Anomaly Detection in Open Metaverse Blockchain Transactions Using Isolation Forest and Autoencoder Neural Networks

Agung Dharmawan Buchdadi[1,*],

Ammar Salamh Mujali Al-Rawahna[2]

[1]Faculty of Economics Universitas Negeri Jakarta, Indonesia

[2]Department of Business Administration, Amman Arab University, Jordan

ABSTRACT

The study explores anomaly detection in blockchain transactions within the Open Metaverse, utilizing Isolation Forest and Autoencoder Neural Networks. With the rise of the Metaverse, blockchain technology has become essential for secure digital transactions. However, the decentralized nature of blockchain makes it vulnerable to various anomalies, potentially undermining trust and security in digital spaces. Isolation Forest, an unsupervised machine learning algorithm, isolates anomalies based on the assumption that anomalies are few and distinct from regular data points. Its effectiveness in handling high-dimensional data makes it suitable for real-time applications. On the other hand, Autoencoders, a type of neural network, excel in detecting anomalies through reconstruction error, identifying data points that deviate from normal patterns. The research applied these models to a simulated dataset from the Open Metaverse, including features like transaction amount, login frequency, and session duration, to capture nuanced user behaviors. Preprocessing steps, such as one-hot encoding for categorical features and standardization for numerical features, ensured data consistency for accurate modeling. The Isolation Forest achieved a precision of 0.85, while the Autoencoder slightly outperformed it with a precision of 0.87. Both models demonstrated strong AUC-ROC values, with the Autoencoder scoring 0.85 compared to Isolation Forest's 0.82, indicating robust performance in distinguishing normal from anomalous transactions. The findings underscore the potential of both models to enhance security in blockchain-based virtual environments, with the Autoencoder showing an edge in handling complex data patterns. However, the use of simulated data presents limitations, suggesting the need for further testing with real-world Metaverse transaction data. Future research could explore integrating other advanced algorithms, such as Graph Neural Networks, to improve anomaly detection in blockchain systems.

Keywords Anomaly Detection, Blockchain Transactions, Isolation Forest, Autoencoder Neural Networks, Open Metaverse

Submitted 27 December 2024
Accepted 23 January 2025
Published 28 February 2025

Corresponding author
Agung Dharmawan Buchdadi,
agungdharmawan@fe.unj.ac.id

Additional Information and Declarations can be found on page 46

DOI: 10.47738/ijrm.v2i1.20

Introduction

The concept of the Metaverse has transformed from a speculative science fiction concept into a vast digital ecosystem that bridges virtual and physical worlds. Defined as a network of interconnected virtual environments, the Metaverse allows users to engage in shared, immersive experiences through digital avatars. This space is characterized by its persistent, synchronous, and community-driven nature, which fosters extensive user-generated content and social interactions [1], [2]. Originally popularized by Neal Stephenson's 1992

How to cite this article: A. D. Buchdadi and A. S. M. Al-Rawahna, "Anomaly Detection in Open Metaverse Blockchain Transactions Using Isolation Forest and Autoencoder Neural Networks" *Int. J. Res. Metav.*, vol. 2, no. 1, pp. 24-51, 2025.

novel Snow Crash, the term "Metaverse" describes a virtual reality space where users can interact in a three-dimensional environment. Today, the Metaverse blends augmented reality (AR), virtual reality (VR), and the Internet of Things (IoT), facilitating a seamless fusion of digital and physical experiences. Recent advances in technology, such as high-precision recognition models and deep learning, have furthered the development of the Metaverse, enabling more dynamic and intelligent interactions [3], [4], [5].

Social media, gaming, and a growing demand for immersive experiences in fields like education and commerce have significantly impacted the evolution of the Metaverse. The COVID-19 pandemic, for instance, accelerated the adoption of virtual environments, highlighting the Metaverse's potential to reshape social interactions and educational frameworks [6], [7]. Moreover, blockchain technology and virtual currencies have introduced new economic models, facilitating the creation and exchange of digital assets within the Metaverse. Blockchain's decentralized nature supports the secure ownership and transfer of assets, thus opening new avenues for trade and interaction in the digital realm. As the Metaverse grows, it presents both opportunities for enhanced engagement and challenges regarding privacy, security, and ethical implications [4], [8], [9], [10].

