ISSN 2347 - 3983
Volume 12. No.1, January 2024
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter041212024.pdf
https://doi.org/10.30534/ijeter/2024/041212024

Anomaly Detection in Block Chain

Abubakkar Siddiq[1], Faris[2] , Mohammed Muneeb[3] , Ranjith s[4]
[1] Department of Computer Science and Engineering, AIET, India, siddiqs005@gmail.com
[2] Department of Computer Science and Engineering, AIET, India, farismohammed1612@gmail.com
[3] Department of Computer Science and Engineering, AIET, India, mummuneeb@gmail.com
[4] Department of Computer Science and Engineering, AIET, India, 4al21cs404@gmail.com

Received Date: November 30, 2023 Accepted Date: December 25, 2023 Published Date : January 07, 2024

ABSTRACT

Blockchain technology has gained significant attention in various domains due to its decentralized and immutable nature. However, ensuring the integrity and security of blockchain systems remains a critical concern. Anomaly detection techniques play a crucial role in identifying abnormal behavior and potential attacks within blockchain networks. This paper presents a comprehensive review of existing research on anomaly detection in blockchain, highlighting the methodologies, challenges, and future directions in this emerging field.

Key Words : Blockchain, Anomaly Detection, Support Vector Machines, Federated Learning

1. LITERATURE SURVEY

Proposed a new model for anomaly detection over bitcoin electronic transactions. Authors used two machine learning algorithms, namely the One Class Support Vector Machines (OCSVM) algorithm to detect outliers and the K-Means algorithm in order to group the similar outliers with the same type of anomalies. They evaluated their work by generating detection results and obtained high performance results on accuracy[1].Proposed a methodology where they can use intelligent software agents to monitor the activity of stakeholders in the blockchain networks to detect anomaly such as collusion, using supervised machine learning algorithm and algorithmic game theory and stop the majority- Attack from taking place[2].

Proposed secure SVM, which is a privacy- preserving SVM training scheme over blockchain- based encrypted IoT data. They utilized the blockchain techniques to build a secure and reliable data sharing platform among multiple data providers, where IoT data is encrypted and then recorded on a distributed ledger. They designed secure building blocks, such as secure polynomial multiplication and secure comparison, by employing a homomorphic cryptosystem, Paillier, and construct a secure SVM training algorithm, which requires only two interactions in a single iteration, with no need for a trusted third-party. Rigorous security analysis prove that the proposed scheme ensures the confidentiality of the sensitive data for each data provider as well as the SVM model parameters for data analysts.

Integrated MCS with industrial systems without introducing any additional dedicated devices.To overcome the drawbacks of traditional MCS systems, they proposed a blockchain-based MCS system (BMCS). In particular, they exploited miners to verify the sensory data and design a dynamic reward ranking incentive mechanism to mitigate the imbalance of multiple sensing tasks. Meanwhile, they also developed a sensory data quality detection scheme to identify and mitigate the data anomaly. They have implemented a prototype of the BMCS on top of Ethereum and conduct extensive experiments on a realistic factory workroom. Both experimental results and security analysis demonstrate that the BMCS can secure industrial systems and improve the system reliability[4].

Proposed a privacy-preserving framework to achieve both privacy and security in smart power networks. The framework includes two main modules: A two-level privacy module and an anomaly detection module. In the two-level privacy module, an enhanced-proof- of-work-Technique-based blockchain is designed to verify data integrity and mitigate data poisoning attacks, and a variational autoencoder is simultaneously applied for transforming data into an encoded format for preventing inference attacks. In the anomaly detection module, a long short-Term memory deep learning technique is used for training and validating the outputs of the two-level privacy module using two public datasets. The results highlight that the proposed framework can efficiently protect data of smart power networks and discover abnormal behaviors, in comparison to several state-of-The-Art techniques[5].

