
# A Proposed Blockchain based System for Secure Data Management of Computer Networks

**Taif Khalid Shakir[1], Rabah Scharif[2], Manal M. Nasir[3,*]**

[1] College de Paris, France

[2]Applied Engineering Department, Institute of Applied Technology, UAE

[3] Gwinnett Technical College, 5150 Sugarloaf Pkwy, Lawrenceville, GA 30043, USA

Emails: taif.shakir@cabling.att-mail.com; rabah.scharif@aths.ac.ae; mnasir@gwinnetttech.edu

**Abstract**

As technology continues to evolve, the importance of information security and management becomes more crucial than ever. Blockchain and machine learning (ML) are two technologies that are gaining increasing attention in this field. Blockchain provides a secure and decentralized platform for storing and sharing information, while ML can help detect patterns and anomalies in data to identify potential security threats. This paper proposes a blockchain-based ML system for securing information management by providing an automated service for detecting anomalies in Ethereum transactions. The system utilizes a blockchain network to securely store and manage data, and ML algorithms to analyze and detect potential security threats. We present a case study using the Ethereum Fraud Detection Dataset to demonstrate the effectiveness of our proposed system in detecting fraudulent transactions. Our results show that our system outperforms traditional ML algorithms in terms of accuracy (99.55%), and F1-score (99.98%), highlighting the potential of blockchain-based ML for improving information security and management in various industries.

**Keywords:** Blockchain; Security; Machine Learning; Big data; Secure Networks

## 1. Introduction

Information security and management are critical aspects of any organization, especially in the digital age where most operations rely on technology. Information security refers to the protection of information and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing various strategies, policies, and technologies to safeguard sensitive information from potential threats such as cyber-attacks, data breaches, and identity theft [1]. Effective information security not only protects an organization's confidential data but also ensures the continuity of operations and builds trust with customers and stakeholders [2].

On the other hand, information management refers to the process of collecting, organizing, storing, retrieving, and disseminating information within an organization. The primary goal of information management is to provide the right information to the right people at the right time, enabling them to make informed decisions [3-4]. Effective information management involves identifying and categorizing information, determining its value, and ensuring that it is appropriately stored and secured. Information management plays a crucial role in supporting organizational operations, improving efficiency and productivity, and facilitating decision-making processes. Effective information security and management are essential for organizations to achieve their strategic objectives and maintain a competitive edge in the marketplace [5-8].



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

Blockchain technology is increasingly being recognized as a powerful tool for information management and security. At its core, a blockchain is a decentralized, distributed ledger that records transactions or data in a secure, tamper-proof manner. This means that once information is entered into the blockchain, it cannot be altered or deleted without the agreement of all participants in the network. This makes blockchain technology an ideal solution for managing sensitive information, such as financial data or personal information, as it provides a high level of security and transparency [9-12].

Blockchain technology also allows for the creation of smart contracts, which are self-executing contracts that automatically enforce the terms of an agreement. This has important implications for information management, as it enables organizations to automate complex business processes and reduce the need for intermediaries or third-party verification. Furthermore, blockchain technology provides a secure and transparent way to track the provenance of data, enabling organizations to verify the authenticity and accuracy of information [12-17].

This work proposes a novel approach that combines blockchain technology with ML for enhancing information management through the automated detection of anomalous transactions. We present a case study using the Ethereum Fraud Detection Dataset to demonstrate the effectiveness of our proposed system in detecting fraudulent transactions, which is used to experimentally evaluate and validate the effectiveness of the proposed approach.

