Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

A DECENTRALIZED BLOCKCHAIN FRAMEWORK FOR MALWARE DETECTION IN IoT NETWORKS

[1]Subbaiahgari R Ajitha and [2]Dr G V Ramesh Babu
[1]Research Scholar, SVU College of CM & CS, Sri Venkateswara University, Tirupati
[2]Associate Professor, SVU College of CM & CS, Sri Venkateswara University, Tirupati

Abstract:

The rapid deployment of interconnected IoT infrastructures has introduced significant cybersecurity challenges across distributed environments. As IoT networks are resource constrained and heterogeneous in architecture, conventional approaches to detecting malware are usually not efficient, scalable, and reliable. In order to overcome these limitations, in this research, an IoT security model, based on distributed ledger technology is incorporated for efficient detection and classification of malware. The goal of block chain and IoT integration is to improve authenticated communication and tamper-resistant threat management in the IoT environment. The immutable distributed validation mechanism of Block chain are advantageous for transaction data dealing with the IoT, decreasing the danger of data manipulation and unauthorized access. This study concentrates on designing a intelligent real-time threat analysis framework with block chain-based consensus mechanism for data authenticity and integrity. This process minimizes classification errors and improves prediction reliability and increases detection accuracy and reliability. Additionally, automated smart contract mechanisms are integrated to facilitate automated enforcement of the security policies, and to quickly respond to malicious actions within the network. The proposed framework contributes to the overall resilience, scalability, and efficiency of IoT ecosystems and offers a common and authenticated data exchange platform. The results of this research help reinforce the cybersecurity solutions for different applications based on the Internet of Things, such as precision agriculture, intelligent healthcare systems, and Industry 4.0 environments, and smart city infrastructures, among others, in order to satisfy the need for proactive solutions to counteract new cyber threats.

Keywords: Internet of Things, Blockchain, Malware Detection, IoT Security, Machine Learning, Smart Contracts, Cybersecurity.

1. INTRODUCTION

IoT technology has transformed modern digital ecosystems through autonomous device connectivity and continuous information exchange by facilitating dynamic communication among distributed edge nodes, sensors, and network-enabled intelligent infrastructures. The internet of things is a network of intelligent devices, including wearable sensing devices and intelligent consumer appliances, home automation and smart home systems, industrial equipment and environmental monitoring sensors. The devices are connected to each other, generating continuous streams of heterogeneous operational data, which leads to improved automation, efficiency, and intelligent decision-making in fields such as healthcare, transportation, manufacturing, agriculture, and smart city infrastructure, among others [1].

The widespread acceptance of the IoT technologies has brought a new dimension of productivity and service quality with its ability to monitor processes in real-time, perform predictive analytics and even control processes automatically. For instance, in the healthcare sector, IoT systems can enable real-time monitoring of patients from a distance and early detection of issues, while in the transportation industry, smart traffic management systems can use real-time data to optimize traffic flow and lower energy costs. Nevertheless, the rapid proliferation of the Interconnected edge nodes has raised serious cyber security issues because of the distributed, heterogeneous and resource limited characteristics of IoT environments [2].

A lot of Interconnected edge nodes have limited computing power, memory and security infrastructure, which makes them very susceptible to cyber attacks and hacking. Besides, users of these devices in different networks are using different devices and it makes implementation of uniform security standards and effective threat management strategy more complicated [3]. With the IoT landscape growing, attacks on connected devices are becoming more complex and more

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

damaging. Some common threats are weak authentication attacks, firmware hacking, malicious intrusion, botnet attack, ransomware, distributed denial-of-service (DDoS) and supply chain attacks. The attacks can be very devastating, causing data breaches, compromising privacy, causing disruption in critical infrastructure, losing finances, and, of course, threatening the safety of human beings [4]. Therefore, robust, scalable and intelligent security solutions for IoT networks has emerged as a critical research area to ensure secure and reliable communications in an increasingly connected digital world.

1.1 SIGNIFICANCE OF RELIABLE MALWARE DETECTION FRAMEWORKS

The security concerns have made it essential to have effective and efficient malware detection and classification mechanisms. Traditional security systems such as signature-based anti-virus and conventional intrusion detection systems (IDS) may not be enough to detect advanced persistent threats (APTs) in IoT networks or zero-day attacks, or polymorphic malware. Further, the IoT devices' computational power, memory, and energy are limited, and the security frameworks must be lightweight and resource-efficient to be able to perform real-time threat analysis with minimal overhead [5].

