Blockchain-and ML based Malware Detection and Integrity Checking: A Decentralized Approach

Araharan Loganayagam

School of Computing and Engineering
University of West London
21524785@student.uwl.ac.uk

Abstract—This review paper provides an overview of the current state of malware detection and integrity checking techniques, highlighting their limitations and challenges. The review then focuses on the use of blockchain technology and machine learning algorithms for malware detection and integrity checking. First, the paper provides a review of the use of blockchain technology for security purposes, highlighting its potential benefits in providing a secure and decentralized platform for malware detection and integrity checking. The paper then discusses the use of machine learning algorithms for malware detection, analysing the different approaches proposed in existing literature. The paper also discusses the limitations and challenges of these approaches, including the need for large datasets and the risk of false positives. The integration of machine learning algorithms enables the system to learn and adapt to new threats, improving its effectiveness over time. The review concludes with a discussion of future directions and emerging trends in blockchain-and ML based malware detection and integrity checking.

Keywords— NLP, Malware, Blockchain, CNN, Cloud, Integrity, Cryptography

Introduction

In recent years, malware attacks have become increasingly prevalent, sophisticated and pose a significant threat to the security of computer systems and networks. To address this challenge, researchers have developed various malware detection and integrity checking techniques, ranging from traditional signature-based methods to more advanced machine learning and blockchain-based approaches. While these techniques have been successful in detecting and preventing malware attacks, the ever-evolving nature of malware requires continued research and innovation to stay ahead of threats. This literature review will focus on the current state of malware detection and integrity checking techniques, specifically exploring the potential of a decentralized approach based on blockchain and machine learning. By decentralizing malware detection and integrity checking, blockchain technology can provide a transparent, secure, and tamper-proof environment for detecting and preventing malware attacks. Machine learning can also enhance the accuracy and effectiveness of malware detection by

analysing large amounts of data and identifying patterns that may not be visible to traditional signature-based methods (Cristian, 2010).

The literature review will evaluate the strengths and limitations of existing techniques, including traditional signature-based methods, anomaly-based detection, and machine learning-based methods. It will then explore how blockchain and machine learning can be used together to create a decentralized approach for malware detection and integrity checking. Finally, the review will analyse the potential benefits of a decentralized approach, including increased transparency, security, and efficiency.

The Current state of malware detection and integrity checking techniques

This section aims to provide an overview of the current state of malware detection and integrity checking techniques. Specifically, we will explore the various approaches used in malware detection and integrity checking, their strengths, and limitations, as well as recent advances and challenges in the field. By synthesizing and analysing the existing literature, this review aims to identify the gaps and opportunities for future research in this critical area of cyber security.

Malware Detection

Malware detection and integrity checking are crucial components of modern cybersecurity systems. With the increasing sophistication of malware attacks, there is a need for advanced techniques to detect and prevent these threats. In this literature review, we will discuss the current state of malware detection and integrity checking techniques.

One of the popular techniques for malware detection is machine learning-based detection. In the paper by Kang et al. (2019), the authors proposed a system for malware detection using Convolutional Neural Networks (CNNs) on network traffic flow data. The system collects network traffic flow data in real-time from different sources such as routers, switches, and firewalls. The data is then processed and pre-processed to extract relevant features for malware detection. The extracted features are pre-processed to normalize the data and convert it into a format suitable for input to the CNN model. The pre-processed data is fed into the CNN model for classification of malware. The architecture of the CNN model includes several convolutional and pooling layers, as well as fully connected layers which are responsible for carrying out the classification process. The model is trained on a dataset of labelled network traffic flow data to learn the patterns of malicious traffic. After the CNN model is trained, it can be used to detect malware in real-time network traffic flow (Kang, 2019).

Another popular technique for malware detection is based on API call frequency analysis. In the paper by Vidhi et al. (2019), the authors proposed a system that uses a Convolutional Neural Network (CNN) to classify malware samples based on the frequency of API calls made by the malware program. The frequency of API calls is

recorded as a sequence of integers, which is treated as an image, and CNN is trained to classify this image as either malware or benign (Vidhi, 2019).

Furthermore, Cristian et al. (2010) proposed a cloud-based malware detection system that uses an intrusion ontology to represent features and machine learning algorithms to classify malware. The proposed system can be deployed in a cloud environment for efficient and scalable malware detection (Cristian, 2010).