## 2. Related Work

The emergence of blockchain technology has brought about significant changes to information security and management practices. As a result, there has been a growing interest in exploring the potential of blockchain technology in enhancing information security and management practices. A literature study on the topic would be an excellent way to gather insights and understand the current state of knowledge in this area. In [9], the authors explored the use of blockchain technology to secure and protect data collected by Unmanned Aerial Vehicles (UAVs). They outlined the challenges associated with securing UAV data and proposed a blockchain-based solution to overcome these challenges. The proposed solution involves using a permissioned blockchain network to store and manage UAV data, ensuring that it remains secure and tamper-proof. In [10], the authors presented a comprehensive survey of the potential of blockchain technology to enhance security in the Internet of Things (IoT) ecosystem. This included an overview of the fundamental concepts of blockchain technology and how it can be applied to address the security challenges of IoT. They also examined various use cases of blockchain technology in the context of IoT security, including device authentication, data integrity, and access control. In [12], the authors explored the security and scalability challenges faced by the blockchain technology behind Bitcoin. They analyzed the security of the blockchain against potential attacks, such as double-spending attacks, and examined the scalability limitations of the blockchain in terms of its transaction processing capacity. They proposed several solutions to address these challenges, including the use of off-chain transactions and the adoption of new consensus mechanisms. Additionally, they examined the trade-offs between security and scalability in the Bitcoin blockchain and provided insights into the design choices made in the development of the blockchain. In [13], the authors examined the potential of blockchain technology in addressing the challenges posed by the COVID-19 pandemic. They identified various use cases for blockchain technology, including contact tracing, supply chain management, and health data management. They provided an overview of the benefits of using blockchain technology in these areas, including increased transparency, data security, and privacy. In [14], the authors argued for the potential of blockchain technology to transform the traditional concept of government and public infrastructure. They proposed the concept of a "blockchain government" that would be built on a decentralized, trustless system that is transparent, secure, and efficient. They argued that a blockchain government would lead to greater transparency and accountability, reduced corruption, and improved citizen participation. In [15], they investigated the potential of blockchain technology to enhance the security and performance of smart grid systems. They identify the key security challenges facing smart grid systems, including the vulnerability of centralized systems to cyber-attacks, and propose the use of blockchain technology as a potential solution. In [16], the authors studied the potential of blockchain technology to address the security challenges facing the IoT. They identified the key security challenges facing IoT systems, including device authentication, data privacy, and data integrity, and propose the use of blockchain technology as a potential solution. They also examined various use cases of blockchain technology in the context of IoT, including supply chain management and healthcare. In [17], the authors proposed a framework for assessing the security of blockchain technology in public sector applications, in which they used the security triad model, which includes confidentiality, integrity, and availability, to evaluate the potential security benefits and challenges of using blockchain technology in public sector applications. They then applied the security triad model to various use cases of blockchain technology in the public sector, including voting and identity management. In [18], the authors provided an overview



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

of the security and privacy challenges associated with blockchain technology, and its underlying principles, including decentralization and immutability. They then explored the security implications of blockchain technology, including the potential for 51% attacks and the need for secure key management. In [20], the paper discussed the potential impact of blockchain technology on various industries, including finance, healthcare, and supply chain management. They then explored the potential applications of blockchain technology in various industries, including the use of smart contracts in supply chain management, and the potential for blockchain technology to improve the security and efficiency of financial transactions. In [22], they proposed a blockchain-based solution for secure and efficient key management in intelligent transportation systems (ITS). They proposed a blockchain-based dynamic key management system that can efficiently distribute and revoke keys while ensuring security and privacy. The system used smart contracts to automate the key management process and uses a blockchain to store and distribute keys securely.

## 3. The used Methodology

This section presents the methodology of the proposed system, which is composed of two main building blocks namely ML classifier and blockchain. The later component initiates transactions, and then the ML classifier is applied to oversee categorizing the transactions as mischievous or lawful. The main objective of our model is to take advantage of the technologies to empower the security of information management by offering a highly accurate anomaly detection service that allows the automatic identification of unusual suspicious events that are different from most of the data. A case study of Bitcoin transactions is adopted in this study to train and evaluate our solution. In the following sections, we explore the main steps involved in our system.

### A. Data Rebalance

Class imbalance is a common problem in ML where the number of samples in each class is not balanced, i.e., one class has significantly fewer samples than the other. In the case of the Ethereum blockchain anomaly dataset, most of the samples are labeled as non-fraudulent, and only a small portion of the samples are labeled as fraudulent. This class imbalance can negatively affect the performance of ML models trained on this dataset, as they tend to be biased towards the majority class, leading to low recall and high false-negative rates for the minority class. To address this issue, the Synthetic Minority Over-sampling Technique (SMOTE) can be used. SMOTE is an oversampling technique that generates synthetic samples of the minority class by creating new samples by interpolating between existing samples of the minority class. This technique helps to balance the class distribution, improving the performance of ML models by reducing the bias towards the majority class. In our case study, SMOTE is applied to increase the number of samples for the minority class, i.e., the fraudulent transactions. By generating synthetic samples, the number of samples in the minority class can be increased to a level that is closer to the majority class, resulting in a more balanced dataset. This can lead to better performance of machine learning models trained on this dataset, as they can learn to distinguish fraudulent transactions more accurately, leading to improved precision and recall rates. The implementation steps of SMOTE are summarized in Algorithm 1.