Block chain technology was initially developed to be used in Bitcoin, but has recently been introduced into other realms, especially cybersecurity and IoT security applications. Block chain is a distributed and decentralized ledger technology, in which transactions are securely recorded between different nodes without the need for any central authority. In every block in the block chain is a cryptographic hash of the preceding block, creating an unalterable chain that ensures that data on the block chain cannot be altered or tampered with by unauthorized parties. Block chain's features make it an appealing approach to this challenge of improving the security, transparency and reliability of IoT communication systems [6]. Block chain technology can greatly mitigate the risks of unauthorized access, data manipulation, and cyberattacks in distributed IoT settings, freeing up resources for businesses to operate more effectively. Here are some key benefits of incorporating block chain technology into the IoT security paradigm.

One of the benefits is that data is immutable, which means that once it's in to the block chain ledger, it cannot be modified or erased without a consent of the networks. This is beneficial for data integrity, traceability, and auditability in IoT systems. Distributed trust management is also interesting, since it makes the network more resilient to malicious attacks and failures, by distributing the responsibility of validation over several nodes participating in the network. Furthermore, smart contracts can be utilized to automatically execute and enforce pre-designed security policies and operational rules in a clear and tamper-evident way. Furthermore, block chain provides solutions for identity management especially for Interconnected edge nodes and users, which means that only authorized devices and users are allowed to access the network and share data; all data is trusted and verifiable [7].

Furthermore, the distributed ledger framework can ensure transparency and accountability as it maintains a record of transactions with auditable records and enable the secure tracking of IoT operations, thus helping to ensure regulatory compliance. In critical infrastructure and industrial settings, where the traceability feature of block chain can help establish the origin, ownership, and operational history of Interconnected edge nodes is valuable. In this research, a new malware detection and classification mechanism based on block chain in IoT network is presented. The proposed solution utilizes block chain technology, which is decentralized, transparent and immutable, and intelligent machine learning techniques, which will enable the provision of a strong real-time detection system for malware. The proposed model overcomes this issue by utilizing block chain-based security mechanisms to enhance the security of IoT systems and protect critical data and infrastructure from new threats in IoT deployments, ensuring reliability, scalability, and resilience [8].

SECURITY THREATS CAUSED BY MALWARE IN IOT NETWORKS

Today, the Internet of Things (IoT) has expanded and is now supporting the deployment of smart devices in many applications and industries, which are interconnected with each other. The increasing complexity and interconnectedness of

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

IoT networks are also facing many new forms of malware and cyber attacks that can pose serious threats to the security, privacy and reliability of connected devices. IOE vulnerabilities are often used to allow malicious actors to compromise the devices, cause them to malfunction, steal sensitive data, and trigger a massive attack on critical infrastructure. Many Interconnected edge nodesare vulnerable to advanced attacks because of their heterogeneous architecture, limited computational capabilities and weak built-in security mechanisms. Thus, it is crucial to have an understanding of the various kinds of malwares affecting the IoT environment as well as the security issues and weaknesses of available traditional protection approaches to be able to build efficient and intelligent cyber security solutions that can protect modern IoT systems [9].

2.1 TYPES OF MALWARE TARGETING IOT DEVICES

Botnets: A botnet is a collection of attacked computers, also known as “zombie computers” that are controlled from a central Command and Control (C&C) server run by attackers. Botnets are used by cybercriminals for coordinated attacks, including distributed denial-of-service (DDoS), sending spam, stealing credentials, and cryptocurrency mining. Many Interconnected edge nodes have weak security configurations, default credentials, and are always connected to the internet, which makes them easy to recruit into botnets. The massive volume and variety of Interconnected edge nodes mean attackers have a vast attack surface to use for launching large-scale cyberattacks and wreaking havoc on network operations.

Ransomware: Ransomware refers to a type of malware that encrypts data, blocks access to devices, or interferes with the operation of the system until a ransom is paid. Over the last few years, ransomware attacks have focused on Interconnected edge nodes, such as network-attached storage (NAS) devices, surveillance cameras, healthcare devices and smart home appliances. Such attacks can cause financial damage, compromise data security, disrupt operations, and impact system reliability. Smartphones, smart meters, smart cameras, and smart speakers are just some of the things that are becoming part of everyday life. Smartphones, smart meters, smart cameras, smart speakers – these are just a few examples of the increasing number of devices that are becoming part of every day life.

Spyware: Spyware is software designed to spy or secretly monitor user activity and record sensitive information without the user's knowledge or permission. Spyware can be used to breach user privacy in an IoT system by gaining access to audio, video, location data, browsing habits, and sensitive operational information from devices connected to it, like smart home systems, wearable devices, and industrial sensors. The information gathered can be used for any unauthorized surveillance, identity theft, espionage, and so on. With the amount of information generated by IoT devices, spyware is a serious threat to personal privacy and organizational security.

Malware is a type of software that is intentionally created with the intent of wreaking havoc on systems, infiltrating systems without authorization, stealing sensitive information, or harming digital systems, according to cybersecurity researchers. There are several types of malware, such as Trojan horse, virus, worm, ransomware, spyware, and botnets, which can cause different types of threats for IoT network and connected environment.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Figure 1 shows the key types of malware typically seen in IoT environments.