Proposed a transaction-based classification and detection approach for Ethereum smart contract to address these issues. They collected over 10,000 smart contracts from Ethereum and focused on the data behavior generated by smart contracts and users. They identified four behavior patterns from the transactions by manual analysis, which can be used to distinguish the difference between different types of contracts. Then 14 basic features of a smart contract are constructed from these. To construct the experimental dataset, They proposed a data slicing algorithm for slicing the collected smart contracts. After that, they used an LSTM network to train and test our datasets. The extensive experimental results show that our

approach can distinguish different types of contracts and can be applied to anomaly detection and malicious contract identification with satisfactory precision, recall, and f1-score[14].

Proposed PPSF is based on two key mechanisms: A two-level privacy scheme and an intrusion detection scheme. First, in a two-level privacy scheme, a blockchain module is designed to securely transmit the IoT data and Principal Component Analysis (PCA) technique is applied to transform raw IoT information into a new shape. In the intrusion detection scheme, a Gradient Boosting Anomaly Detector (GBAD) is applied for training and evaluating the proposed two-level privacy scheme based on two IoT network datasets, namely ToN-IoT and BoT-IoT. They also suggest a blockchain-InterPlanetary File System (IPFS) integrated Fog- Cloud architecture to deploy the proposed PPSF framework. Experimental results demonstrate the superiority of the PPSF framework over some recent approaches in blockchain and non-blockchain systems[7].

Proposed various detection methods fostered by machine learning (ML) techniques. Federated learning (FL), as a promising distributed ML paradigm, has been employed recently to improve detection performance due to its advantages of privacy-preserving and lower latency. However, existing FL-based methods still suffer from efficiency, robustness, and security challenges. To address these problems, in this article, they initially introduced a blockchain- empowered decentralized and asynchronous FL framework for anomaly detection in IoT systems, which ensures data integrity and prevents single- point failure while improving the efficiency. Further, they designed an improved differentially private FL based on generative adversarial nets, aiming to optimize data utility throughout the training process. To the best of our knowledge, it is the first system to employ a decentralized FL approach with privacy-preserving for IoT anomaly detection. Simulation results on the real-world dataset demonstrate the superior performance from aspects of robustness, accuracy, and fast convergence while maintaining high level of privacy and security protection.

Proposed in this article a collaborative clustering-characteristic-based data fusion approach for intrusion detection in a Blockchain-based system, where a mathematical model of data fusion is designed and an AI model is used to train and analyze data clusters in Blockchain networks. The abnormal characteristics in a Blockchain data set are identified, a weighted combination is carried out, and the weighted coefficients among several nodes are obtained after multiple rounds of mutual competition among clustering nodes. When the weighted coefficient and a similarity matching relationship follow a standard pattern, an abnormal intrusion behavior is accurately and collaboratively detected. Experimental results show that the proposed algorithm has high recognition accuracy and promising performance in the real-time detection of attacks in a Blockchain[9].

Proposed a solution where contributing parties in federated learning can be held accountable and have their model updates audited. They described a permissioned blockchain-based federated learning method where incremental updates to an anomaly detection machine learning model are chained together on the distributed ledger. By integrating federated learning with blockchain technology, our solution supports the auditing of machine learning models without the necessity to centralize the training data. Experiments with a realistic intrusion detection use case and an autoencoder for anomaly detection illustrate that the increased complexity caused by blockchain technology has a limited performance impact on the federated learning, varying between 5 and 15%, while providing full transparency over the distributed training process of the neural network. Furthermore, our blockchain-based federated learning solution can be generalized and applied to more sophisticated neural network architectures and other use cases[10].

