detection accuracy improvement by eight percentage points. Results show superior performance by approach compared with state-of-the-art methods.	N/A
[16]	Used to detect malicious Android applications using static, dynamic, and hybrid-based detection using 6192 benign and 5560 malware apps collected from the Google Play and Chinese App Store. Clustering, classification, and blockchain-in-sequence (BIS) approaches were used to select and remove irrelevant features. Permission-based blockchain is used as a database to store the malware feature information.	Results show the proposed framework can achieve higher accuracy for malware detection with a low number of false-negative and false-positive rates through using a naive Bayes classifier based on a decision tree to address multi-feature problems and efficient runtime detection by using permissioned blockchain.	Inability to handle some obfuscation techniques and the feature hiding techniques when decompiling the APK using Dex2jar.
[17]	The botnet detection approach used behavior-based detection network traffic preprocessing, and cache detection optimization techniques used a permissioned blockchain dataset containing 40 million network flows.	Experiments showing that the approach can support more than 15,000 NFPS and that blockchain adds an overhead of 1,168 seconds for the considered testing scenario.	A synchronization system is needed for transactions' submission and detecting malware containment mechanism implementation.
[18]	Approach to storing and distributing cyber attack signatures securely using private-public blockchains. The Ethereum blockchain platform presented a standard format for saving and distributing signature-based IDS attack signatures. The signature owner's private key is used to sign the submit to the blockchain for verification.	The approach automatically collected attack signatures from any signature-based. Then, it was converted to a standard format compatible with other signature-based IDS. It leveraged the distributed ledger technology, data immutability, and tamper-proof abilities of blockchain technology.	Performance optimization scalability compromised node detection different transaction standard format for anomaly detection nodes.
[19]	Used to detect malicious Android applications in app stores using internal and external private blockchains. Internal private blockchain stores feature blocks external blockchain stores the detection results used static and dynamic based detection.	Framework to detect malicious android applications which used hybrid-based detection to decreases the false positive rate and blockchain to overcome the deficiency of storage space and limited computer power on the mobile platform.	N/A
[20]	Used to detect malware in IoT devices using static, dynamic, and hybrid-based detection, which used information gain functioning feature selection, and local neural networks (LNN) used intelligent contracts. It collected around 13,000 Android application packages (. APK) as regular apps from different resources and 6971 malicious applications from known sources such as the DroidKin dataset.	Detection accuracy improvement compared to three state-of-the-art models.	N/A
[21]	Used to detect and control the propagation and generation of android malware used behavior-based detection by analyzing memory logs used a dataset consisting of 100 benign software and 400 software containing malicious behaviors used Consortium Blockchain.	Used blockchain to overcome the deficiency of storage space and limited computer power on the mobile platform. Experimental results show that the framework detects and identifies malicious applications with an 89.3% detection rate.	The system has some problems like weak real-time authentication of the consortium blockchain. And the excessive memory consumption.
[22]	Used to detect malicious Android applications. The proposed fuzzy comparison method, which uses marking	Reduce the number of false positives, higher accuracy, and lower time cost compared with previous solutions.	N/A

	functions to detect the multi-feature, used a dataset of 4486 malware samples and 2140 benign software samples collected from real scenarios. public blockchain shared by users, consortium blockchain shared by the test members.	

4.1 Malware detection approaches for windows

Traditional antiviral software detects malicious files primarily based on a signature database. Thus, if the suspicious file has a signature in the signature database, it is removed; however, no action is taken if the signature does not exist. Lately, if a suspicious file is declared new malware, it is sent to the lab for further analysis and to extract a suitable signature. During this process, many users execute the file.

Pichikala et al. [6] proposed a new malware detection framework that benefits from blockchain technology's distributed and decentralized features in a quick-update signature database with new suspicious file signatures. Thus, every node in the network will decide whether a suspicious file exhibits malicious behavior.

Fuji et al. [7] proposed a blockchain-based malware-detection method. The proposed method depends on sharing malicious file signatures among users to achieve a rapid response. Malware detection accuracy is improved by using blockchain in signature utilization. After Fuji et al. [8] performed an accurate simulation to measure the accuracy improvements, the false-negative and false-positive rates decreased. A blockchain network consists of users who wish to detect and share malware files. They assumed that each user uses a heuristic or behavior-based malware detection scheme that employs different detection methods. The users had the proposed signature-based detection system, and the shared signatures were stored in the blockchain. Every time a user uses a file, their detection system will judge it suspicious and send it to the blockchain. Subsequently, any other user using the same file will check if the signature exists, judge it again using his detection scheme, and send his vote to the blockchain. Finally, the user-detection system blocks the file based on the voting results.