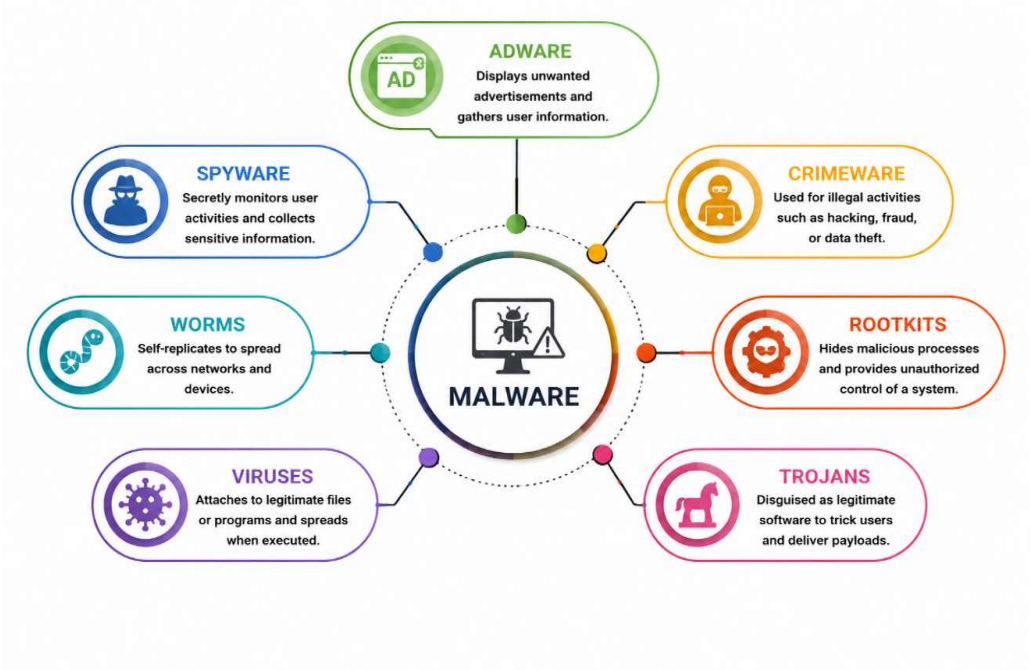

Figure 1. Classification of Malware Types

2.2 MALWARE CHALLENGES IN IOT ENVIRONMENTS

Scale and Heterogeneity: IoT ecosystems are made up of an enormous network of device-to-device interactions that communicate with different communication standards, operating systems and hardware platforms as well as different network protocols. This diversity presents a huge challenge to the implementation of a uniform security mechanism throughout the entire IoT infrastructure. Each device could have different vulnerabilities, security features, and restrictions, making for extensive protection. Moreover, when implementing large-scale IoT deployments with millions of IoT devices, there is a tremendous amount of data and network traffic to be monitored, detected and managed for threats. In addition, there is a massive amount of data generated and network traffic in large deployments with millions of Interconnected edge nodes, making threat monitoring, malware detection and security management more complex.

Resource Constraints: Most Interconnected edge nodes have limited computational resources such as low computing power, less memory, and short battery life. Conventional security technologies like intrusion detection systems and antivirus software are costly to run and typically require significant computing resources and power, which are not available in resource-limited IoT devices. Overly complex security processing can make devices slow, consume power, and decrease the efficiency of running them. Thus, lightweight and efficient malware detection mechanisms are crucial to ensure effective protection without compromising the functionality and usability of the Interconnected edge nodes[11].

Security by design: Most of the Interconnected edge nodes are designed primarily for connectivity and functionality with little implementation of security. This implies some of these gadgets lack some security features such as secure boot mechanisms, firmware validation, encrypted communication, and secure over-the-air (OTA) update choices. The lack of awareness among users, insufficient authentication techniques, outdated firmware, and poor security design give attackers the chance to take advantage of a vulnerability and gain access into an IoT system. It is easy for malicious code to penetrate the IoT environment, gain access, and the opportunity for a cyber attack on a large scale.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

However, there are some drawbacks to Signature Based Detection: Traditional methods for detecting malware, such as signature-based antivirus programs, use existing signatures and patterns of malicious intrusions to detect malicious actions. These techniques work well against known threats, but do not provide protection against new variants of malware, polymorphic attacks, or zero-day exploits, which are constantly changing and exploiting known techniques. The evolving and volatile nature of the threat in IoT makes it necessary to have a smart and adaptive security solution that can detect unknown and new attacks in real time.