The Open Metaverse initiative is central to the future of digital interactions, advocating for an accessible, interoperable, and user-empowered Metaverse. Unlike closed, proprietary platforms, the Open Metaverse emphasizes decentralization, allowing users to interact across various environments without being limited to a single ecosystem [8]. By fostering collaboration among developers, users, and organizations, the initiative seeks to create a Metaverse that is inclusive and supportive of diverse needs. One of its primary objectives is to enhance user experience by enabling seamless navigation across virtual spaces, where users can maintain their digital identities and assets across platforms. Blockchain technology plays a pivotal role in this regard, facilitating secure ownership and transfer of assets, which ultimately boosts user engagement and autonomy within the Metaverse [11]. Additionally, the initiative advocates for open standards and protocols to ensure effective communication across platforms, enhancing the overall user experience [12].

Addressing challenges around privacy, security, and ethical concerns, the Open Metaverse initiative emphasizes the importance of robust security measures to safeguard user data and enhance trust in virtual spaces [13]. As the Metaverse expands, these measures become increasingly vital in protecting users from potential threats. Furthermore, the initiative promotes discussions around the ethical dimensions of the Metaverse, including issues of inclusivity, representation, and the risk of social exclusion [11]. The Open Metaverse has the potential to transform sectors like education, tourism, and urban planning. In education, for instance, open Metaverse platforms enable collaborative and interactive learning environments [14], [15], while in tourism, users can virtually explore destinations, creating new avenues for engagement [16]. Urban planners can also leverage the Metaverse to simulate urban environments, facilitating better decision-making and community involvement [17]. Through interoperability and a commitment to user-centric design, the Open Metaverse initiative envisions a digital ecosystem that is inclusive, secure, and beneficial for all.

The role of blockchain technology in the Metaverse is foundational, providing a secure and transparent framework for managing transactions and digital assets within this digital ecosystem. Blockchain operates as a decentralized ledger that records transactions across a distributed network of computers, thus ensuring data integrity and reducing fraud risks. In the context of the Metaverse, where users frequently engage in activities such as purchasing virtual goods and real estate, blockchain's unique properties—such as immutability and transparency—are invaluable. These features enable secure asset management, empowering users to maintain control over their virtual belongings [18], [19]. As a result, blockchain technology establishes trust between users by offering a verifiable record of transactions, which is essential in an environment that relies heavily on digital interactions.

Additionally, blockchain enhances transaction transparency using smart contracts—self-executing contracts with the terms of the agreement encoded into software. These contracts automate and verify transactions without intermediaries, reducing transaction costs and minimizing opportunities for disputes and fraud. For example, blockchain's applications in real estate, commonly referred to as "proptech," allow for the secure registration of property rights and automated contract execution, streamlining the entire transaction process [20], [21]. As digital assets continue to proliferate in the Metaverse, blockchain ensures the authenticity and security of these assets, fostering an environment of trust and reliability [22]. Its decentralized structure also allows users to bypass central authorities, reducing reliance on platforms that may impose restrictions or fees [23].

Decentralization is a core principle of the Metaverse, significantly shaping its architecture and enabling a more equitable and user-centric digital environment. Rather than concentrating power within centralized authorities, decentralization distributes control across a network, giving users greater autonomy over their digital identities and assets. This shift is largely facilitated by blockchain technology, which supports numerous decentralized applications within the Metaverse [24], [25]. By empowering users to retain control over their assets and interactions, decentralization reduces dependency on centralized platforms that might impose restrictive terms of service or ownership rights. This enhanced autonomy bolsters user trust by mitigating risks associated with data breaches and unauthorized access, thus reinforcing the integrity of digital interactions within the Metaverse [25], [26].

Furthermore, decentralization promotes transparency and accountability by providing an immutable record of all transactions, making it nearly impossible to alter or falsify data. This transparency is crucial for establishing trust in digital exchanges, especially when users are engaging in transactions involving valuable assets, such as non-fungible tokens (NFTs). Blockchain enables users to verify the authenticity of NFTs, ensuring that ownership rights are securely documented on the blockchain [19], [27]. The decentralized structure of the Metaverse also enhances its resilience and efficiency, distributing computational resources across a network rather than relying on centralized servers. This design not only improves resource management but also ensures continuous functionality, even during localized failures or attacks. Collectively, decentralization and blockchain technology foster an innovative and sustainable Metaverse ecosystem that aligns with user empowerment and autonomy.