**Algorithm 1:** Data balancing through SMOTE

**Inputs:** Minor class samples, with $i\ in\ \{1, 2, 3, \cdots, D\}$
**Outputs:** Artificial data $S$
4: Amount of minority data, $D$.
5: Proportion of SMOTE, $P$.
6: The count of adjoining neighbors, $K$.
7: **for** $n$ from 1 to $D$ **do**
8: Get $K$ adjoining neighbors of instance $D_i$
9: Validate that $\hat{P} = \frac{P}{100}$
10: **While** $\hat{P}! = 0$ **do**
11: Choose an arbitrary sample $m$ from minority class
12: Locate neighbors for $m$
13: Choose an arbitrary number $\alpha \in [0,1]$
14: $\hat{m} = m_i + \alpha(\hat{m} - m_i)$
15: Loop till $\hat{m}$ added to S
16: Validate that $\hat{P} = P - 1$
17: **end loop**



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

18: **end loop**
19: **End**

B. ML Model for blockchain anomaly detection

When it comes to Ethereum anomaly detection in blockchain, our system apply Catboost as a powerful ML algorithm that is specifically designed for handling categorical variables in datasets. It is an open-source gradient boosting (GB) approach that can be used for classification. The GB is defined as the follows:

$$\frac{\sum_{j=1}^{p} [x_{j,k} = x_{i,k}]Y_i}{\sum_{j=1}^{p} [x_{j,k} = x_{i,k}]}. \quad (1)$$

Catboost is highly effective in dealing with imbalanced data and can handle large datasets efficiently. This can be highly beneficial in detecting fraudulent transactions in the blockchain network. It can handle the high-dimensional and categorical data of Ethereum transactions and identify the patterns of fraudulent activities by considering the interaction between the variables.

With Ethereum blockchain anomaly dataset $D = \{(x_k, y_k)\}_{k=1}^{n}$, in which $x_k = \left(x_k^1, \dots, x_k^{d'}\right)$ and $y_k$ denote feature vector and label. The symmetrical decision trees are assembled by recursively separating the whole attribute space. Given that the attribute space of CatBoost is partitioned into $J$ separate nodes, each with a value $b_j$. The tree $h$ is expressed as a projected value of all states:

$$h(x) = \sum_{j=1}^{J} b_j f_{\{x \in R_j\}}, \quad (2)$$

The above $f_{\{x \in R_j\}}$ designate and marker function:

$$f_{\{x \in R_j\}} = \begin{cases} 1 & if \quad x \in R_j \\ 0 & otherwise \end{cases} \quad (3)$$

Then, GP is applied as a chain of estimated functions to reduce the expected cost in a greedy way:

$$F^t = F^{t-1} + \alpha h^t \quad (4)$$

$$h^t = \text{argmin}_{h \in H} \mathcal{L}(F^{t-1} + h) \quad (5)$$

The cost function is designed with the least-squares function:

$$h^t = \text{argmin}_{h \in H} \mathbb{E}\left(-g^t(x, y) - h(x)\right)^2 \quad (6)$$

The learning process of CATBoost for anomaly detection is summarized in Algorithm 2.

**Algorithm 2: Training Catboost for Anomaly Detection**

**Inputs:** Preprocess dataset $S$
**Outputs:** Blockchain Transactions $chain$

1: Split $S$ into train and test set
2: $X_{train} \leftarrow$ training samples
3: $Y_{train} \leftarrow$ training labels
4: $X_{test} \leftarrow$ testing samples
5: $Y_{test} \leftarrow$ testing labels
6: $\boldsymbol{\mathcal{M}}$ = **Catboost** ($layers = 6$)
7: $\boldsymbol{\mathcal{M}}$ = $\boldsymbol{\mathcal{M}}$.fit($X_{train}$, $Y_{train}$)
8: $Y_{pred}$ = $\boldsymbol{\mathcal{M}}$.predict ($X_{test}$)
9: Preds = [round ($p$) for $p$ in $Y_{pred}$]
10: **if** Preds==0 **then:**
11: trans=real