Centralized Security Architectures: Under traditional security architecture, monitoring, analysis and decision making functions are usually carried out by a single point server or control centre. Centralized security models, however, also come with the risk of having a single point of failure, and an increased exposure to targeted cyberattacks. Centralized architectures can also experience scalability challenges, delays, and bottlenecks in large-scale IoT deployments. Distributed and decentralized security strategies can help to enhance the resilience of systems by spreading security responsibilities among various nodes and devices, which helps to minimize the impact of any single component failing and increases the reliability of the network.

Manual Security Management: In large deployments of IoT, traditional security management methods can include manual patching and updating, manual configuration, monitoring, and maintenance, all of which can be difficult, time consuming and prone to errors. It can be difficult to manage the devices in remote areas and out of reach, resulting in slow updates, misconfigurations and undetected vulnerabilities. By leveraging machine learning, AI, and orchestration technologies, automated security solutions can be more effective in IoT environments, enabling easier threat detection, quicker reaction to security incidents, and efficient security operations management. As it can be seen from the above mentioned challenges and limitations there is a great need for advanced Malware Detection & Classification framework for IoT environments. Block chain can be a solution to address security issues and malicious activities in the IoT ecosystem, as discussed in this research. The proposed framework integrates the decentralized, transparent and immutable nature of the block chain technology along with intelligent algorithms, which would utilize machine learning techniques for secure, scalable and real-time detection, classification and mitigation of malicious entities on IoT networks. The proposed approach is designed to overcome the drawbacks of the existing security mechanisms and also enhance the resilience, reliability and trustworthiness of IoT systems to the new cyber attacks [12].

3. ROLE OF BLOCKCHAIN IN IOT SECURITY

Block chain is a new and powerful technology, originally created for cryptocurrencies, such as the Bitcoin, but with many uses outside the realm of money. Block chain's decentralized, transparent and tamper-proof capabilities have created a huge amount of interest in cybersecurity for enhanced data security, transaction reliability and digital trust management. Block chain technology represents secure solutions to guarantee data integrity, secure digital transactions and better identity and access management in distributed settings. The use of block chain tech with the Internet of Things (IoT) networks has been introduced in recent years to tackle crucial concerns regarding security issues for connected devices. The decentralized and cryptographic nature of block chain provide significant advantages when it comes to securing IoT ecosystems, including trust management, authenticated data exchange, data authenticity, and cyberattacks [13].

3.1 BLOCKCHAIN TECHNOLOGY: BASIC CONCEPTS AND FEATURES

Block chain is a distributed, decentralized ledger technology, which is designed to record, verify and store transactions securely, transparently and immutably. In the centralized system, the data is managed and maintained by a central authority. In block chain, the data is stored in a decentralized network of nodes, where each node maintains its own copy of the block chain. This distributed architecture provides increased fault-tolerance, reliability and protection against single point failures. The immutability is one of the key features of block chain, making it extremely hard to alter or delete information once it is added to a block. Every block contains the hash of the previous block, creating a secure link between the blocks in the chronological order. If anyone tried to change the information in a block, they would have to change the

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

next block and so on, as this would be impractical from a computing standpoint. Furthermore, block chain is transparent as all authorized transaction participants in the network can validate and verify the transactions in accordance with the consensus mechanisms, such as the Proof-of-Work (PoW) or Proof-of-Stake (PoS), without depending on any centralized authority [14].

There are several important benefits that block chain provides in IoT systems for better network security and reliability. This is one of the main advantages as it guarantees the integrity of data and that it cannot be tampered with. Block chain can securely record transactions and data generated by IoT devices, allowing for real-time detection of unauthorized changes or malicious activity. All data recorded is cryptographically secured and stored forever so that attack attempts to alter or forge the data on the device are not easily done without detection. Another key benefit is distributed trust management.

Block chain facilitates authenticated data exchange between IoT devices, enabling them to connect in a decentralized manner. By being decentralised, the likelihood of central control systems failure, whether this is a single point failure, a targeted attack or data breach, is reduced. A major benefit of block chain in IoT is its ability to secure device authentication and device identity management in the IoT ecosystems. With the help of cryptographic keys, digital signatures and block chain-based identity management systems, Interconnected edge nodescan ensure secure identification and communication among trusted devices. It is used to protect against unauthorized access, spoofing and impersonation of devices in a networked environment.

Moreover, no one can alter the audit trail of block chain to track any activity, communication, and transaction on the IoT environment. Use of this permanent and transparent record allows the effective monitoring, auditing and forensic investigations should an incident or unexpected activity be detected in the system. Security administrators can trace back to what's happening and determine if the devices are compromised in some way and what can be done to minimize the effects and restore system integrity.

Furthermore, the distribution of the trust and control mechanisms in the nodes of the block chain makes IoT networks resilient and robust. A few devices or nodes, if compromised, do not affect the integrity of the entire network of block chains, as the other nodes can work independently without any problems. The decentralized nature, cryptographic security, transparency, and immutability of Block chain make it an effective tool for protecting IoT systems from cyber threats. It is a solution with numerous applications that help to ensure the reliability, scalability, and trustworthiness of the modern IoT infrastructures and protects sensitive data and critical systems from malicious attacks [15].