They first discuss how anomaly detection can aid in ensuring security of blockchain based applications. They demonstrated certain fundamental evaluation metrics and key requirements that can play a critical rolewhile developing anomaly detection models for blockchain. Afterwards, they presented a thorough survey of various anomaly detection models from the perspective of each layer of blockchain. Finally, they concluded the article by highlighting certain important challenges alongside discussing how they can serve as future research directions for new researchers in the field. (Morishima, 2021) Proposed a subgraph-based anomaly detection method to perform the detection using a part of the blockchain data. The proposed structure of the subgraph is suitable for graphics processing units (GPUs) to accelerate detection by using parallel processing. In an evaluation using real Bitcoin transaction data, when the number of targeted transactions was one hundred, the proposed method was 11.1x faster than an existing GPU-based method without lowering the detection accuracy[15].

They discuss anomaly identifcation in this paper with particular reference to the Bitcoin transaction network(BTN). In this instance, anomalies behaviors is a proxy for apprehensive activity, thus our objective is to nd anomalies in the dataset in terms of their percentage. To achieve they used the feature selection method which is sequential forward feature selection along with three ML techniques, k-means clustering, isolation forest, and support vector machine (SVM) and got the highest accuracy of 98.2% in SVM as compared to all other methods. Use the enter key to start a new paragraph. The appropriate spacing and indent are automatically applied[13].

2. OVERVIEW OF BLOCKCHAIN STRUCTURE AND DESIGN

The blockchain is a type of distributed ledger. Apparent from its name, it is a chain of logically connected data blocks. A list of growing records is referred to as blocks, and each block contains a timestamp, transactional data, and a unique cryptographic hash. The hash in the block links it to the previous block in the distributed ledger, forming a chain of logical links to the first block called the genesis block using these cryptographic hashes (see Figure 1). The blockchain is a discrete design which makes it resistant to modification of the data as well as duplicate entries. Iansiti and Lakhani (2017) stated that it is an open-distributed ledger that can be utilized to document transactions between two unknown parties verifiably and permanently.

A blockchain usually uses a peer-to-peer network for seamless inter-node communication and validating new blocks[8]. Once transaction data is appended to the block, it cannot be altered retroactively without modification of all subsequent blocks. In order to alter any record, it would require a consensus of the majority of network nodes, which is highly challenging to achieve.

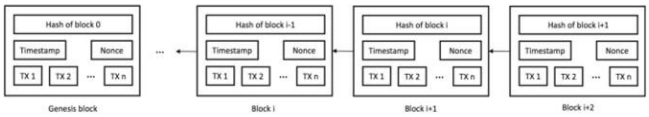

Figure 1: Example of a blockchain.

Although records of a blockchain are not immutable, it may still be considered a secure design and less prone to vulnerabilities. It also illustrates a distributed computing system with high Byzantine fault tolerance. The concepts of decentralization and the Byzantine problem will be explained later in this chapter. Raval and Siraj (2016) state that the blockchain claims to have achieved decentralized consensus.

3. BLOCKCHAIN NETWORK

The communication channel of participant network nodes is a defining aspect of blockchain networks. The most commonly used network in blockchain is the gossip peer-to-peer network. However, with the increasing need for privacy, semi-gossiping networks and simple peer-to-peer networks are also being utilized. In addition to the communication channel, a blockchain also defines its scope and protocols, which clarify its intentions as a platform. Depending on the specific applications, the scope and protocol of a blockchain may vary, ranging from a small- scale node infrastructure to a massive hub platform.

This thesis aims to propose a possible solution that can be applicable to blockchain scopes of all sizes. However, due to data availability reasons, the focus of the study is on a public blockchain.

Public Blockchain : A state-of-the-art public blockchain is characterized by being open source and permissionless, as outlined by Lin, Liao, and Lin (2017). In this context, participants are not required to obtain permission to join the network. Anyone can freely download the blockchain's source code or binaries and run it locally on their computer to validate transactions and contribute to the consensus process[14]. This open participation empowers every network participant to process and determine which new blocks will be added to the chain.