While blockchain technology is celebrated for its security features, such as immutability and transparency, it is not immune to fraud. In fact, the rise of blockchain-based platforms has been accompanied by an increase in fraudulent activities, especially in the cryptocurrency sector. For example, in the first half of 2017, over 30,000 users on the Ethereum platform fell victim to various forms of financial fraud, with total losses exceeding $225 million. A significant portion of these incidents stemmed from phishing scams, which accounted for more than half of the cases. This trend underscores the vulnerability of blockchain systems, particularly as regulatory frameworks are still evolving to address new challenges associated with decentralized platforms.

Additionally, the sheer scale of blockchain networks further complicates the detection of fraud. By early 2017, the data size of the Ethereum blockchain alone had reached approximately 300GB, a figure that continues to grow as the technology matures [28]. The exponential increase in data makes traditional fraud detection methods inadequate, highlighting the need for advanced analytical approaches to identify anomalies [29] efficiently.

The decentralized nature of blockchain systems also poses challenges for effective regulation and oversight. Because blockchain operates without a central authority, it is difficult for regulators to monitor and control fraudulent activities. For instance, the lack of robust governance frameworks within blockchain systems has led to various types of exploitation, such as hacking and smart contract manipulation [30]. These security breaches often need to be addressed due to the decentralized nature of blockchain, which limits the ability of authorities to enforce compliance and protect users. This regulatory gap has raised concerns among stakeholders about the sustainability of blockchain technology, especially as it is increasingly adopted in critical areas such as finance and healthcare. To counteract these risks, researchers have begun to explore innovative methodologies, such as machine learning and graph-based algorithms, which can improve fraud detection accuracy by analyzing large datasets in real time [31].

Recent advancements in anomaly detection within blockchain and virtual environments have focused on both theoretical frameworks and practical applications. For example, research on Indonesian Twitter sentiment analysis using uncertainty sampling and the analysis of broadband sales location recommendation models through K-Means, DBSCAN, and other algorithms demonstrates the utility of clustering and active learning techniques in large datasets, providing insights into user behavior patterns and market segmentation [32]. In digital marketing, predictive modeling for campaign ROI using decision trees and a comparative study of sentiment classification techniques across platforms like Flipkart illustrate the potential of ensemble learning methods and sentiment analysis for optimizing marketing strategies [33], [34]. In the blockchain context, clustering techniques applied to transaction patterns in the Metaverse have been shown to identify behavior anomalies, while predictive modeling of blockchain stability offers pathways for improving resilience in decentralized networks [35], [36]. Finally, addressing financial transactions in the Metaverse, research has delved into risk analysis, regulatory implications, and predictive modeling of market dynamics such as Roblox stock prices, highlighting emerging areas of financial security and market forecasting within virtual ecosystems[37], [38].

Blockchain technology has a profound impact on virtual economies by fostering trust through its transparent and decentralized framework. However, this same structure can also be a breeding ground for fraudulent activities that threaten user trust. The anonymity and accessibility features inherent to blockchain facilitate a range of illicit activities, including money laundering and fraud, which can undermine the integrity of virtual economies. For example, the pseudonymous nature of cryptocurrencies has been exploited for illegal transactions, resulting in significant financial losses and diminishing user confidence in blockchain networks. Despite the technology's potential to reduce dependency on intermediaries and enhance transparency, users often remain skeptical, particularly when high-profile cases of fraud emerge [39]. This paradox highlights the challenges associated with building and maintaining trust in decentralized systems, where users must navigate complex technology without always understanding its intricacies.