Gupta et al. [9] proposed a malware detection framework to classify PE executable files into malware and benign. The proposed malware detection module uses both multi-antivirus-based and signature-based detection methods. The framework is based on blockchain. If a tested PE file is classified as malware, its hash is recorded on the blockchain. Every machine in the network is called a node or an installed detection engine based on its resources. When a new file accesses the machine, it calculates the hash of the file and scans the signature database. If a file is found in the database, the node makes a threat alert, broadcasts the file to each node, and quarantines. If a file hash is not found in the signature database, each node in the network receives the file and scans it using a different detection engine. Finally, the scanning result is sent by every node to the first node, and the file signature is recorded on the blockchain. The main advantage of the proposed engine is that it enhances the efficiency of the low-end system, which cannot use the heuristic detection method because it requires a large amount of resources.

Gupta et al. [10] designed and developed a decentralized and distributed database-oriented intrusion detection framework powered by three malware detection frameworks: behavior-, multi-antivirus-, and signature-based. The detection system is reliant on Blockchain Technology with the aim of classifying as benign or malignant the transferred executable files. A network comprises several general-purpose low- or high-end resource type computers or nodes. A conveyable executable file is broadcast on the network when it arrives at a node. Then, each file is individually scanned by all active nodes. Where the file receives a malicious or malign assessment, its file hash is included in the blockchain as a transaction, alongside its malicious likelihood. Next, the client or node broadcasting the file can pass through the entire chain so the final outcomes can be obtained, namely, that file hash's weighted probabilities average. Therefore, the multi-malware detection engine proposed merely employs low-end resources with the tendency for superior and more accurate results in malware detection and quarantine while negating the requirement for high-end resources that are both expensive and specialized.

Raje et al. [11] designed and developed a decentralized firewall system based on a malware-detection engine. A firewall was implemented using blockchain technology. The framework target is Portable Executable (PE) file classification as malicious or benign. Malware detection is based on a deep belief neural network (DBN). Portable Executable (PE) files were converted into grayscale images, and the DBN was used to classify the images. They used a dataset containing 10,000 files for DBN training. A proof-of-work-based consensus was used to decide whether to allow or block a file in the blockchain network.

Noyes [12] presented BitAV, a malware detection framework. A pattern-matching scheme was used in this study. To generate a structure facilitating constant-time key-value queries while excluding the high likelihood of false positives characterstic of probabilistic data stores, the scanning method used a Bloom filter as well as one of its derivative data structures. Blockchain technology creates a decentralized network for users to share information such as unique characteristics. The authors reported that their proposed methodology was 1,400% faster in field scanning than in other industrial antimalware solutions. In addition, their experiments achieved improvements in the end-to-end scanning speed.

5. ANDROID MALWARE DETECTION TECHNIQUES

Android is a modified version of the Linux operating system developed by Google. The device was designed for use in touchscreen smartphones. According to the Statista Research Department [13], in 2019 87% of the global market used Android operating system-based mobile devices, with this proportion estimated to increase in subsequent years, while the Apple (iOS) mobile operating system held the remaining market share segment of 13%. Simultaneously, Android operating systems are open-source and encourage attackers to write malicious software on the Android platform. By contrast, IOS security has stern rights supervision of the system, which gives it a high level of protection. On the other hand, Android users use different application markets to install various applications because of the lack of Google Store, which leaves them in great danger of malicious software and Trojan horses.

Typically, malicious applications are Android malware. It can be downloaded from a Play Store or other third-party store. Android malware has different and severe activities on victim mobile devices, such as information leakage, system damage, and financial losses to users. Thus, there is a significant need for anti-malicious software to protect the Android system, which must consider mobile devices' lack of resources, such as storage and power. Owing to resource problems, blockchain technology has been used in recent malware detection approaches for Android operating systems, as shown in Figure 2. Smartphone malware's intense growth indicates malware developers' shift to mobile devices from traditional desktop systems. Hence, security researchers must switch to and propose new anti-malware mechanisms to achieve the required protection.