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

```
    chain.add (trans)
else if Preds==1 then
    trans=anomalous
end if
return chain
End
```

## 4. Results and Analysis

As a case study of this work, the Ethereum Fraud Detection (EFD) dataset is used, which was created by researchers from the University of Texas at Austin and the University of California, Riverside. This dataset consists of over 11,000 Ethereum transactions from January 2018 to October 2018, including both legitimate transactions and fraudulent ones. The dataset includes information on the amount of Ether (the cryptocurrency used on the Ethereum network) involved in each transaction, the timestamp of the transaction, and various other features that can be used for analysis and modeling. One notable feature of the EFD dataset is that it includes information on the addresses involved in each transaction, which can be used to identify patterns of fraudulent behavior across different transactions. For example, researchers have used the EFD dataset to identify clusters of fraudulent addresses that are linked to specific types of fraud. The dataset is composed of 49 attributes and a label [23-25].

Descriptive statistical analysis is applied here as a critical step in understanding the characteristics and trends of the blockchain transaction dataset in our system. By performing descriptive statistical analysis, we can gain insights into the central tendency, variability, distribution, and other characteristics of the data (See Table 1). We can use descriptive statistics to understand the distribution of transaction values, the frequency of transactions, the number of unique addresses, and other features of the dataset.

Table 1: Descriptive statistics of the ETHEREUM transactions

| | count | mean | std | min | 25% | 50% | 75% | max |
|---|---|---|---|---|---|---|---|---|
| FLAG | 9841 | 0.22 | 0.42 | 0 | 0 | 0 | 0 | 1 |
| Avg min between sent tnx | 9841 | 5086.88 | 21486.55 | 0 | 0 | 17.34 | 565.47 | 430287.7 |
| Avg min between received tnx | 9841 | 8004.85 | 23081.71 | 0 | 0 | 509.77 | 5480.39 | 482175.5 |
| Time Diff between first and last (Mins) | 9.84E+03 | 218333.30 | 322937.90 | 0.00E+00 | 3.17E+02 | 4.66E+04 | 3.04E+05 | 1.95E+06 |
| Sent tnx | 9841 | 115.93 | 757.23 | 0 | 1 | 3 | 11 | 10000 |
| Received Tnx | 9841 | 163.70 | 940.84 | 0 | 1 | 4 | 27 | 10000 |
| Number of Created Contracts | 9841 | 3.73 | 141.45 | 0 | 0 | 0 | 0 | 9995 |
| Unique Received From Addresses | 9841 | 30.36 | 298.62 | 0 | 1 | 2 | 5 | 9999 |
| Unique Sent To Addresses | 9841 | 25.84 | 263.82 | 0 | 1 | 2 | 3 | 9287 |
| min value received | 9841 | 43.85 | 325.93 | 0 | 0.001 | 0.095856 | 2 | 10000 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... |
| ERC20 max val rec | 9.01E+03 | 125252400.00 | 10537410000.00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 9.90E+01 | 1.00E+12 |



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ERC20 avg val rec | 9.01E+03 | 4346203.00 | 214119200.00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 2.95E+01 | 1.72E+10 |
| ERC20 min val sent | 9.01E+03 | 11741.26 | 1053567.00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 1.00E+08 |
| ERC20 max val sent | 9.01E+03 | 13035940.00 | 1179905000.00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 1.12E+11 |
| ERC20 avg val sent | 9.01E+03 | 6318389.00 | 591476400.00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 5.61E+10 |
| ERC20 min val sent contract | 9012 | 0.00 | 0.00 | 0 | 0 | 0 | 0 | 0 |
| ERC20 max val sent the contract | 9012 | 0.00 | 0.00 | 0 | 0 | 0 | 0 | 0 |
| ERC20 avg val sent the contract | 9012 | 0.00 | 0.00 | 0 | 0 | 0 | 0 | 0 |
| ERC20 uniq sent token name | 9012 | 1.38 | 6.74 | 0 | 0 | 0 | 0 | 213 |
| ERC20 uniq rec token name | 9012 | 4.83 | 16.68 | 0 | 0 | 1 | 2 | 737 |