4. A Novel Blockchain Model for Malware Detection and Classification

In this section, we provide a detailed proposal for the detection and classification of malware in IoT networks based on Block chain technology. The proposed solution is a hybrid system that leverages Block chain's decentralized and immutable nature along with machine learning algorithms to build a powerful and intelligent system for real-time malware detection and mitigation.

i. IoT Devices: These are the points in the network that are connected such as sensors, actuators and other devices. Every IoT device can sense and send data to other Interconnected edge nodesand to the Block chain network.
ii. Block chain Network: It is the network that will be used to record transactions and store metadata associated with malware detection and classification in a decentralized manner. It's composed of a distributed network of nodes, each holding an up-to-date version of the Block chain ledger.
iii. Malware Detection and Classification Module: This module is charged with examining data from incoming Interconnected edge nodesto determine if there is any malware present and categorize it into a known category. It uses a machine learning algorithm to perform predictive analysis and anomaly detection.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

This research paper introduces the typical machine learning workflow used to detect and classify malware and explores some of its obstacles and flaws. Moreover, it analyzes the newest innovations and developments in the field, specifically deep learning Methods. In order to improve the understanding of proposed machine learning approach to detect malicious application, the complete workflow process is shown in Figure 2 and Figure 3.

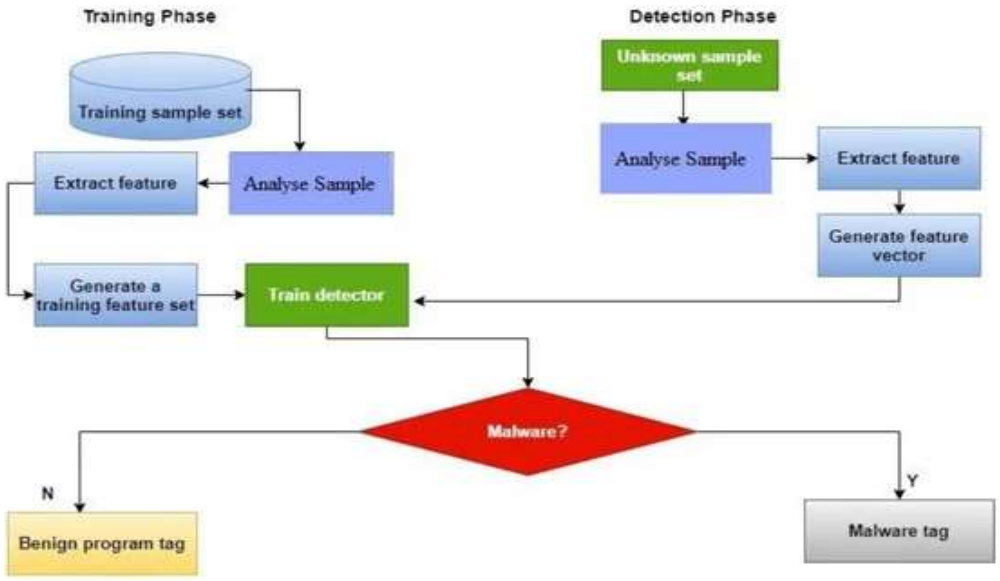

Figure 2. Proposed method for malware detection

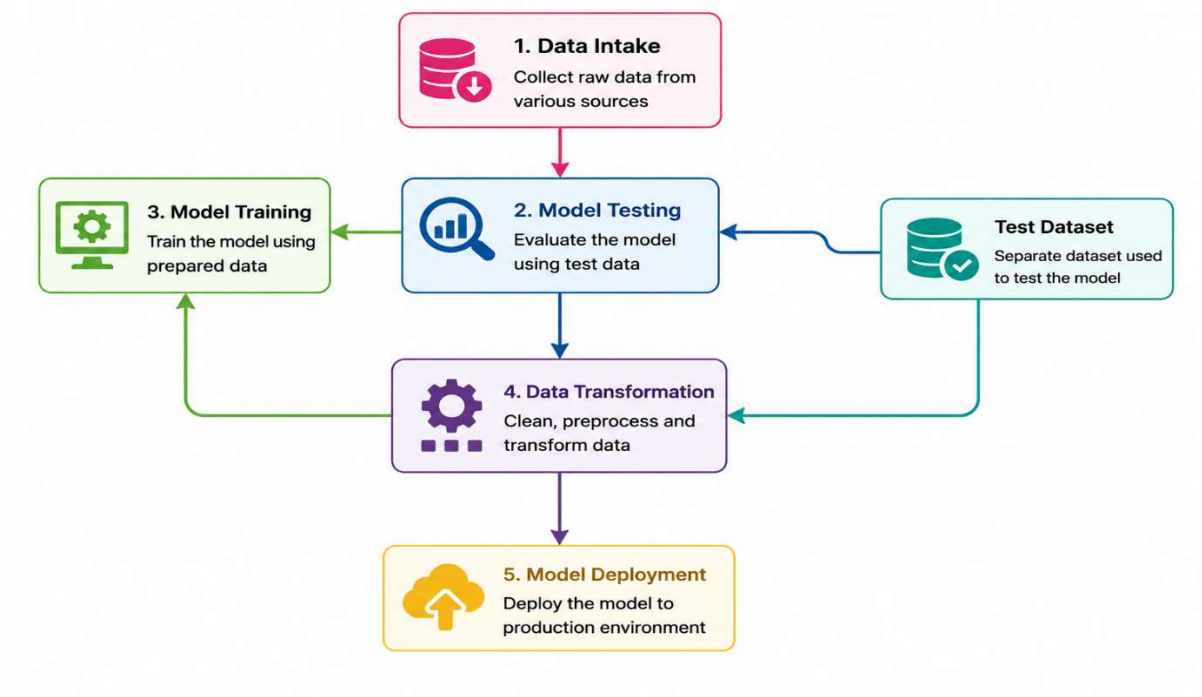

Figure 3. Workflow

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

4.1 Integration of Blockchain Techniques in Malware Detection Systems

The proposed framework is based on distributed ledger technology, which is coupled with machine learning technologies to create a secure and decentralized approach to malware detection in IoT networks. Within the proposed architecture, the data generated by the operational data of the connected IoT edge nodes, the network logs and the communication records are continuously uploaded and are securely transmitted to the validation nodes that are linked to the blockchain. Every transaction is recorded and cryptographically verified on the distributed ledger to ensure that no unauthorized input and output are affecting the security information.

The blockchain layer ensures that the records related to malware are secure, traceable, and reliable, using consensus-based validation mechanisms. The distributed ledger architecture, unlike traditional centralized storage solutions, ensures that there are no single points of failure and reduces vulnerabilities of malicious attacks on the IoT infrastructure.