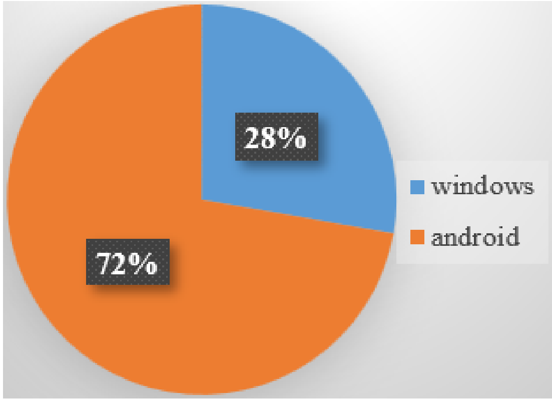

Figure 2. Targeted operating systems

5.1 Malicious Android applications detection using blockchain

In the context of attaining greater concrete predictions, Gupta et al. [14] presented a consensus-based blockchain framework, since blockchains are low-cost and highly reliable. When a Random Forest classifier was used, the proposed model was demonstrated by the experimental results to provide a 95.44% detection accuracy, achieved via the top 45 Information Value-ranked permissions.

For the identification of users and distinguishing permissions that could detect Android malware efficiently, the permissions were ranked via the weight of evidence and information value. After that, each application's obtained permissions were converted into sentences through their concatenation and separation based on the space. The above sentences had TF-IDF applied for their convention into numeric values. To obtain numeric values, machine learning algorithms were employed, namely, Extremely Randomized Trees, Naive Bayes, and Random Forest. A deep learning architecture was also applied through word embedding and an LSTMS to numeric permissions. Finally, the development of a consensus-based blockchain architecture facilitated superior predictions of greater accuracy in terms of the aforementioned problem.

Aneja et al. [15] proposed a blockchain-based system for detecting Android malware applications. Machine learning was used in the proposed malware detection system. They used two types of blockchain networks: an internal blockchain used in feature extraction and an external blockchain used to provide feedback on different machine-learning feature algorithms to complete the task. They used different internal blockchains for each application to improve the detection ratio and decrease the false positive rate.

Alotaibi [16] introduced a new malware detection method called the biserial correlative Miyaguchi–Preneel. It is a Ruzicka-index deep multilayer perceptive learning (BCMPB-RIDMPL) algorithm based on blockchain. The present research aims to improve malware detection accuracy and minimize time consumption. One input layer, three hidden layers, and one output layer are included in the BCMPB-RIDMPL technique. The input layer receives malware features. The malware features are then referred to as the first hidden layer to perform feature selection using a point biserial correlation. The authors found that this step reduces the time required for malware detection. Subsequently, the second hidden layer received the selected features and applications. This layer generates a blockchain hash based on every selected feature using Miyaguchi–Preneel. The generated hash values are then recorded in the blockchain. In the third hidden layer, classification was performed. The Ruzicka index is used to confirm the training and testing of malware feature hash values. The application was classified as malicious if the hash was present; otherwise, it was classified as benign. Compared with state-of-the-art methods, the authors improved malware detection accuracy, Matthews' correlation coefficient, and required time for malware detection.

Kumar et al. [17] presented a new framework to benefit from blockchain technology and machine learning methodology to detect Android malware in IoT devices. The proposed method uses a clustering, classification, and blockchain-in-sequence (BIS) approach. First, classification is used to classify the target file as benign or malware. They calculated each feature set weight to improve clustering by making feature selections and removing irrelevant features. They then used a naive Bayes classification algorithm in the second phase of malware classification. Finally, a permission-based blockchain is used as a database to store the malware feature information. Thus, new blocks were generated to identify new IoT malware, which improved the runtime malware detection efficiency.

Lekssays et al. [18] provided a dynamic framework for botnet detection. Botnets are used as DDoS attacks for different attacks against IoT devices. A botnet is a set of victim machines compromised and controlled by an attacker using Command and Control (C&C) servers. The authors proposed AutoBotCatcher, based on a blockchain, to detect botnets. They used several optimization methods, such as caching detection output and preprocessing of shared network traffic. Moreover, various privacy-preserving methods protect machines from botnet detection and reidentification. The experimental results indicated a high detection ratio.

In reference [19], an architecture was proposed for the real-time secure storage and distribution of such attack signatures to ensure detection in a prompt manner. The architecture proposed leverages blockchain technology's data immutability, distributed ledger technology, and tamper-proof nature. The examination of the proposed system's performance employed the blockchain network's latency. In the detection of cooperative intrusion, attack signatures are exchanged by IDS nodes to enable the detection of any attack promptly detected by other IDS. Thus, a significant problem is the security of the database housing these shared attack signatures. It is essential to detect and prevent malicious signature deletion, injection, or manipulation.

In reference [20], a Blockchain-Based Malware Detection Framework (B2MDF) was proposed by Homayoun et al. for the detection in mobile application (app) marketplaces (stores) of malicious applications. The B2MDF featured two private blockchains of an internal and external nature, thus representing a dual consortium/private blockchain to achieve the ultimate decision. Blocks attained by dynamic and static feature extractors are stored by the internal private blockchain, whereas the detection results are stored as blocks for current application versions by the external blockchain. Moreover, third parties receive feature blocks shared by B2MDF, thus assisting antimalware vendors in the provision of solutions with greater accuracy.