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

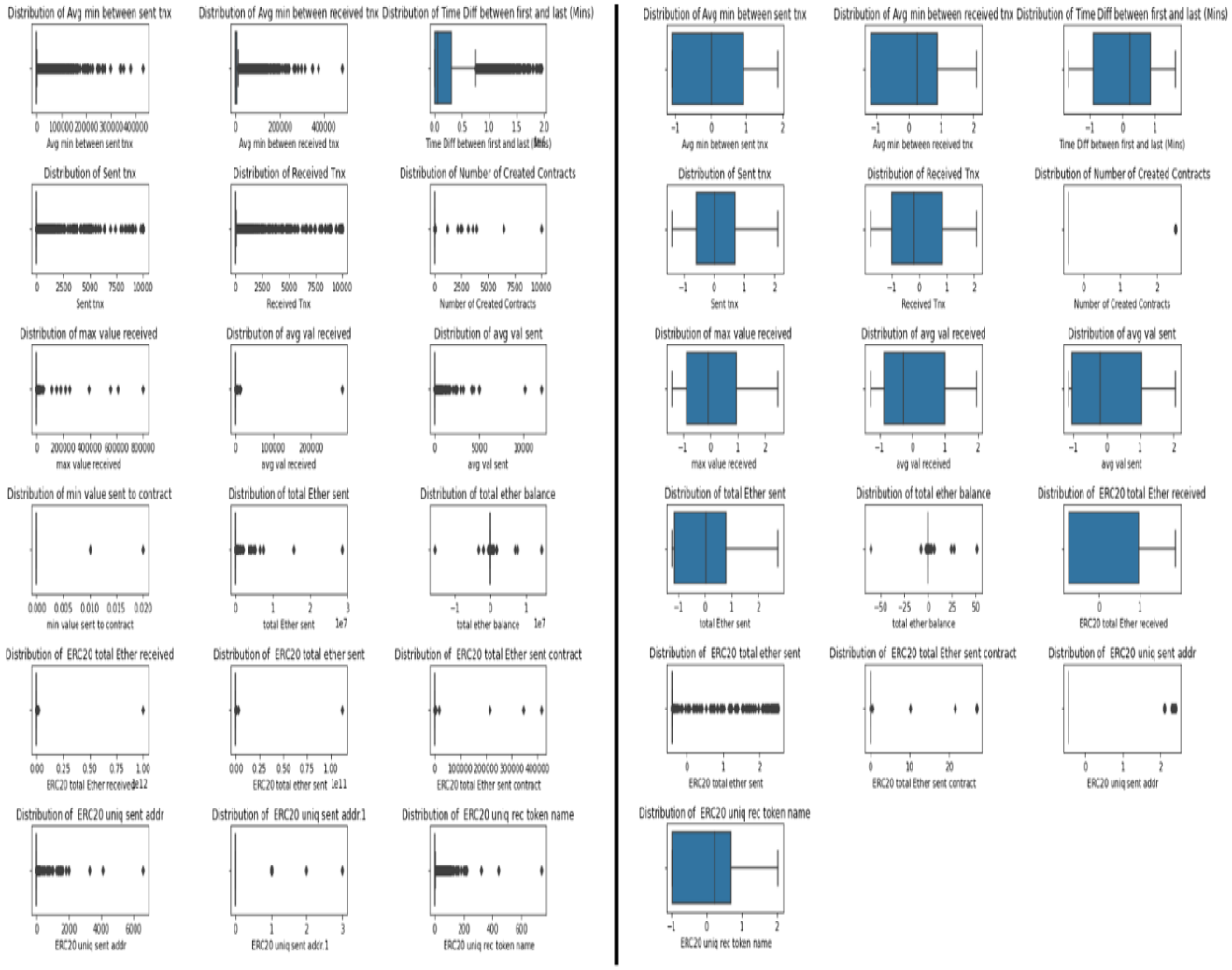


Figure 1: Visualization of features before and after normalization.