In conclusion, machine learning-based detection techniques such as flow-based detection and API call frequency analysis, and cloud-based malware detection systems with intrusion ontology representation have shown promising results in detecting malware. Integrity checking techniques such as code signing, checksums, and cryptographic hash functions are also important for ensuring the integrity of software. However, with the increasing complexity and sophistication of malware attacks, there is a need for continuous research and development of new techniques for malware detection and integrity checking.

Integrity Checking

The literature review covers several papers that propose different techniques to ensure data integrity in various systems. Suchetha et al. (2020) conducted a survey on data integrity and verification techniques for cloud storage, categorizing them into cryptographic, erasure coding, replication, and secret sharing techniques. The paper provides insights into the strengths and limitations of each technique and can guide the selection of appropriate techniques for ensuring data integrity and verification. In a similar vein, Yindong Chen et al. (2017) proposed an approach that leverages digital signatures and hash functions for data verification and authentication. The paper also highlights the importance of using cloud storage service APIs to interact with the cloud storage service and retrieve or store data blocks and digital signatures. The approach outlined in this paper can help to mitigate the risk of data tampering and ensure the authenticity and integrity of data stored in the cloud. These two papers can provide a comprehensive overview of data integrity and verification techniques in cloud storage and guide the selection of appropriate techniques for ensuring data integrity and verification. (Suchetha R, 2020; Yindong Chen, 2017)

The research papers by Jambulingam et al. (2019) and Danyang et al. (2010) propose methodologies for ensuring data integrity in cloud storage. Jambulingam et al. (2019) presents an adaptive methodology that employs multiple techniques, such as data replication, hashing, Merkle tree, secret sharing, and adaptive fault detection, to detect single and multiple intrusions in cloud data. The combination of these techniques makes the proposed methodology an effective approach for ensuring data integrity in cloud storage. On the other hand, Danyang et al. (2010) proposes a system that uses MD5 hashing, block-based approach, redundant storage, error correction, and user authentication to ensure the integrity of data in cloud storage. The system generates an MD5 hash of the original file and stores it securely, uses a block-based approach to detect changes in specific parts of the file, and stores the file and its corresponding hash values in multiple locations to ensure data availability. Additionally, the system allows

only authorized users to access and modify the data, ensuring data security and integrity. These proposed methodologies provide effective solutions for ensuring the integrity of data stored in cloud storage and can guide the selection of appropriate techniques for data integrity and verification in cloud storage (Jambulingam, 2019; Danyang, 2010).

Several research papers have proposed techniques to ensure data and file integrity in cloud storage environments. The adaptive methodology presented by Jambulingam et al. (2019) uses data replication, hashing, Merkle tree, secret sharing, and adaptive fault detection techniques. Danyang et al. (2010) proposes a system that uses MD5 hashing, block-based approach, redundant storage, error correction, and user authentication to ensure the integrity of data in cloud storage. Ahmed et al. (2022) provides an overview of various techniques used by file integrity checkers, including hashing, digital signatures, change monitoring, and rootkit detection, and discuss attacks that can be used to bypass them. Gopalan et al. (2005) discuss techniques such as cryptographic hash functions, error-correcting codes, RAID, data mirroring, data scrubbing, and data verification used to ensure data integrity in storage. Varalakshmi et al. (2012) propose a new methodology that uses encryption algorithms, hash functions, and message authentication codes to protect data integrity in cloud environments. These papers contribute to the existing literature by providing effective solutions for ensuring data and file integrity in cloud storage and can be valuable resources for researchers and practitioners working in the field of cybersecurity. (Jambulingam, 2019; Danyang, 2010; Ahmed, 2022; Gopalan, 2005; Varalakshmi, 2012).

The Review of the use of blockchain technology for security purposes

In recent years, ensuring data integrity has become increasingly important due to the proliferation of data breaches and cyber-attacks. Several research papers propose different techniques to ensure data integrity, each with its own strengths and weaknesses. Ahmed et al. (2022) provides a comprehensive overview of various techniques used by file integrity checkers, while Gopalan et al. (2005) describe techniques used to ensure data integrity in storage. Varalakshmi et al. (2012) propose a new methodology for ensuring data integrity in a cloud environment, and Yiran et al. (2022) propose a novel scheme that uses blockchain technology for data integrity in multi-cloud storage environments. Finally, Chao et al. (2019) suggest using a combination of blockchain technology, smart contracts, data encryption, hashing, and access control techniques to ensure data integrity, security, and privacy in service collaboration environments. These papers provide valuable insights into different techniques used for data integrity, each with its own unique approach, and can be useful resources for researchers and practitioners working in the field of cybersecurity.