Kumar et al. [21] presented different malware detection methods. It is based on the blockchain. This framework uses a local neural network (LNN) for classification. They use smart contracts to ensure their authenticity. They used static and dynamic malware analysis to extract the features and then selected features using the information gain function. Malicious applications are verified by the smart contract for both download and upload network processes via the local models' stored aggregated features. The authors achieved improvements in malware detection accuracy besides model efficacy with blockchain in comparison to three state-of-the-art models.

Du et al. [22] proposed a new consortium blockchain-based framework for innovatively detecting and controlling malware generation and propagation. Considering a range of factors, including the mobile platform's limited computing power and storage space, the mobile platform is not directly joined to the blockchain. Rather, a detection and reporting framework is utilized according to the log analysis of malicious behavior searches on mobile phones. The daemon process then resides in the memory. The system log information is recorded, with the Aho-Corasick automata algorithm used for matching log information potentially exhibiting behavior of a malicious nature, while identifying and reporting the application's malicious behavior. Based on the experimental results, the approach is able to carry out the detection, identification, and control of Android platform-based malicious applications.

Gu et al. [23] developed a malware-detection framework. The proposed framework is based on blockchain. It consists of two Blockchain networks. Users shared the public network, and the test members shared the consortium network. They used a fuzzy comparison method to create an equivalent to a multi-featured model and multiple-making functions to reduce the number of false positives. They extracted features from different malware files, such as software packages, blockchain networks, permissions and applications, and function call features. A malicious code fact base is used in blockchain technology.

5.2 Using blockchain in defensive description

A different approach was taken by Badih et al. [24], who built upon their previous work in reference [25], which was initially used for malware detection and later redirected to a decoy driver to capture specific data. They demonstrated that combining access control with defensive deception is more effective than other methods, as malware operates within deception mechanisms while attempting to bypass access control. Their approach enabled the detection of secondary webcam spyware more effectively than ever before by analyzing behavior.

They proposed integrating defensive deception methods into a chain of interactions that directs decoy I/O device usage with decoy servers. In their proposed paper, they utilized a smart contract as a decoy along with a decoy key management server. Their framework incorporates blockchain concepts, such as smart contracts and key management approaches, to evade malware while simultaneously leveraging its detection.

6. CONCLUSIONS

Blockchain is a promising technology that serves various research fields. It has essential features like decentralization, persistence, anonymity, and audibility. The malware detection field requires new technologies to help researchers prevent malware from spreading. Blockchain technology offers solutions that eliminate the spreading of malware by using different techniques, platforms, and networks to evade security devices. This paper presents a study of various approaches to using blockchain in malware detection. Moreover, we classified different attempts based on targeted operating systems. The limitation was that some studies did not mention detailed architecture. Our future work will be to provide a hybrid malware detection framework for IoT devices. It will be based on the Consortium blockchain to benefit from previous studies.

FUNDING

This work is supported by the National Telecom Regulatory Authority (NTRA).

REFERENCES

[1] Ransomware Statistics in 2024: From Random Barrages to Targeted Hits. https://dataprot.net/statistics/ransomware-statistics/.

[2] The Connected Enterprise: IoT Security Report 2020. https://www.paloaltonetworks.com/resources/research/connected-enterprise-iot-security-report-2020.

[3] Mehta, G., Das, P., Tripathi, V. (2022). Challenges in malware detection and effecting areas: Survey. In Advances in Information Communication Technology and Computing: Proceedings of AICTC 2021, pp. 89-97. https://doi.org/10.1007/978-981-19-0619-0_9

[4] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, pp. 557-564. https://doi.org/10.1109/BigDataCongress.2017.85

[5] Sarmah, S.S. (2018). Understanding blockchain technology. Computer Science and Engineering, 8(2): 23-29. https://doi.org/10.5923/j.computer.20180802.02

[6] Pichikala, S.M., Rachana, G., Sanjanapatel, H., Shanu, S., Vineeth, N. (2021). Malware detection using blockchain technology. In 2021 2nd International Conference for Emerging Technology (INCET), Belagavi, India, pp. 1-4. https://doi.org/10.1109/INCET51464.2021.9456161

[7] Fuji, R., Usuzaki, S., Aburada, K., Yamaba, H., Katayama, T., Park, M., Shiratori, N., Okazaki, N. (2019). Investigation on sharing signatures of suspected malware files using blockchain technology. In

International Multi Conference of Engineers and Computer Scientists (IMECS), Hong Kong, pp. 94-99.