Transparency is a fundamental aspect of public blockchains. Each transaction recorded on the blockchain ledger is visible to all participants and can be accessed using a block explorer. However, while transactions are transparent, they are also anonymous, making it exceedingly difficult to trace the identity of the transaction owner. Prominent examples of public blockchains include Bitcoin, Ethereum, and Litecoin, as elucidated by Milutinović (2018)[6]. These decentralized networks enable participants to send transactions and expect their inclusion in the ledger, provided they meet the required validity criteria.

Consortium Blockchain :Consortium blockchains operate under the governance and leadership of specific groups that share a common vision, as highlighted by Lin, Liao, and Lin (2017). Unlike public blockchains, consortium blockchains do not allow unrestricted participation by anyone with internet access to verify transactions. Access to the blockchain is controlled, and the right to read the blockchain can be defined by the consortium groups, resulting in public, restricted, or hybrid access levels. Consortium blockchains are highly scalable and efficient, offering improved transactional privacy. These characteristics make them well-suited for practical applications in various industries. According to Buterin (2016), consortium blockchains can be described as "partially decentralized." Enterprises often leverage consortium blockchains for collaborative purposes. Groups of companies collaborate and utilize blockchain technology to enhance their business processes. Consortium blockchains have gained traction in industries such as healthcare, supply chain, finance, and more, as noted by Valenta and Sandner (2017). Examples of consortium blockchains include Quorum, R3 Corda, and Hyperledger.

Private Blockchain :Private blockchains are primarily developed, maintained, and centralized within organizations, as stated by Lin, Liao, and Lin (2017). Unlike public blockchains, private blockchains are not open source and are typically kept proprietary. Access permissions within private blockchains can be defined as public, restricted, or hybrid, depending on the specific system requirements.

In a closed environment, external public audits are often necessary to ensure the integrity of the system. Private blockchains leverage the technology while keeping the solution exclusive to the organization. While the centralization factor of private blockchains introduces potential security risks, it also offers distinct advantages over public blockchains. These advantages include pre- approved

network participants and known identities, allowing for increased control and trust. Notable examples of private blockchains include MONAX and Multichain, as mentioned by Sajana, Sindhu, and Sethumadhavan (2018)[13].

4. BLOCKCHAIN SECURITY

The fundamental concept of blockchain security revolves around enabling secure and tamper-proof sharing of valuable information, particularly among individuals or entities that lack trust in one another. Through sophisticated decentralized storage and consensus algorithms, the blockchain system becomes highly resilient against manipulation attempts by attackers. Encryption plays a crucial role in ensuring the integrity and confidentiality of data, validating the communication channels within the network.

In addition to data security, blockchain technology also aims to address the problem of Byzantine agreement. Byzantine agreement refers to establishing trust and dependability within the system, especially in the event of failures or malicious actors[12]. By utilizing consensus mechanisms and distributed validation processes, blockchain seeks to provide a reliable and resilient framework.

The combination of encryption, decentralized storage, consensus algorithms, and Byzantine agreement mechanisms enhances the overall security of the blockchain, enabling trustworthy and transparent information sharing in a decentralized manner.

Centralized data storage poses significant risks, making it vulnerable to various threats. However, blockchain technology mitigates these risks by adopting a decentralized approach to data storage on a peer-to-peer network. The distributed nature of the network makes it challenging to exploit vulnerabilities, as there are no centralized points of failure. By storing data in a decentralized manner, blockchain ensures that there is no single point of failure in the system[3]. As Brito and Castillo (2013) explain, blockchain utilizes cryptographic public-private keys for secure communication among network nodes, ensuring privacy and security. The usage of private keys for encryption and public keys for decryption enhances the overall security of the blockchain system.

The Economist (2015) highlights that data stored on the blockchain is generally incorruptible. Decentralization plays a vital role in ensuring data quality, as there is no official, centralized copy of a record. Instead, each node in the network maintains a copy, and the trust among nodes is at an equal level.