Several research papers propose different schemes for ensuring data integrity in cloud computing environments using blockchain technology. Ravishankar et al. (2010) proposed a novel approach that uses blockchain technology, smart contracts, distributed consensus mechanisms, public key cryptography, and Merkle trees to ensure the integrity and security of data stored in the cloud. On the other hand, Zhenpent

et al. (2022) proposed a scheme that leverages blockchain expansion technology, smart contracts, Merkle trees, SHA-256 hash function, and Bloom filters to provide a tamper-proof and efficient way of auditing data integrity. Their proposed scheme uses expansion technology to reduce the size of the blockchain and improve its efficiency. Both schemes provide efficient and secure ways to verify the integrity of data in cloud storage environments, while reducing the computational overhead and false positive rate (Ravishankar, 2020; Zhenpeng, 2022).

One proposed solution for multi-cloud storage environments utilizes blockchain technology along with Merkle trees, Shamir's secret sharing, and homomorphic encryption, while another paper suggests using blockchain technology, smart contracts, data encryption, hashing, and access control techniques to ensure data integrity, security, and privacy in service collaboration environments. Another paper proposes using blockchain technology, smart contracts, distributed consensus mechanisms, public key cryptography, and Merkle trees to ensure data integrity in cloud computing environments, while another paper leverages blockchain expansion technology, smart contracts, Merkle trees, SHA-256 hash function, and Bloom filters to ensure data integrity in cloud storage environments. Additionally, the literature review covers papers that propose techniques to ensure data integrity in specific areas such as land registration and file systems. The proposed techniques in these papers utilize various components of blockchain technology such as smart contracts, decentralized identity management, consensus mechanisms, and decentralized storage, as well as other techniques such as checksums, hashing, data mirroring and redundancy, and multi-factor authentication to ensure data integrity and security (Vinothiyalakshmi, 2022; Chao, 2019; Ravishankar, 2020; Zhenpeng, 2022; Jerzy, 2008; Sivanantham, 2022).

Review of the use of machine learning algorithms for malware detection

The literature review covers several papers that propose technical architecture and approaches for malware detection and classification using different techniques. Pejman et al. (2021) presents a novel approach to malware detection using natural language processing, entity behaviour analytics, and machine learning techniques. The approach involves extracting features from system call traces using NLP techniques and analysing them using EBA to detect anomalies in system entity behaviour that could be indicative of malware. Machine learning techniques such as Random Forest and Support Vector Machine are then used to classify the system behaviour as normal or malicious based on the extracted features. On the other hand, Priya et al. (2023) provides a comprehensive overview of recent research on malware classification and detection using transfer learning. The paper highlights the significance of techniques such as malware feature extraction, transfer learning, deep learning, ensemble methods, and feature selection in improving the performance of malware detection models. Sanjeev et al. (2016) presents a technical architecture for real-time protection against malware using semantics-based techniques that involves several components, including data collection, pre-processing, malware detection model, decision engine, real-time protection module, and malware analysis and reporting. Finally, Wu et al. (2011) propose a comprehensive technical architecture for malware analysis and detection that

incorporates several stages, including data collection, feature extraction, pre-processing, machine learning, evaluation, and malware detection. The paper emphasizes the use of behaviour-based detection techniques and highlights the importance of evaluation using cross-validation to evaluate the model's performance. Overall, these papers provide valuable insights into different approaches and techniques for malware detection and classification that could help improve the accuracy and efficiency of existing systems.

The literature offers various approaches to malware detection, including real-time protection against malware using semantics-based techniques proposed by Sanjeev et al. (2016). Wu et al. (2011) propose a comprehensive technical architecture for malware analysis and detection that employs behaviour-based detection techniques and machine learning algorithms to achieve high detection accuracy. Kambiz et al. (2021) propose a cloud-based approach that detects malware by analysing user behaviour using the behavioural entropy metric, which can detect unknown and zero-day malware. Bander et al. (2017) proposes a lightweight and effective approach to malware detection on Windows platforms using behaviour-based analysis that compares behavioural profiles to a pre-defined baseline. Cristian et al. (2010) propose a novel approach to malware detection that leverages cloud computing and ontology-based feature extraction using machine learning algorithms, which demonstrate the effectiveness of the proposed system compared to other state-of-the-art malware detection systems. These proposed approaches demonstrate the importance of a multi-faceted approach to malware detection, incorporating various techniques to improve detection accuracy and scalability.