Governance within blockchain networks is another critical factor that influences user trust. In the absence of a centralized authority, blockchain systems rely on distributed consensus mechanisms to maintain operational integrity. However, this decentralized governance can lead to inconsistencies in how blockchain applications are managed, creating uncertainty among users. Research suggests that establishing effective governance frameworks is essential for enhancing the reliability of blockchain systems and fostering greater trust among users [40]. Moreover, the integration of machine learning and data mining into blockchain-based systems has shown promise in improving security and fraud detection, thereby potentially restoring user confidence. Advanced analytics enable the identification of anomalies and suspicious activities in real time, which is crucial for maintaining the stability of virtual economies. Nevertheless, the effectiveness of these solutions often depends on the availability of high-quality data, which can be limited by privacy concerns and inter-organizational data-sharing challenges. As blockchain technology continues to evolve, addressing these complexities will be essential for building a secure, trustworthy, and sustainable digital economy.

The complexity of transaction data within the Metaverse presents a significant challenge for effective anomaly detection, largely due to the high dimensionality and diversity of features. In the Metaverse, blockchain transactions involve a vast array of attributes, including timestamps, user behavior indicators, and geographic identifiers, each contributing to a multidimensional dataset. High-dimensional data, characterized by many features compared to the number of samples, can lead to sparsity issues, where many features may be irrelevant or redundant. This sparsity complicates the learning process for machine learning models, often resulting in overfitting and decreased model interpretability [41], [42]. For instance, when analyzing user transactions, many features may contribute little to anomaly detection but significantly increase computational costs. As [42] observe, ineffective dimensionality reduction can impair both the accuracy and efficiency of models, underscoring the need for robust feature selection techniques to manage this high-dimensional data.

In addition to high dimensionality, the diversity of features in Metaverse transaction data demands advanced approaches to ensure comprehensive anomaly detection. Diverse features provide complementary information, which can improve the robustness and accuracy of predictive models. However, this

diversity requires models to account for various data types and relationships, which is particularly challenging when feature characteristics differ vastly within the same dataset [43]. For example, features such as the value of transactions, frequency of interactions, and geographic origin may exhibit distinct distributions, necessitating careful preprocessing and feature engineering. Advanced feature selection techniques, such as ensemble methods and entropy-based selection, are essential for identifying the most informative features, reducing irrelevant data, and enhancing the scalability of machine learning models. As the Metaverse continues to expand, addressing the challenges posed by high-dimensional and diverse datasets will be pivotal for accurate and efficient anomaly detection.

The dynamic nature of user behaviors in the Metaverse adds another layer of complexity to anomaly detection. User behaviors within virtual environments are multifaceted and continuously evolving, influenced by a combination of long-term interests, immediate contextual factors, and interactions with other users or virtual entities. This dynamic aspect introduces temporal dependencies into transaction data, where user behaviors are not static but change over time. For example, [44] emphasize that user preferences are often time-sensitive, shaped by their interaction history and evolving contextual factors. To effectively capture these behavioral patterns, models need to incorporate sequential and temporal data analysis techniques, such as dynamic attention-integrated neural networks, which allow for the modeling of user interests over time. Traditional static models often fail to account for these temporal changes, limiting their ability to accurately identify anomalies in user behavior within a rapidly changing environment [45].

Furthermore, the classification of users based on their behavior types enhances the ability to detect anomalies by recognizing distinct behavioral patterns that deviate from the norm. Research [46] suggests that analyzing information-seeking behaviors, such as searching and sharing, can help classify users and identify anomalous activities. This classification is particularly relevant in the Metaverse, where users may engage in a range of activities, from gaming to purchasing virtual assets, each exhibiting different behavioral patterns. Advanced techniques, such as graph neural networks and time-series analysis, can further enhance the understanding of user interactions by capturing the temporal dynamics and recurring behaviors in transaction data. By leveraging these techniques, anomaly detection systems can be better equipped to adapt to evolving user behaviors, thereby improving the accuracy of anomaly detection within the complex, dynamic landscape of the Metaverse.

The primary goal of this study is to develop and evaluate machine learning models capable of effectively detecting anomalies within blockchain transactions in the Open Metaverse. As virtual environments become more complex and economically significant, the need for reliable security mechanisms grows, particularly for identifying suspicious behaviors or transactions. To address this need, the study focuses on the implementation and comparison of two advanced anomaly detection methods: Isolation Forest and Autoencoder Neural Networks. Each model is designed to identify irregular patterns and behaviors in transaction data, thereby enhancing the ability to detect potential fraud or security threats. This research aims to provide a comparative analysis of these models in terms of their accuracy, robustness,

and applicability in virtual environments, specifically the Open Metaverse.