The Byzantine problem, as originally described by Lamport, Shostak, and Pease (1982), raises the concern that in a decentralized network, computers cannot be entirely certain that they are consistently displaying the same data. Due to the unreliability of network nodes, there is no guarantee that the data communicated by one node has reached its intended destination. The essence of the Byzantine problem lies in achieving consensus across a distributed network of nodes, even in the presence of potentially faulty or malicious nodes. Byzantine nodes, in particular, pose a significant challenge as they can mislead other nodes and provide corrupted information during the consensus process. Blockchain technology must operate robustly in such situations and reach consensus despite the interference of these Byzantine nodes. While it is impossible to fully solve the Byzantine problem, different blockchains and distributed ledgers employ various consensus mechanisms, such as proof of work and proof of stake, to address the problem in a probabilistic manner.

Consensus mechanisms play a crucial role in achieving agreement among network nodes, allowing them to validate transactions and reach a shared view of the blockchain state. These mechanisms provide incentives for honest participation and disincentives for malicious behavior, increasing the overall security and reliability of the blockchain network.

5. ANOMALY DETECTION

Anomaly detection, as described by Zimek and Schubert (2017), involves identifying unique items, observations, or events that raise suspicion due to their significant deviation from the majority of the data. These anomalies can manifest as abnormalities such as credit card fraud, structural defects, or errors in text. They can also be characterized as noise, outliers, or novelties[13]. However, Pedregosa et al. (2011) emphasize the distinction between outlier detection and novelty detection. In novelty detection, the training data is not contaminated by outliers, and the goal is to detect whether a newly introduced observation is abnormal for the system. On the other hand, outlier detection involves training data that contains outliers, which are observations that deviate significantly from the rest.

This thesis focuses on the detection of anomalies in blockchain data structures. Irrespective of the specific domain of the blockchain, specific techniques can be applied to this data structure to identify anomalies. Anomaly detection in blockchain poses an unsupervised learning problem, and the data in such cases is often highly imbalanced. Given the availability of data and existing academic literature, this thesis leverages a public financial blockchain, namely Bitcoin, for analysis. Bitcoin's transactional data undergoes rigorous preprocessing, followed by the application of various modeling methods to identify transactions associated with theft, heists, or money laundering. Through a comprehensive evaluation process, the thesis aims to identify the optimal solution by comparing different models.

While previous studies have explored anomaly detection in similar contexts, this thesis seeks to approach the problem of blockchain anomaly detection in a generalized manner. Moreover, it proposes the utilization of cutting-edge machine learning algorithms in conjunction with graph theory to analyze anomalies within blockchain data in an innovative and advanced manner.

6. CYBER FRAUD AS A PROBLEM

In recent decades, the prevalence of computer-oriented crimes has experienced a significant surge, highlighting the critical importance of digital security across all domains. Sandle and Char (2014) released a report estimating an annual damage of 445 billion USD to the global economy as a result of these crimes. Smith (2015) further projected that cybercrime costs could escalate to as high as 2.1 trillion USD by 2019[3]. A report by North-Denver-News (2015) highlighted that approximately 1.2 billion USD was lost to financial credit card fraud in the United States alone in 2012. Additionally, the European-Central-Bank (2014) revealed that 1 EUR out of every 2,635 EUR spent on debit and credit cards was lost to fraud.

While cybercrimes encompass various categories such as cyberterrorism, cyberextortion, cyberwarfare, and financial fraud crimes, this thesis primarily focuses on the financial domain. It recognizes the significant impact and potential threats posed by financial cybercrimes and aims to address them comprehensively. Among various domains, the financial sector remains highly susceptible to cyber crimes, posing significant threats to both users and systems. Security breaches and hacks often exploit vulnerabilities in user practices and system weaknesses. While the advent of blockchain technology has significantly reduced risks, many financial systems remain hesitant to embrace the upgrade due to internal policies and bureaucratic hurdles. Consequently, the financial industry continues to suffer substantial losses each year.