Analysis of the different approaches proposed in existing literature

Malware Detection

Title and Researchers	Purpose	Key Findings	Advantages	Limitations
NLP-based Entity Behaviour Analytics for Malware Detection (Pejman Najafi, Daniel Koehler, Feng Cheng, Christoph Meinel)	A framework that utilizes Entity Behaviour Analytics (EBA) based on Natural Language Processing (NLP) to detect malware in computer networks.	NLP-based EBA approach could effectively detect malware in computer networks with a high degree of accuracy. By analyzing the language used in network logs, the system could identify anomalous behavior and alert network administrators to potential security threats.	It can detect malware that traditional signature-based approaches may miss, as well as identify new, previously unknown threats. The approach is also more scalable than traditional methods, as it can analyze large amounts of log data	For the method to work efficiently, it requires precise and comprehensive log data. If log data is incomplete or inaccurate, the system may miss malware infections. Additionally, the approach may have difficulty detecting malware that is

			quickly and efficiently.	specifically designed to evade NLP-based detection methods. Finally, the approach may generate false positives if normal network behavior is mistakenly identified as anomalous.
Review on Malware Classification and Malware Detection Using Transfer Learning Approach (Priya V, Dr. Sathya Sofia A)	This paper provides a summary of the current advanced methods and techniques for detecting and categorizing malware, with a specific emphasis on approaches that employ transfer learning.	Transfer learning allows for the transfer of knowledge from one domain to another, this enables the enhancement of precision and effectiveness of malware detection systems. Hybrid models that combine different types of features, such as static and dynamic features, have been found to be effective in malware classification and detection. Deep learning methods such as CNNs and RNNs have demonstrated encouraging outcomes in the field of malware classification and detection.	A thorough examination of the latest advanced techniques and methods for identifying and categorizing malware is provided in this review. The review emphasizes the possibility of enhancing the precision and efficiency of malware detection systems by utilizing transfer learning-based approaches.	The focus of the analysis was on comparing the various transfer learning-based approaches and did not involve addressing the difficulties and restrictions linked to using transfer learning for malware detection and classification.
Semantics-Based Online Malware Detection: Towards Efficient Real-Time Protection Against Malware	new approach to online malware detection based on semantic analysis of application behaviour.	The proposed approach can detect both known and unknown malware in real-time.	Improved detection rates: The semantic analysis-based approach is more effective at detecting malware than	High false positive rate: The semantic analysis-based approach may generate false positives.

(Sanjeev Das, Yang Liu, Wei Zhang, and Mahintham Chandramohan)	The authors aim to provide more efficient real-time protection against malware.	The semantic analysis of application behaviour provides a more effective way to detect malware than traditional signature-based approaches. The approach can handle code obfuscation and other techniques used by malware authors to evade detection. The approach can detect malware even when it is injected into legitimate processes.	traditional signature-based approaches. Real-time protection: The approach provides real-time protection against malware. Handling of obfuscation techniques: The approach can detect malware even when it is hidden using code obfuscation techniques. Detection of injected malware: The approach can detect malware that has been injected into legitimate processes.	Performance overhead: The approach may have a performance overhead due to the need for semantic analysis of application behaviour. Limited application coverage: The approach may not be able to detect all types of malwares, especially those that do not exhibit malicious behaviour. Requires access to network traffic: The approach requires access to network traffic to detect malware that communicates with external servers.
Behaviour-based Malware Analysis and Detection (LIU Wu1), REN Ping2), LIU Ke3), DUAN Hai-xin1)	propose a behaviour-based approach to detect and analyse malware. The paper proposes a new system architecture that includes three components: behaviour monitoring, analysis, and detection.	A behaviour-based approach is effective in detecting and analysing malware. The proposed system architecture has the potential to be an efficient and accurate method for malware detection and analysis. The use of machine learning algorithms can enhance the performance of	The proposed behaviour-based approach can detect and analyse malware even if it is not known beforehand. The system architecture proposed in the paper is scalable and can be adapted to different environments and applications. Machine learning techniques have	The proposed system architecture requires significant computational resources to analyse the behaviour of the malware. The accuracy of the system heavily depends on the quality of the behaviour models used. The system may generate false positives or false negatives,