[8] Fuji, R., Usuzaki, S., Aburada, K., Yamaba, H., Katayama, T., Park, M., Shiratori, N., Okazaki, N. (2020). Blockchain-based malware detection method using shared signatures of suspected malware files. In Advances in Networked-based Information Systems: The 22nd International Conference on Network-Based Information Systems (NBiS-2019), Oita, Japan, pp. 305-316. https://doi.org/10.1007/978-3-030-29029-0_28

[9] Gupta, S., Thakur, P., Biswas, K., Kumar, S., Singh, A.P. (2021). Toward a novel decentralized multi-malware detection engine based on blockchain technology. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, pp. 811-819. https://doi.org/10.1007/978-981-33-4367-2_77

[10] Gupta, S., Thakur, P., Biswas, K., Kumar, S., Singh, A.P. (2021). Developing a blockchain-based and distributed database-oriented multi-malware detection engine. In Machine Intelligence and Big Data Analytics for Cybersecurity Applications, pp. 249-275. https://doi.org/10.1007/978-3-030-57024-8_11

[11] Raje, S., Vaderia, S., Wilson, N., Panigrahi, R. (2017). Decentralised firewall for malware detection. In 2017 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, pp. 1-5. https://doi.org/10.1109/ICAC3.2017.8318755

[12] Noyes, C. (2016). Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. arXiv preprint arXiv:1601.01405. https://doi.org/10.48550/arXiv.1601.01405

[13] Share of global smartphone shipments by operating system from 2014 to 2023. https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/.

[14] Gupta, S., Sethi, S., Chaudhary, S., Arora, A. (2021). Blockchain based detection of android malware using ranked permissions. International Journal of Engineering and Advanced Technology, 10(5): 68-75. https://doi.org/10.35940/ijeat.E2593.0610521

[15] Aneja, N., Suri, S., Papneja, S., Khurana, N. (2021). Malware mobile application detection using blockchain and machine learning. In 2021 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, pp. 1-7. https://doi.org/10.1109/GCAT52182.2021.9587880

[16] Alotaibi, A.S. (2021). Biserial Miyaguchi–Preneel blockchain-based Ruzicka-indexed deep perceptive learning for malware detection in IoMT. Sensors, 21(21): 7119. https://doi.org/10.3390/s21217119

[17] Kumar, R., Wang, W., Kumar, J., Yang, T., Ali, W. (2021). Collective intelligence: Decentralized learning for Android malware detection in IoT with blockchain. arXiv preprint arXiv:2102.13376. https://doi.org/10.48550/arXiv.2102.13376

[18] Lekssays, A., Landa, L., Carminati, B., Ferrari, E. (2021). PAutoBotCatcher: A blockchain-based privacy-preserving botnet detector for Internet of Things. Computer Networks, 200: 108512. https://doi.org/10.1016/j.comnet.2021.108512

[19] Ajayi, O., Cherian, M., Saadawi, T. (2019). Secured cyber-attack signatures distribution using blockchain technology. In 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, pp. 482-488. https://doi.org/10.1109/CSE/EUC.2019.00095

[20] Homayoun, S., Dehghantanha, A., Parizi, R.M., Choo, K.K.R. (2019). A blockchain-based framework for detecting malicious mobile applications in app stores. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, pp. 1-4. https://doi.org/10.1109/CCECE.2019.8861782

[21] Kumar, R., Zhang, X., Wang, W., Khan, R.U., Kumar, J., Sharif, A. (2019). A multimodal malware detection technique for Android IoT devices using various features. IEEE Access, 7: 64411-64430. https://doi.org/10.1109/ACCESS.2019.2916886

[22] Du, Y., Liu, C., Su, Z. (2019). Detection and suppression of malware based on consortium blockchain. IOP Conference Series: Materials Science and Engineering, 490(4): 042031. https://doi.org/10.1088/1757-899X/490/4/042031

[23] Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., Wang, Z. (2018). Consortium blockchain-based malware detection in mobile devices. IEEE Access, 6: 12118-12128. https://doi.org/10.1109/ACCESS.2018.2805783

[24] Badih, H., Alagrash, Y., Rrushi, J. (2020). A blockchain and defensive deception co-design for webcam spyware detection. In DASC/PiCom/CBDCom/CyberSciTech, Calgary, AB, Canada, pp. 593-600. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00104

[25] Badih, H., Bond, B., Rrushi, J. (2020). On second-order detection of webcam spyware. In 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, pp. 424-431. https://doi.org/10.1109/ICICT50521.2020.00074