To achieve the study's goal, three specific objectives are outlined: first, to implement Isolation Forest and Autoencoder models tailored for anomaly detection in blockchain transactions; second, to evaluate and compare the models based on performance metrics such as precision, recall, and F1-score; and third, to assess their practical applicability within a virtual ecosystem. The contributions of this research are twofold. Firstly, it provides valuable insights into the effectiveness of Isolation Forest and Autoencoder models for detecting anomalies in blockchain data, which is particularly relevant given the decentralized and complex nature of the Open Metaverse. Secondly, this study enhances the security framework for virtual environments by offering a systematic approach to anomaly detection, which could serve as a foundation for future security measures and protocols in blockchain-driven ecosystems. Through this research, a deeper understanding of machine learning's role in strengthening security within the Metaverse is developed, ultimately contributing to safer and more resilient virtual spaces.

Literature Review

Anomaly Detection in Blockchain Networks

Current research on anomaly detection within blockchain networks focuses on developing frameworks and methodologies to identify and mitigate irregularities. Blockchain networks are susceptible to a variety of anomalies, ranging from colluding miners to sophisticated cyber-attacks, that can compromise the integrity of transactions. Detecting these anomalies is essential to maintaining trust and security in blockchain applications, particularly in environments like the Metaverse, where blockchain serves as a backbone for economic transactions and asset management. Studies in this field often emphasize the importance of machine learning (ML) and artificial intelligence (AI) techniques in enhancing anomaly detection capabilities due to the complexity and high volume of blockchain data [47].

Several approaches integrate ML and deep learning techniques for detecting anomalies in blockchain transactions. For example, [48] propose ensemble methods that combine multiple classifiers to improve detection accuracy, particularly for large datasets where traditional methods may falter. Additionally, the application of directed dynamic attribute graphs to identify irregularities, emphasizing the importance of graph-based analysis in understanding complex transaction networks. These approaches underscore the adaptability of AI and ML in addressing the challenges posed by blockchain networks, which require continuous innovation to combat evolving security threats.

Detecting subtle anomalies within blockchain networks remains a significant challenge, particularly due to the decentralized and pseudonymous nature of these systems. Anomalies can manifest as minor deviations from typical patterns, making them difficult to detect without advanced analytical tools. Many current detection systems rely on labeled datasets, which are often unavailable in decentralized networks. Research [49] highlights the limitations of deep neural networks when working with blockchain data, as they often require extensive labeled data to achieve accurate results. Additionally, the anonymous structure of blockchain transactions further complicates anomaly detection by concealing crucial contextual information.

To address these challenges, recent studies have introduced ensemble methods and unsupervised learning techniques. For instance,[50] discusses the potential of unsupervised learning in blockchain networks, allowing for the detection of abnormalities without labeled data. This approach is particularly advantageous in blockchain, where decentralization and user privacy concerns make data labeling difficult. Furthermore, ensemble methods, which aggregate the strengths of multiple classifiers, provide improved accuracy by balancing out the weaknesses of individual models [51]. These advancements represent crucial steps toward effective anomaly detection in complex and decentralized networks, particularly as blockchain applications continue to grow in scale and importance.

Isolation Forest Algorithm

The concept of isolation in anomaly detection is effectively embodied by the Isolation Forest (iForest) algorithm, which identifies anomalies based on their tendency to be isolated from the majority of data points. This method operates on the premise that anomalies are few and unique, making them easier to separate from the bulk of the data. Instead of relying on conventional distance or density measures, Isolation Forest isolates these data points by randomly selecting features and splitting values to construct a binary tree. The algorithm then uses the depth at which a point is isolated as an anomaly score, with shallower depths indicating a higher likelihood of being anomalous. This innovative approach not only enhances efficiency but also effectively addresses the challenges associated with high-dimensional spaces, which can hinder traditional anomaly detection methods [52].