		malware detection.	the potential to enhance the precision and effectiveness of identifying malware.	leading to incorrect detection or non-detection of malware.
Cloud Based Malware Detection Through Behavioural Entropy (Kambiz Vahedi ,Khadijeh Afhamisisi)	propose a cloud-based malware detection system that uses behavioural entropy to detect and classify malware in real-time.	The proposed system achieved a high detection rate of 98% and low false-positive rate of 0.05%. The system can classify malware into different families with high accuracy. The system is scalable and can handle many requests simultaneously.	It can detect previously unknown malware and zero-day attacks. It can handle many requests simultaneously, making it suitable for use in cloud environments. It uses behavioural entropy, which is a novel approach that can detect subtle changes in malware behaviour.	It may not be effective against malware that uses sophisticated evasion techniques. It may generate false positives if the user's behaviour changes frequently.
Lightweight Behavioural Malware Detection for Windows Platforms (Spiros Mancoridis, Hunter Dong, Avinash Srinivasan, Bander Alsulami)	propose a lightweight and efficient method for detecting malware in Windows platforms based on the analysis of the behaviour of software.	development of a behaviour-based malware detection system for Windows platforms, which is lightweight and efficient, and can detect previously unseen malware.	The development of a fast and accurate malware detection system that is effective against zero-day attacks and new malware variants. The system is also lightweight, which means that it can be deployed on low-resource systems without affecting performance.	system relies on the analysis of behavioural patterns of malware, which may be limited in certain situations. Additionally, the system may not be effective against malware that is designed to evade behaviour-based detection systems.
Flow-based Malware Detection Using Convolutional Neural Network	propose a new method for detecting malware using flow-based analysis and convolutional	achieves high accuracy in detecting malware and outperforms traditional machine learning approaches.	The advantage of the proposed method is that it can handle large volumes of network traffic data and detect	the limitation of the paper is that it only focuses on detecting a specific type of malware and does not

(Gustavo Isaza Echeverri, Andrés G ,Khadijeh Afhamisis)	neural networks (CNN).		malware with high accuracy.	consider other types of cyber threats.
Malware Detection based on API Calls Frequency (Vidhi Garg, Rajesh Kumar Yadav)	propose a method for malware detection using the frequency of API calls made by a software program. The paper presents a framework that analyses the sequence of API calls made by a program and uses it to classify it as either malicious or benign.	analysing API calls frequency is an effective method for detecting malware. The proposed framework achieved an accuracy of 99.05% in detecting malware samples from the Zoo malware dataset.	It has the ability to detect zero-day malware and doesn't necessitate access to the program's source code. Additionally, the method is computationally efficient and can be applied in real-time.	it may produce false positives if the program under analysis makes many API calls. it may not be effective against malware that does not make API calls. Furthermore, it may be vulnerable to attacks that modify the frequency of API calls made by a program to evade detection.
Malware Detection based on Cloud Computing integrating Intrusion Ontology representation. (Cristian Adrián Martínez, Gustavo Isaza Echeverri, Andrés G. Castillo Sanz)	Computing integrating Intrusion Ontology representation is to propose a novel approach for detecting malware in cloud computing environments by integrating intrusion ontology representation.	The malware detection technique has demonstrated high efficiency in identifying both known and unknown malware in cloud computing environments with a low rate of false positives. The use of intrusion ontology representation helps to improve the accuracy and efficiency of malware detection. The proposed approach is scalable and can handle large-scale cloud computing environments.	The approach can detect both known and unknown malware. The use of intrusion ontology representation helps to improve the accuracy and efficiency of malware detection. The approach is scalable and can handle large-scale cloud computing environments.	The approach may require significant computing resources to handle large-scale cloud computing environments. The approach may require frequent updates to the intrusion ontology to keep up with new malware threats. The approach may be vulnerable to evasion techniques employed by advanced malware.