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

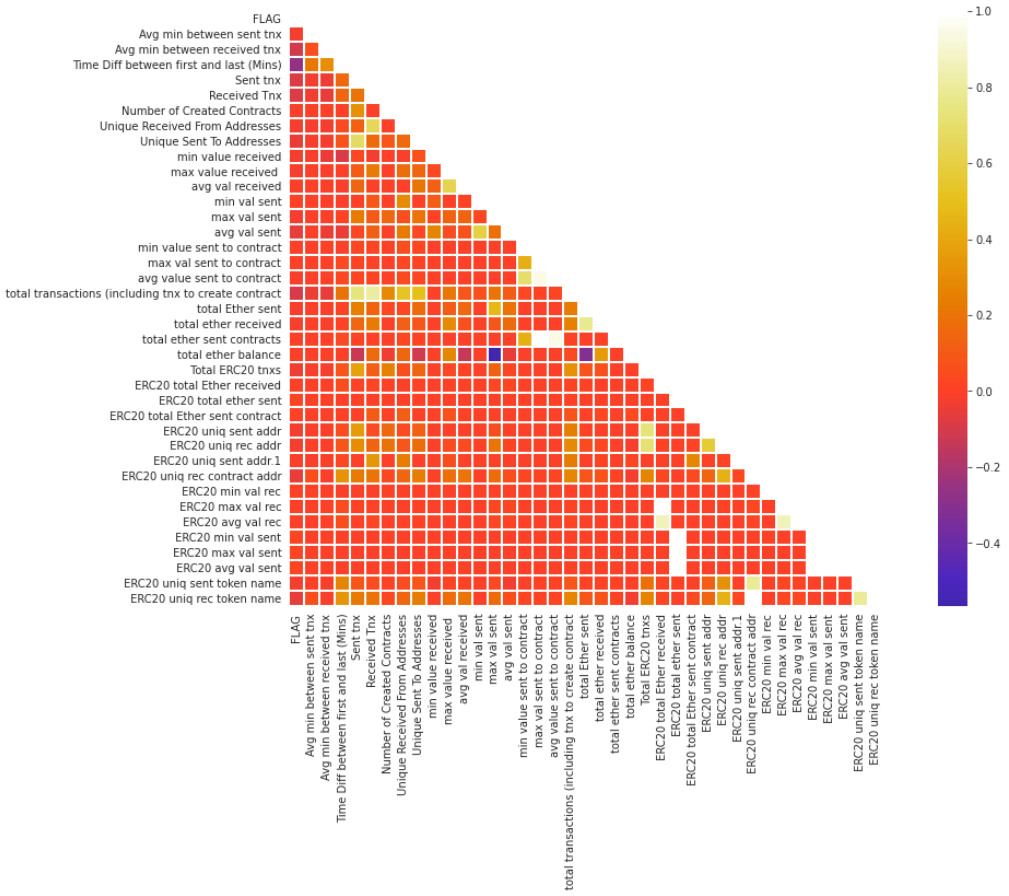


Figure 2: Correlation analysis for the ETHEREUM transactions data.

According to the above statistics, the data is prepared by dropping features with Variance=0. Then, we investigate the feature distribution with box plots in the left part of Fig .1, and it could be noted that we got a small feature with a small distribution. Hence, we prepare the dataset by applying the log transformation, where the distribution of features is displayed in the right part of Fig. 1. Correlation analysis displayed in Fig. 2 has an important role in understanding the relationship between different variables in a blockchain transaction dataset. With the visualized correlation coefficients between pairs of variables, we can identify how strongly and in what direction they are related. Accordingly, we drop some of those highly correlated features.

Experimental comparative analysis is conducted on blockchain transaction datasets to help us identify the best-performing algorithm for a specific use case. Table 2 presents the numerical results of competing methods across different metrics of performance as accuracy, precision, recall, and F1 score. It is important to note that the legacy ML algorithms have the lowest detection performance. Comparatively, the tree-based ML algorithms attain more improved performance (F1-score: 97%-99%). Remarkably, the proposed model achieved the best detection performance overcoming all the competing methods.