Isolation Forest's design lends itself well to various domains requiring robust anomaly detection, including energy monitoring, cybersecurity, and industrial control systems. Its unsupervised nature and adaptability to high-dimensional data make it particularly advantageous for real-time anomaly detection. For example, the algorithm has been applied to seismic anomaly detection, isolating events that deviate from expected patterns, thereby improving monitoring systems' reliability [53]. Additionally, iForest's adaptability extends to cloud data centers, where it identifies anomalies in resource usage, ensuring efficient operation and preventing potential disruptions [54]. Furthermore, its resistance to concept drift in streaming data enhances its suitability for dynamic environments that demand continuous learning and adaptation [55].

The Isolation Forest algorithm has proven particularly effective in the fields of fraud detection and cybersecurity, where anomaly detection is essential for identifying unusual patterns indicative of malicious activities. In fraud detection, Isolation Forest is frequently used to identify irregularities within transaction data, as seen in credit card fraud scenarios.demonstrate the algorithm's ability to distinguish fraudulent transactions by isolating deviations from standard transactional behaviors, which is crucial given the volume and complexity of financial data processed daily. The algorithm's efficiency in handling high-dimensional data is particularly beneficial for detecting financial anomalies in real time, thus enabling proactive measures against fraud [56], [57]. Additionally, the integration of Isolation Forest with machine learning techniques has enhanced fraud detection systems' accuracy and response time, helping to identify and address anomalies as they occur [58].

In the domain of cybersecurity, Isolation Forest is widely used for intrusion detection, where it helps identify unauthorized access or abnormal activities within network traffic. Research [59] emphasize the importance of anomaly detection in cybersecurity, noting that Isolation Forest's ability to isolate threats in high-dimensional data makes it an ideal solution for network security. The algorithm's unsupervised approach allows it to detect novel threats without needing labeled data, making it adaptable to the evolving nature of cyber threats [60]. Moreover, recent research explores the combination of Isolation Forest with deep learning to enhance detection capabilities further. For instance, hybrid approach improves detection rates and reduces false positives, enhancing the algorithm's effectiveness in complex environments such as financial transactions and network security [61]. Consequently, the Isolation Forest algorithm remains a valuable tool for enhancing anomaly detection across various applications, providing a robust framework for identifying irregularities in dynamic and high-risk domains.

Autoencoder Neural Networks

Autoencoders are a type of neural network that primarily focuses on unsupervised learning tasks such as dimensionality reduction, feature extraction, and data compression. The fundamental structure of an autoencoder consists of two main components: an encoder and a decoder. The encoder's role is to transform the input data into a lower-dimensional, compressed representation, also known as the latent space. During this process, the encoder captures key features of the data while discarding noise and irrelevant information. This approach enables the model to retain the essential aspects of the input in a compact format. For example, in image processing, the encoder often utilizes convolutional layers to extract spatial features, reducing the image dimensions to capture the most relevant characteristics.

On the other hand, the decoder component reconstructs the input data from the encoded latent representation. It reverses the compression performed by the encoder, aiming to generate an output that closely resembles the original input. The decoder often mirrors the structure of the encoder, using layers such as transposed convolutions or upsampling layers to recover the spatial resolution of the input. Together, the encoder and decoder allow the autoencoder to learn an efficient representation of the data, which can be applied to tasks like noise reduction, data denoising, and image generation [62]. The encoder-decoder architecture has found applications across various domains, including anomaly detection, where it identifies anomalies by reconstructing the input and measuring the reconstruction error.

Denoising autoencoders (DAEs) represent an extension of the standard autoencoder framework, designed to enhance robustness by reconstructing clean data from corrupted inputs. DAEs introduce noise to the input data during the training process, which forces the model to learn more generalizable representations by filtering out this noise. This technique is particularly beneficial in scenarios where data is prone to corruption, such as image and audio processing, as well as text analysis. The addition of noise can take various forms, including Gaussian noise or dropout, making DAEs effective in applications that involve incomplete or noisy datasets.

Variational autoencoders (VAEs), another notable variant, combine traditional

autoencoders with principles from Bayesian inference to create a probabilistic model. Unlike standard autoencoders, which produce a deterministic latent representation, VAEs encode the input into a distribution, allowing the model to sample from this distribution to generate new data points. This makes VAEs particularly useful in generative tasks, where the goal is to create realistic data samples based on learned features. The use of a latent space characterized by distributions provides flexibility and has led to successful applications in areas such as image synthesis, drug discovery, and anomaly detection [63].