The malware analysis engine uses machine learning-based anomaly detection and classification algorithms to analyze incoming traffic flow and behavior of connected devices. Once trained, the classification model can detect suspicious activities based on their unusual communication patterns, malicious signatures, and traffic irregularities in the IoT environment.

Moreover, the framework includes smart contract technology to automate malware verification, threat reporting and security policy enforcement. If any suspicious activity is detected, redefinable smart contract rules prompt threat mitigation actions, produce alerts and update the blockchain ledger in real time. This automatic decision-making process ensures greater efficiency in the response, and reduces human efforts and delays in the operations.

The proposed malware detection system based on the blockchain improves the authenticity of data, secure communication, scalability, and trust management in distributed IoT systems, and helps to monitor cyber threats in real time and intelligently mitigate attacks. [16].

4.2 DATA ACQUISITION AND PREPROCESSING METHODS

To ensure reliable malware detection, efficient data acquisition and data preprocessing mechanisms that enhance the quality and uniformity of IoT traffic data before machine learning analysis is necessary.

i. Data Collection: The proposed framework collects diverse data from the various interconnected IoT edge devices, such as traffic data, communication logs, telemetry data from the devices, sensor readings, and operational behaviour patterns. The gathered information is then safely communicated via authenticated communication paths to the analysis environment, supported by the blockchain, where further analysis and threat evaluation can be carried out.

ii. Data Pre-processing: The gathered data is first subjected to several pre-processing steps in order to remove inconsistencies and enhance learning efficiency before it is classified. The preprocessing step includes handling the missing values, removing repeated data, filtering noise, normalizing the data, encoding categorical variables, and scaling the features. These operations process raw IoT traffic data and convert it to an intelligent model of malware classes that are more structured. Feature engineering and dimensionality reduction techniques are also employed to select those features with high relevance that help increase the accuracy of detecting malware, while also reducing the complexity of computation and resource consumption.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

4.3 FEATURE EXTRACTION AND SELECTION FOR ACCURATE CLASSIFICATION

Feature extraction and dimensionality reduction by means of feature selection are significant methods to identify informative patterns and to decrease dimensionality:

Feature Extraction: Extracted features are meaningful in terms of the pre-processed data, and these features represent the characteristics of malware infection. This may include statistical parameters, frequency domain and time series characteristics of the raw data.

Feature Selection: Dimensionality reduction methods are used, like principal component analysis (PCA) or feature importance ranking, to select the most discriminative features for classification. This improves the performance of the models and reduces computation.