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

Table 2: Comparisons between the performance of the proposed model against competing ML algorithms.

| Model | Accuracy | AUC | Recall | Prec. | F1 | Kappa | MCC |
|---|---|---|---|---|---|---|---|
| **Ada Boost** | 99.36 | 99.91 | 98.17 | 98.94 | 98.55 | 98.14 | 98.14 |
| **CatBoost** | **99.55** | **99.98** | **98.23** | **99.73** | **98.98** | **98.69** | **98.69** |
| **Decision Tree** | 98.74 | 98.3 | 97.51 | 96.84 | 97.16 | 96.35 | 96.36 |
| **Extra Trees** | 99.03 | 99.95 | 97.18 | 99.8 | 98.47 | 98.04 | 98.06 |
| **Extreme gradient Boosting** | 98.43 | 99.96 | 98.23 | 99.21 | 98.72 | 98.35 | 98.36 |
| **Gradient Boosting** | 99.29 | 99.96 | 97.84 | 98.95 | 98.38 | 97.93 | 97.93 |
| **K Neighbors Classifier** | 91.48 | 93.35 | 76.92 | 83.35 | 79.98 | 74.58 | 74.7 |
| **Light Gradient Boosting Machine** | 99.09 | 99.96 | 98.36 | 99.34 | 98.85 | 98.52 | 98.53 |
| **Linear Discriminant Analysis** | 89.94 | 95.99 | 55.55 | 98.28 | 70.91 | 65.4 | 69.33 |
| **Logistic Regression** | 79.88 | 64.51 | 9.39 | 64.64 | 15.59 | 13 | 19.79 |
| **Naive Bayes** | 23.97 | 46.12 | 99.87 | 22.55 | 36.78 | 1.03 | 6.49 |
| **Quadratic Discriminant Analysis** | 39.24 | 60.95 | 97.11 | 26.35 | 41.45 | 10.16 | 21.33 |
| **Random Forest Classifier** | 98.33 | 99.91 | 97.05 | 99.93 | 98.47 | 98.04 | 98.06 |
| **Ridge Classifier** | 89.94 | 92.3 | 55.42 | 98.49 | 70.86 | 65.36 | 69.34 |

## 5. Conclusion

This paper investigates a hybrid approach to Information Security and Management using blockchain-based Machine Learning. The proposed approach demonstrated promising results in detecting fraudulent transactions in the Ethereum blockchain dataset, showcasing the effectiveness of using blockchain technology and machine learning algorithms together. The study also demonstrated the importance of data preprocessing and feature engineering in improving the performance of machine learning models. Furthermore, this paper discussed the role of descriptive statistics, correlation analysis, and comparative analysis in evaluating the performance of our models. The system compared with various ML algorithms included, and the results showed that Catboost outperformed the other algorithms with an accuracy of 99.55%.

## References

[1] Zubaydi, Haider Dhia, Yung-Wey Chong, Kwangman Ko, Sabri M. Hanshi, and Shankar Karuppayah. "A review on the role of blockchain technology in the healthcare domain." *Electronics* 8, no. 6 (2019): 679.

[2] Si, Haiping, Changxia Sun, Yanling Li, Hongbo Qiao, and Lei Shi. "IoT information sharing security mechanism based on blockchain technology." *Future generation computer systems* 101 (2019): 1028-1040.

[3] Tse, Daniel, Bowen Zhang, Yuchen Yang, Chenli Cheng, and Haoran Mu. "Blockchain application in food supply information security." In *2017 IEEE international conference on industrial engineering and engineering management (IEEM)*, pp. 1357-1361. IEEE, 2017.

[4] Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of financial and cyber security." In *2016 2nd international conference on contemporary computing and informatics (IC3I)*, pp. 463-467. IEEE, 2016.



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

[5] Abu-Elezz, Israa, Asma Hassan, Anjanarani Nazeemudeen, Mowafa Househ, and Alaa Abd-Alrazaq. "The benefits and threats of blockchain technology in healthcare: A scoping review." *International Journal of Medical Informatics* 142 (2020): 104246.

[6] Chattu, Vijay Kumar, Anjali Nanda, Soosanna Kumary Chattu, Syed Manzoor Kadri, and Andy W. Knight. "The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security." *Big Data and Cognitive Computing* 3, no. 2 (2019): 25.

[7] Sunarya, Po Abas, Untung Rahardja, Lusyani Sunarya, and Marviola Hardini. "The Role Of Blockchain As A Security Support For Student Profiles In Technology Education Systems." *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan* 4, no. 2 (2020): 203-207.

[8] Shrier, David, Weige Wu, and Alex Pentland. "Blockchain & infrastructure (identity, data security)." *Massachusetts Institute of Technology-Connection Science* 1, no. 3 (2016): 1-19.