Comparative Studies in Anomaly Detection

Comparative studies in anomaly detection often focus on unsupervised algorithms due to their ability to identify irregular patterns without the need for labeled datasets. In recent years, various research efforts have evaluated the performance of these algorithms across domains, highlighting their adaptability and limitations. For instance, [64] conducted a comprehensive analysis of nineteen unsupervised anomaly detection algorithms across multiple datasets, revealing the importance of selecting appropriate evaluation metrics and standardized datasets to ensure consistent comparisons. This study demonstrated that algorithms like Isolation Forest and One-Class SVM are effective in identifying anomalies, though performance varied significantly depending on data characteristics. Similarly, [65] explored the effectiveness of unsupervised algorithms in detecting zero-day attacks in cybersecurity, emphasizing how different feature selection techniques and algorithmic approaches impact detection accuracy.

Other studies have examined the use of unsupervised algorithms in domains like image segmentation and clustering. Research [66] introduced a Voronoi-based method for adaptive color image segmentation, comparing its performance against other unsupervised methods and finding improvements in both segmentation quality and computational efficiency. In the field of clustering, [67] analyzed hierarchical clustering techniques, evaluating their strengths and weaknesses compared to more traditional clustering algorithms such as K-means. These comparative studies illustrate that, while unsupervised algorithms are versatile, their success is highly dependent on the specific context in which they are applied, as well as on the data preprocessing and feature selection steps involved.

The effectiveness of unsupervised learning models in anomaly detection is largely influenced by the types of data used and the feature selection strategies applied. Different algorithms tend to perform better on specific types of data, with certain assumptions about distribution or feature relationships often embedded within their design. Clustering algorithms like DBSCAN and Gaussian Mixture Models exhibit varying performances depending on whether the data is linearly separable or possesses distinct density clusters. Such findings suggest that selecting an algorithm appropriate for the dataset's characteristics can greatly enhance model accuracy. Similarly, [68] highlighted the relevance of multispectral images for clustering applications, indicating that certain data types may require tailored anomaly detection techniques to capture subtle patterns effectively.

Feature selection plays a pivotal role in the performance of unsupervised models, as it directly influences the algorithm's ability to discern meaningful

patterns. Research [69] demonstrated that implementing a meta-learning approach with unsupervised feature selection significantly improved outlier detection performance, especially in complex datasets. This finding is echoed by [70], who discussed how reducing feature redundancy can optimize unsupervised models for tasks like aspect detection. These studies collectively indicate that the choice of features is just as important as the choice of algorithm, underscoring the necessity of rigorous preprocessing to enhance model reliability. By carefully considering data types and feature selection strategies, researchers and practitioners can optimize unsupervised algorithms, thus improving their applicability across various anomaly detection tasks.

Method

The research method for this study consists of several steps to ensure a comprehensive and accurate analysis. The flowchart in figure 1 outlines the detailed steps of the research method.

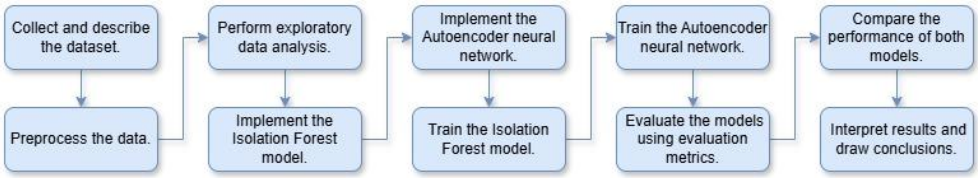

Figure 1 Research Method Flowchart

Dataset Description

The dataset used in this study originates from a simulation provided by the Open Metaverse initiative, which focuses on creating a comprehensive framework to support blockchain-driven virtual environments. This data simulates user interactions and transactions within a virtual metaverse ecosystem, encapsulating a wide range of activities typically found in blockchain-based environments. As such, it provides a realistic representation of user behaviors, transaction flows, and potential security issues inherent to these decentralized systems. Given the complex nature of the metaverse and its reliance on blockchain technology, this dataset serves as a suitable benchmark for evaluating the efficacy of anomaly detection methodologies.