The proposed technique integrates Block chain technology, machine learning algorithm, and effective data collection, pre-processing, feature extraction, and feature selection techniques to provide a robust and adaptable solution for the detection and classification of IoT network malwares. The fact that Block chain is decentralized and immutable ensures the integrity and transparency of information, while machine learning helps to provide predictive analytics and real-time detection of malware threats.. This approach can be crucial to the security of IoT systems, protecting vital infrastructure and valuable information from cyber attacks.

5. RESULTS AND DISCUSSION

There are advantages and disadvantages of using the Internet every day, and the Internet is becoming more crime prone than the real world because of the cyber attacks and new viruses that can be introduced and defeat the security measures. Today, malware detection is more complex and challenging than in the past. The signature-based approach to malware detection is too old and insufficient for advanced malware detection today. While new methods for malware detection exist, it is still challenging to detect all new infections. The steps of the detection of Malware are analysing, extracting features, and classification of the Malware as malicious or benign. The most recent areas of research in cybersecurity are threat hunting, threat intelligence, digital forensics, malware detection and intrusion detection.

Block chain technology has lately become popular. Technologies that agree on the use of consensus such as fault-tolerant distributed computing systems are crucial. IoT data analysts: Understand the block chain based IoT data, which is based on DPOS, PoW, PBFT, PoS and others. Therefore, to overcome the multi-feature malware detection issue, we use a permissioned block-chain structure to store the information of the malware features. Four layers make to the architecture: 1) Network, 2) Storage, 3) Support 4) Interconnected edge node scan afford the Application Layer design. The architecture of the block chain in the IoT Malware Detection is shown in figure 10. The network, support and storage layers of the block chain layer are illustrated in Figure 4. There is substantial evidence that the proposed framework outperforms the results of the acquired experiments. In this section we review some of the basics of experimentation, including data sources, statistics to understand the performance needs of the machine learning algorithm employed, and results that support the need to pursue our model.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

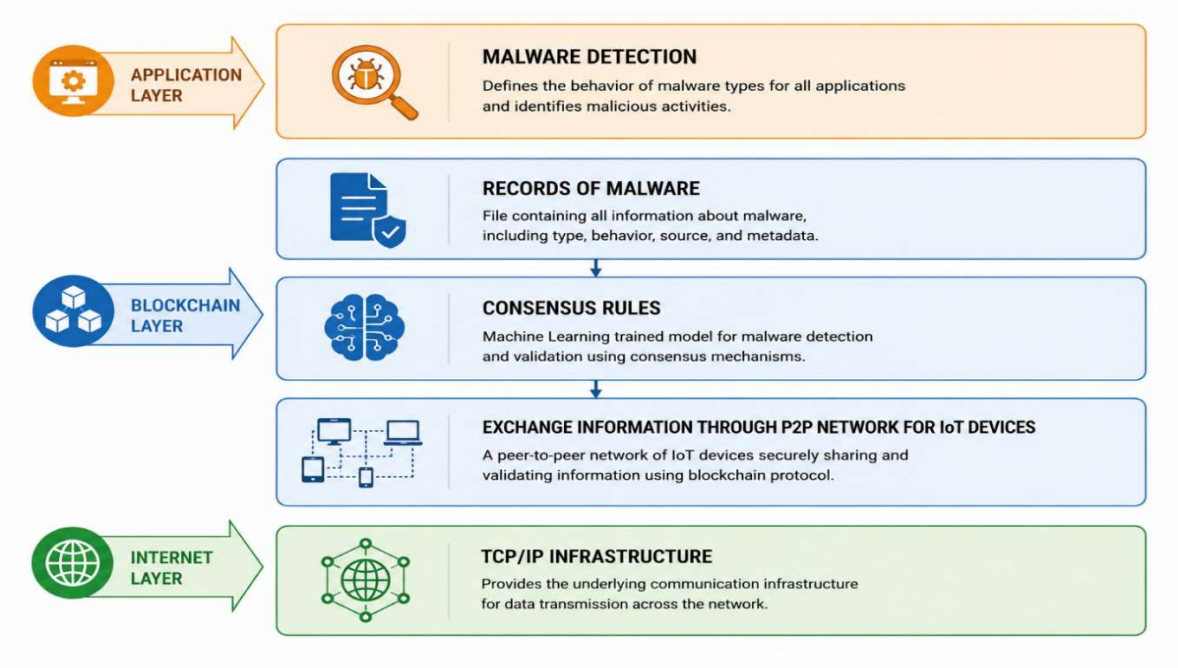

Figure 4. Malware detection using block chain.