Integrity Checking

Title and Researchers	Purpose	Key Findings	Advantages	Limitations
An Approach to Verifying Data Integrity for Cloud Storage (Yindong Chen, Liping Li, Ziran Chen)	propose a method for verifying data integrity in cloud storage services using digital signatures. The paper aims to address the challenge of ensuring the authenticity and integrity of data stored in the cloud.	The system utilizes hash functions for creating an exclusive digest of data blocks saved in the cloud, while digital signatures are used to guarantee the authentication and integrity of the hash values produced by the hash functions. The management of digital certificates and public keys required for generating and verifying digital signatures is accomplished through the use of a PKI. The approach is implemented using the cloud storage service API to interact with the cloud storage service to retrieve and store data blocks and digital signatures.	Ensuring the authenticity and integrity of data stored in the cloud. Providing a secure and efficient method for verifying data integrity in cloud storage services. Seamless integration with cloud storage services using the cloud storage service API. Use of widely available cryptographic techniques such as hash functions and digital signatures.	The proposed approach may have limitations due to its reliance on the API of the cloud storage service, which may not be accessible or may lack the required features. The need for a PKI to manage the digital certificates and public keys, which may add complexity and overhead to the implementation. The approach may not provide protection against other types of security threats, such as unauthorized access or data leakage. The proposed approach may require additional processing and storage resources, which could affect performance and cost.
An Adaptive Methodology for Integrity Checking in Cloud Storage (L Jambulingam, T V Ananthan, P S Rajakumar)	adaptive methodology for integrity checking in cloud storage that can detect both single and multiple intrusions in cloud data.	The proposed approach utilizes various techniques, such as data replication, hashing, Merkle tree, secret sharing, and adaptive fault detection, to ensure the integrity of data	The approach efficiently guarantees the security and authenticity of cloud-stored data by incorporating several techniques, thereby enhancing its resilience and protection.	The methodology relies on the use of multiple techniques, which may increase computational overhead and complexity. The proposed methodology assumes that

		stored in cloud storage in an effective manner. The adaptive fault detection mechanism used in the methodology can detect both single and multiple intrusions in cloud data by utilizing statistical analysis to detect anomalies in data patterns. The proposed methodology is flexible and can be customized to meet the specific requirements of different cloud storage systems.	The adaptive fault detection mechanism used in the methodology can detect both single and multiple intrusions in cloud data, providing an added layer of security. The methodology is flexible and can be customized to meet the specific requirements of different cloud storage systems.	cloud storage providers are honest and do not collude with attackers, which may not always be the case in practice. The effectiveness of the proposed methodology may be affected by the size and complexity of the cloud storage system, as well as the quality of the statistical analysis used in the adaptive fault detection mechanism.
Design and implementation for MD5-based data integrity checking system. (Danyang Cao, Bingru Yang)	The authors suggest a solution for preserving the authenticity of data stored in cloud storage by utilizing the MD5 algorithm.	The proposed system can detect changes in specific parts of the file by dividing it into blocks and generating a hash for each block. The system uses error-correcting codes to detect and correct errors in the hash values, thus ensuring data integrity. The system provides redundant storage to ensure that data can be retrieved in case of failures. The system allows only authorized users to access and modify the data,	it can ensure the integrity of data in cloud storage by using a simple and efficient MD5-based algorithm. The system also provides additional features such as user authentication, redundant storage, and error correction to ensure data security and availability.	MD5 algorithm is susceptible to collision attacks, which can compromise the integrity of the data. Additionally, the system may not be suitable for very large files as it may become computationally intensive to generate and store hashes for each block.

		thus ensuring data security.		
Integrity Checking for Cloud Environment Using Encryption Algorithm (P.Varalakshmi , Hamsavardhini Deventhiran)	ensuring data integrity in the cloud environment using encryption algorithms.	The AES encryption algorithm is utilized for ensuring data integrity in the cloud environment. The proposed technique uses a hash function to calculate the hash value of the data before encryption and stores the hash value along with the encrypted data. During data retrieval, the hash value is recalculated, and the recalculated hash value is compared with the stored hash value to ensure data integrity.	The data stored in the cloud environment is highly secure. The use of encryption algorithms ensures that the data is secure from unauthorized access. The use of a hash function for calculating the hash value of the data ensures that any modifications to the data are detected.	The computational burden linked with the utilization of encryption algorithms and hash functions. The use of encryption algorithms may slow down the data transfer rate, and the use of hash functions may increase the processing time required for data retrieval. Additionally, the technique does not provide protection against attacks that exploit vulnerabilities in the encryption algorithm.
A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage (Yiran Zhang,Huizheng Geng,Li Su and Li Lu)	propose a new approach for ensuring the integrity of data stored in a multi-cloud storage environment. The authors propose a blockchain-based scheme for efficient data integrity verification using a combination of cryptographic techniques and blockchain technology.	The key findings of the research paper are that the proposed scheme is more efficient and effective than existing schemes for data integrity verification in multi-cloud storage environments. The scheme provides a high level of security and reliability while reducing the computational overhead and communication costs associated with traditional integrity	The main advantage of the proposed scheme is that it ensures data integrity in a distributed environment without relying on a trusted third party or central authority. It also provides a transparent and tamper-proof way to verify the integrity of data in a multi-cloud storage environment.	Further research and experimentation are required to assess the scalability and performance of the proposed scheme in larger and more complex multi-cloud storage environments. There may also be challenges in implementing the scheme in practice due to the need for coordination and agreement among multiple cloud providers.