One prevalent form of cyber fraud in the financial sector is credit card fraud, which occurs globally. Although artificial intelligence has played a crucial role in detecting such fraud, a considerable number of hackers still evade capture. For instance, Krebs (2013) reported a hack on Adobe Systems that compromised around 40 million sets of payment card data, including encrypted card payment numbers, customer names, card expiration dates, and other related information. In another case, McCurry (2016) described a coordinated attack by 100 individuals who utilized the data of 1,600 South African credit cards to steal 12.7 million USD from 1,400 stores within a mere three hours. The perpetrators managed to escape from Japan before authorities even discovered the heist[11]. Despite the implementation of various security measures to safeguard credit and debit cards, these incidents demonstrate that centralized systems are still vulnerable, thereby exposing the entire financial industry to considerable risk.

Blockchains are often touted for their ability to bring privacy and security to financial systems. However, there have been instances where individuals have managed to exploit this supposedly unbreakable infrastructure[12]. These hackers aim to engage in illegal activities while avoiding detection, either by covering their tracks or by deceiving the system into believing their actions are legitimate. While many small to medium- scale cases may go unreported, larger incidents can make headlines.

Bitcoin, being the first and oldest financial blockchain, has faced its fair share of challenges related to illegal activities. One notable example is the Bitcoin theft known as "All In Vain," described by Reid and Harrigan (2011), where approximately 25,000 bitcoins were stolen. The visual representation of the theft patterns, as shown in Figure 2, illustrates the involvement of a hacker (represented by the red node) and the victim (represented by the green node). The theft began with the initial pilfering of a single bitcoin, which eventually escalated to the heist of 25,000 bitcoins. As depicted in Figure 6.1, the hacker attempted to conceal their illicit activities by employing multiple small transactions to taint the stolen bitcoins[6]. Additionally, a victim named Stone- Man (2010) shared his loss on a bitcoin forum, reporting the robbery of 8,999 bitcoins through the unauthorized use of his original private key.

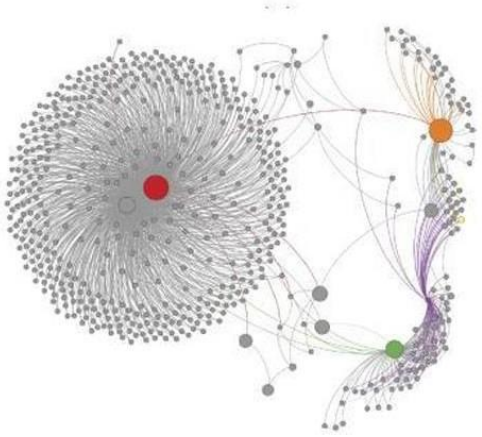

Figure 2: All in vain robbery network.

In Stone-Man's case, he had initially purchased 9,000 bitcoins from an exchange. He subsequently transferred these bitcoins to a physical disc and also created a backup on a USB flash drive. As part of an unknown transaction, he sent a single bitcoin to another address under his control.

After confirming and backing up all the wallet data, he later discovered an unrecognized transaction involving 8,999 bitcoins being sent to an unknown address without his approval. These incidents highlight the challenges and vulnerabilities that can exist within blockchain-based financial systems, emphasizing the need for robust security measures and constant vigilance to mitigate the risk of illegal activities and protect users' assets.

7. CONCLUSION

Evaluation of multiple unsupervised algorithms for detecting anomalous behavior in an unspent transaction output (UTXO) based blockchain has shown promising results in identifying malicious activities. This aligns with existing research on anomaly detection in blockchains, although the comparison with previous studies would have been more apparent if their evaluation metrics had been disclosed. It is important to note that while credit card fraud detection can provide some indirect comparison, the dynamics and characteristics of blockchain data present unique and complex challenges.