The experimental results will demonstrate whether the features extracted from the proposed framework will be important. The clustering results are shown in Figure 5, optimized for the high dimension and noise in the data set. In clustered data, harmful samples are marked in red color while the benign samples are marked in blue color in the two following axes: feature reduction. Figure 6 (a) shows inefficient means, that is, the cluster is spread out, and Figure 6 (b) shows efficient clustering. Although two separate clusters are indicated, the representation of the subspace area of features is clearly dominating. However, a comparison of the distribution of scores will not be easy to distinguish the two groups. Placing a hyperplane becomes much easier if two clusters are shown as projections on to the data points. It is hard to produce such a data projection because a thorough analysis of the data points during separation would be required. The visualization of sample data projections in Figures 6 and 7 illustrate that our proposed approach is effective at separating the malware samples from the benign ones.

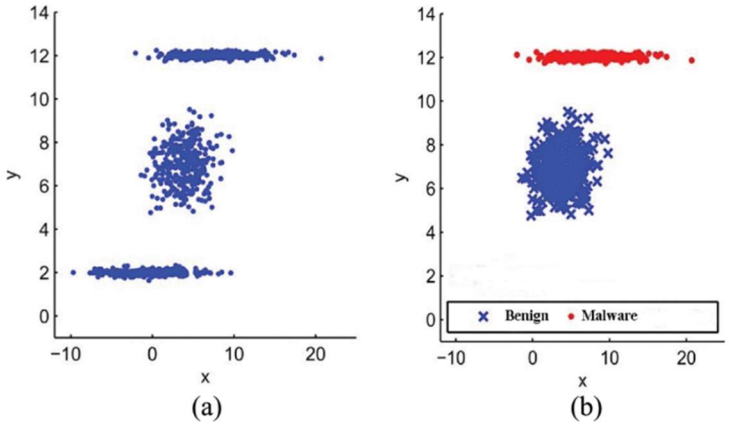

Figure 5. Classification of Malware and Benign Programs

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

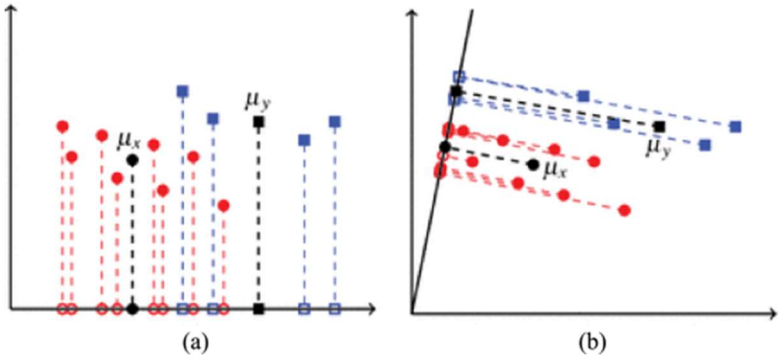

Figure 6. Feature analysis based on clustering (a) Widely dispersed means (b) Denotes a closer proximity

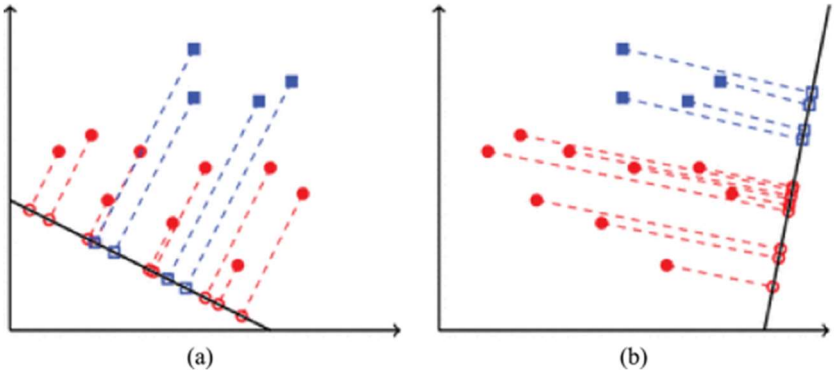

Figure 7. Analysis of projection features (a) A forecast. (b) improved forecast

6. CONCLUSION

The Internet of Things is revolutionizing the world, as various exciting applications delve into sensing, intelligent health care, long-distance monitoring, intelligent agriculture, and others. Internet of Things (IoT) devices and applications that are based on the Android platform are working together to make IoT aspirations come true. Hence, the aim of this research is to develop a system which can effectively identify malicious behavior on Android IoT devices. The information on the malware was gathered, grouped and categorized and subsequently this information was added to the block chain. In this way, all malware info documented in the block chain history can be sent out over the network, and consequently, the latest malware can be easily recognized. The clustering method we've proposed determines the weights of each feature set, and then it gradually minimizes the elements that are not needed. Although malware has many properties similar to those of benign applications, this method could be very effective at differentiating between malware and benign applications. Finally, the information that is used in our framework is authentic and is stored in a distributed malware database in the permissioned block chain. This information will aid in making the malware detection process more efficient at runtime.

REFERENCES

[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

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:6(2), June 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

[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