[9] Ch, Rupa, Gautam Srivastava, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, and Sweta Bhattacharya. "Security and privacy of UAV data using blockchain technology." *Journal of Information security and Applications* 55 (2020): 102670.

[10] Alkurdi, Fahad, Ibrahim Elgendi, Kumudu S. Munasinghe, Dharmendra Sharma, and Abbas Jamalipour. "Blockchain in IoT security: a survey." In *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1-4. IEEE, 2018.

[11] Mingxiao, Du, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. "A review on consensus algorithm of blockchain." In *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, pp. 2567-2572. IEEE, 2017.

[12] Karame, Ghassan. "On the security and scalability of bitcoin's blockchain." In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 1861-1862. 2016.

[13] Kalla, Anshuman, Tharaka Hewa, Raaj Anand Mishra, Mika Ylianttila, and Madhusanka Liyanage. "The role of blockchain to fight against COVID-19." *IEEE Engineering Management Review* 48, no. 3 (2020): 85-96.

[14] Jun, MyungSan. "Blockchain government-a next form of infrastructure for the twenty-first century." *Journal of Open Innovation: Technology, Market, and Complexity* 4, no. 1 (2018): 7.

[15] Kim, Seong-Kyu, and Jun-Ho Huh. "A study on the improvement of smart grid security performance and blockchain smart grid perspective." *Energies* 11, no. 8 (2018): 1973.

[16] Kumar, Nallapaneni Manoj, and Pradeep Kumar Mallick. "Blockchain technology for security issues and challenges in IoT." *Procedia Computer Science* 132 (2018): 1815-1823.

[17] Warkentin, Merrill, and Craig Orgeron. "Using the security triad to assess blockchain technology in public sector applications." *International Journal of Information Management* 52 (2020): 102090.

[18] Halpin, Harry, and Marta Piekarska. "Introduction to Security and Privacy on the Blockchain." In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 1-3. IEEE, 2017.

[19] Demirkan, Sebahattin, Irem Demirkan, and Andrew McKee. "Blockchain technology in the future of business cyber security and accounting." *Journal of Management Analytics* 7, no. 2 (2020): 189-208.

[20] S. Farshidi, S. Jansen, D. Van Den Heuvel, and S. Brinkkemper, "Decision support for blockchain platform selection: Three industry case studies," *IEEE Software*, vol. 37, no. 5, pp. 50–57, 2020.

[21] Liu, Hong, Yan Zhang, and Tao Yang. "Blockchain-enabled security in electric vehicles cloud and edge computing." *IEEE Network* 32, no. 3 (2018): 78-83.

[22] Lei, Ao, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P. Anyigor Ogah, and Zhili Sun. "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems." *IEEE Internet of Things Journal* 4, no. 6 (2017): 1832-1843.

[23] Zeng, Zilong, Yong Li, Yijia Cao, Yirui Zhao, Junjie Zhong, Denis Sidorov, and Xiangcheng Zeng. "Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application." *Energies* 13, no. 4 (2020): 881.

[24] Alphand, Olivier, Michele Amoretti, Timothy Claeys, Simone Dall'Asta, Andrzej Duda, Gianluigi Ferrari, Franck Rousseau, Bernard Tourancheau, Luca Veltri, and Francesco Zanichelli. "IoTChain: A blockchain security architecture for the Internet of Things." In *2018 IEEE wireless communications and networking conference (WCNC)*, pp. 1-6. IEEE, 2018.



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023

[25] Wang, Hai, Yong Wang, Zigang Cao, Zhen Li, and Gang Xiong. "An overview of blockchain security analysis." In *Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018, Revised Selected Papers 15*, pp. 55-72. Springer Singapore, 2019.

[26] Ahmad, Farhan, Zeeshan Ahmad, Chaker Abdelaziz Kerrache, Fatih Kurugollu, Asma Adnane, and Ezedin Barka. "Blockchain in internet-of-things: Architecture, applications and research directions." In *2019 International conference on computer and information sciences (ICCIS)*, pp. 1-6. IEEE, 2019.

[27] Wu, Sihua, and Jiang Du. "Electronic medical record security sharing model based on blockchain." In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pp. 13-17. 2019.



Doi : https://doi.org/10.54216/JCIM.110204
Received: November 24, 2022 Revised: January 26, 2023 Accepted: March 14, 2023