		checking methods.		
Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments (Dr.B. Ravishankar, Prateek Kulkarni, Vishnudas M V)	propose a solution for ensuring data integrity in cloud computing environments using blockchain technology. The paper introduces a blockchain-based database system that provides a tamper-proof, secure, and efficient method for data integrity verification in cloud computing.	The proposed system, which utilizes a blockchain-based approach for data integrity verification, has been successfully implemented and offers several advantages over traditional methods, including enhanced security, transparency, and tamper-proofing.	The proposed system offers a secure and tamper-proof way to verify data integrity in a cloud computing environment, along with increased transparency and decreased dependence on central authorities. The system also provides efficient and cost-effective data integrity verification, which can benefit organizations that deal with large amounts of data.	The limitations of the research paper include the fact that the proposed system is not immune to attacks, and there may be some scalability issues when dealing with many transactions. Additionally, the paper does not provide a detailed analysis of the performance of the proposed system, and further research may be required to optimize the system's performance.
Data Integrity Audit Scheme Based on Blockchain Expansion Technology (Zhenpeng Liu Yongjiang, Lele Ren and Weihua Zheng)	to propose a data integrity audit scheme based on blockchain expansion technology for cloud storage. The paper aims to enhance data security by providing a tamper-proof and decentralized mechanism for data integrity verification in the cloud.	achieve efficient and secure data integrity verification in the cloud environment. The scheme uses blockchain expansion technology to improve the performance of blockchain-based data integrity verification schemes, making it more practical for use in large-scale cloud storage systems.	The proposed method offers several benefits, including the capability to achieve real-time data integrity verification while maintaining a low computational overhead, its decentralized and tamper-proof nature, and its capacity to provide an effective and scalable solution for data integrity verification in cloud storage.	proposed scheme has not been implemented and evaluated in a real-world cloud storage system. which may affect its practicality and performance. Additionally, the paper does not provide a detailed analysis of the security and privacy implications of the proposed scheme, which could be a potential area for further research.
Land Registration System Using Blockchain (SaiApurva Gollapalli, Gayatri	propose a blockchain-based land registration system that can address issues related to land registration such as fraud, corruption,	The paper proposes a blockchain-based system for land registration that can eliminate intermediaries and provide a	The proposed system can bring several advantages, including improved efficiency, transparency,	The paper does not discuss the challenges related to the implementation of the proposed system, such as the legal and

Krishnamoorthy, Neha Shivaji Jagtap, Rizwana Shaikh)	and inefficiencies in the current centralized systems.	tamper-proof and transparent system for land registration. The proposed system utilizes smart contracts to automate the registration process, reduce transaction costs, and ensure secure and efficient transfer of land ownership. The system also provides a decentralized platform for storing and managing land records, which can be accessed by stakeholders in a secure and transparent manner.	security, and reduced costs. The use of blockchain technology can eliminate intermediaries, reduce transaction costs, and minimize the risk of fraud and corruption in land registration. The system can provide a tamper-proof and transparent platform for managing land records, which can improve transparency and reduce the time required for processing land transactions.	regulatory framework, scalability, and interoperability with existing systems. The paper also does not provide a detailed analysis of the potential risks and vulnerabilities associated with the use of blockchain technology in land registration.
Reliable Data Storage and Sharing using Blockchain Technology and Two Fish Encryption (S. Sivanantham, M. Sakthivel, V. Krishnamoorthy, N. Balakrishna, V. Akshaya)	propose a secure and reliable data storage and sharing system using blockchain technology and Two Fish encryption.	The proposed system provides a high level of security and reliability for data storage and sharing. Blockchain technology ensures data integrity, immutability, and transparency. Two Fish encryption provides strong data confidentiality. The system is resistant to attacks such as data tampering, data theft, and denial of service attacks.	High level of security and reliability for data storage and sharing. Decentralized and transparent data management using blockchain technology. Strong data confidentiality using Two Fish encryption. Resistant to various types of attacks.	The system relies on the availability of the blockchain network and the Two Fish encryption algorithm. The system may have slower performance compared to centralized data storage and sharing systems. The system may require significant computational resources for encryption and decryption operations.