One limitation of the evaluation is the scarcity of malicious transactional data points in the dataset, which limits the ability to recognize anomalous patterns. To address this issue, synthetic generation of malicious data points was attempted while ensuring it was not excessive. However, this approach may have affected the quality of anomaly detection, resulting in weaker performance of the models[11]. The selection of relevant features extracted from the blockchain transaction graph is a critical factor in determining anomalous behavior. Certain variables may hold unique insights, and considering the problem as a time- series issue could reveal different solutions. However, this particular research focused on detecting anomalous patterns using unsupervised learning techniques, and incorporating a time-series element would have increased the complexity of the scope.

Researchers have explored various unsupervised techniques to detect anomalous transactions in blockchains and have achieved some level of success. However, the challenges arise from the lack of relevant data, limitations of computing power, and the handling capabilities of the algorithms, all of which contribute to the complexity of the problem. The future improvement of anomaly detection in blockchains relies on several factors. Availability of relevant and comprehensive data, advancements in feature engineering, and exploring alternative perspectives such as time-series or network analysis can unlock new potential solutions. Furthermore, leveraging distributed computing can enhance the computing capabilities of algorithms and enable more sophisticated analysis. Overall, while there are challenges to overcome, the field of anomaly detection in blockchains holds promise for improvement in the future through advancements in data availability, feature capabilities.

REFERENCES

[1] Sayadi S, Rejeb S, Choukair Z, "**Anomaly detection model over blockchain electronic transactions**,"2019 15thInternational Wireless Communications and Mobile Computing Conference.

[2] Dey, Somdip, **Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory: A Proof of Work** 2018 10th Computer Science and Electronic Engineering Conference, CEEC 2018

[3] Shen M, Tang X, Guizani M **Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities**, […], IEEE Internet of Things Journal (2019) 6(5)

[4] Huang J, Kong L, Zeng P **Blockchain-Based Mobile Crowd Sensing in Industrial Systems**, […],IEEE Transactions onIndustrial Informatics (2020) 16(10)

[5] Keshk M, Turnbull B, Choo K **A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks**[…],IEEE Transactions on Industrial Informatics (2020) 16(8)

[6] Hu T, Liu X, Liu Y **Transaction-based classification and detection approach for Ethereum smart contract**[…],Information Processing and Management (2021) 58(2)

[7] Kumar P, Kumar R, Xiong N **PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-DrivenSmart Cities** […],IEEE Transactions on Network Science and Engineering (2021) 8(3)

[8] Cui L, Qu Y, Yu S **Security and Privacy-Enhanced Federated Learning for Anomaly Detection in IoT Infrastructures**,[…],IEEE Transactions on Industrial Informatics (2022) 18(5)

[9] Liang W, Xiao L, Li K **Data Fusion Approach for Collaborative Anomaly Intrusion Detection in Blockchain- Based Systems**, […],IEEE Internet of Things Journal (2022) 9(16)

[10] Preuveneers D,Rimmer V, Ilie-Zudor E **Chained anomaly detection models for federated learning: An intrusion detection case study**, […],Applied Sciences (Switzerland) (2018) 8(12

[11] Morishima S **Scalable anomaly detection in blockchain using graphics processing unit** ,Computers and Electrical Engineering (2021) 92

[12] Singh P, Agrawal D, Pandey S **Anomaly detection and analysis in blockchain systems** ,(2023)

[13] Arthur, David and Sergei Vassilvitskii (2007). **k-means++: The advantages of careful seeding**. In: Proceedings of the eighteenth annual ACM-SIAM symposium on Discrete algorithms. Society for Industrial and Applied Mathematics, pp. 1027–1035.

[14] Bayer, Dave, Stuart Haber, and W Scott Stornetta (1993). Improving the efficiency and reliability of digital time- stamping. In: Sequences II. Springer, pp. 329–334

[15] Bentley, Jon Louis (1975). **Multidimensional binary search trees used for associative searching**.. [Online; accessed 7- September-2019