Conclusion

In conclusion, traditional malware detection methods have limitations that make them less effective in detecting new and unknown types of malwares. These limitations have led to the development of new approaches such as blockchain-and ML based malware detection and integrity checking. This approach addresses the challenges of making generalized malware detection models by using machine learning algorithms to detect malware behaviour and combining them with blockchain technology for decentralized and secure verification of the integrity of the detection system. However, there are still challenges to overcome, such as adversarial attacks and the need for fast and efficient models. Further research is needed to develop more robust and effective solutions that can keep up with the constantly evolving threat landscape. Overall, blockchain-and ML based malware detection and integrity checking present a promising direction for the development of more effective and efficient malware detection systems.

References

Ahmed, M., 2022. File Integrity Checkers: Functionality, Attacks, and Protection. *2022 2nd International Conference on Digital Futures and Transformative Technologies (ICoDT2).*

Bander, A., 2017. Lightweight behavioral malware detection for windows platforms. *2017 12th International Conference on Malicious and Unwanted Software (MALWARE).*

Chao, S., 2019. Block Chain-Based Data Audit and Access Control Mechanism in Service Collaboration. *2019 IEEE International Conference on Web Services (ICWS).*

Cristian, G., 2010. Malware detection based on Cloud Computing integrating Intrusion Ontology representation. *2010 IEEE Latin-American Conference on Communications.*

Danyang, B., 2010. Design and implementation for MD5-based data integrity checking system. *2010 2nd IEEE International Conference on Information Management and Engineering.*

Gopalan, C., 2005. Ensuring data integrity in storage. *Proceedings of the 2005 ACM workshop on Storage security and survivability.*

Jambulingam, A., 2019. An Adaptive Methodology for Integrity Checking in Cloud Storage. *International Journal of Engineering and Advanced Technology*, 8(6), pp. 4470-4475.

Jerzy, M., 2008. Modern approaches to file system integrity checking. *2008 1st International Conference on Information Technology.*

Kambiz, K., 2021. Cloud Based Malware Detection Through Behavioral Entropy. *2021 IEEE International Conference on Big Data (Big Data).*

Kang, H. K. K. &. K. J., 2019. Flow-based Malware Detection Using Convolutional Neural Network. *Journal of Information Processing Systems,* pp. 95-105.

Misbah, A., 2020. Security of IoT Using Block chain: A Review. *2020 International Conference on Information Science and Communication Technology (ICISCT).*

Pejman, D., 2021. NLP-based Entity Behavior Analytics for Malware Detection. *2021 IEEE International Performance, Computing, and Communications Conference (IPCCC).*

Priya, S. S., 2023. Review on Malware Classification and Malware Detection Using Transfer Learning Approach. *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT).*

Ravishankar, P., 2020. Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments. *2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI).*

Sanjeev, Y., 2016. Semantics-Based Online Malware Detection: Towards Efficient Real-Time Protection Against Malware. *IEEE Transactions on Information Forensics and Security*, 11(2), pp. 289-302.

Sivanantham, S., 2022. Reliable Data Storage and Sharing using Block chain Technology and Two Fish Encryption. *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA).*

Suchetha R, P. ,. S. ,. A., 2020. Survey on Data Integrity and Verification for Cloud Storage. *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT).*

Varalakshmi, H., 2012. Integrity checking for cloud environment using encryption algorithm. *2012 International Conference on Recent Trends in Information Technology*.

Vidhi, R., 2019. Malware Detection based on API Calls Frequency. *2019 4th International Conference on Information Systems and Computer Networks (ISCON).*

Vinothiyalakshmi, M., 2022. Digitized Land Registration Using Blockchain Technology. *Blockchain Technology,* pp. 73-86.

Wu, P.-x., 2011. Behavior-Based Malware Analysis and Detection. *2011 First International Workshop on Complexity and Data Mining.*

Yeo, K., 2018. 2018 International Conference on Information Networking (ICOIN). *2018 International Conference on Information Networking (ICOIN).*

Yindong Chen, L., 2017. An Approach to Verifying Data Integrity for Cloud Storage. *2017 13th International Conference on Computational Intelligence and Security (CIS).*

Yiran, H., 2022. A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage. *IEEE Access,* Volume 10, pp. 105920-105929.

Zhenpeng, Y., 2022. Data Integrity Audit Scheme Based on Blockchain Expansion Technology. *IEEE Access,* Volume 10, pp. 55900-55907.