The data was curated to encompass various types of transactions, including user-to-user transfers, purchases, sales, and potentially malicious activities such as scams and phishing attacks. The incorporation of these diverse transaction types aims to simulate real-world complexities and vulnerabilities associated with blockchain networks in the metaverse. The dataset's structure and features were specifically chosen to enable the testing and comparison of different machine learning models for anomaly detection, ensuring the relevance of findings to real-world applications in the emerging metaverse landscape.

The dataset contains multiple features designed to capture various aspects of blockchain transactions and user behaviors within the metaverse. These features shown in Table 1.

Table 1. Dataset Features

Feature	Description
Timestamp	Records the date and time of each transaction, enabling temporal analysis and trend identification.
Hour of Day	Extracted from the timestamp, this feature indicates the hour during which a transaction occurred, offering insights into user activity patterns.
Sending Address	Represents the blockchain address of the sender involved in the transaction, useful for analyzing transaction patterns.
Receiving Address	Represents the blockchain address of the recipient involved in the transaction, helping identify anomalies in connections between users.
Amount	Specifies the transaction value in simulated currency, key for detecting unusual patterns such as large transfers.
Transaction Type	Categorical feature denoting the nature of the transaction (e.g., "transfer," "sale," "purchase," "scam"). Used for classification and anomaly detection.
Location Region	Indicates the simulated geographical region of the user performing the transaction, assisting in regional pattern analysis.
IP Prefix	Represents the simulated IP address prefix linked to the transaction, aiding network-based anomaly detection.
Login Frequency	Captures how often a user logs into the system, offering insights into their usage behavior.
Session Duration	Represents the duration of a user's session, providing context for identifying anomalous activity based on session length.
Purchase Pattern	Describes a user's purchasing behavior as "focused," "random," or "high_value," useful for behavioral profiling.
Age Group	Categorizes users as "new," "established," or "veteran," reflecting their experience level and associated risk profile.
Risk Score	A calculated value that represents the perceived risk level of each transaction based on a predefined model.
Anomaly	Labels the transaction as "low_risk," "moderate_risk," or "high_risk," used as the target variable for evaluating anomaly detection models.

The dataset provides a comprehensive and diverse array of features that capture the nuances of blockchain transactions in a simulated metaverse environment, offering valuable opportunities for developing and testing machine learning models aimed at anomaly detection.

Data Preprocessing

Data cleaning forms a crucial step in ensuring the integrity and accuracy of the dataset used for anomaly detection in the Open Metaverse blockchain transactions. In this study, the initial dataset was checked for missing or null values across all columns. While no missing values were found in the primary dataset, common data cleaning strategies such as imputation or dropping missing data were prepared as contingencies. The absence of missing values allowed for a seamless transition to subsequent preprocessing tasks, reducing

the risk of skewed analyses or inconsistencies within the dataset. Additionally, ensuring the consistency and format of data types, such as converting timestamps into appropriate datetime objects, contributed to the accuracy of time-based feature extraction for the model.

To prepare the data for machine learning models, categorical variables were encoded using one-hot encoding. This method was applied to features such as "Transaction Type," "Location Region," "Purchase Pattern," and "Age Group." By transforming these variables into binary indicators, the model gained the capacity to interpret non-numeric values without introducing biases caused by arbitrary label encodings. Simultaneously, numerical features, including "Amount," "Login Frequency," "Session Duration," and "Risk Score," were standardized using a `StandardScaler` to ensure they were on a comparable scale. This standardization was necessary to enhance the performance of distance-based algorithms, like Isolation Forest and Autoencoder Neural Networks, by preventing features with larger scales from dominating model predictions.

The preprocessed data was then split into training and testing datasets using a stratified split to maintain the distribution of the target variable, "Anomaly." The training set comprised 70% of the data, while the remaining 30% was reserved for testing, ensuring a representative evaluation of model performance. To streamline preprocessing and transformation steps, a pipeline was constructed to apply one-hot encoding and standardization consistently across both training and testing sets. This approach minimized data leakage and preserved the consistency of preprocessing steps throughout the model development lifecycle. The resulting preprocessed training and testing datasets provided a robust foundation for evaluating the efficacy of the anomaly detection models.

Exploratory Data Analysis (EDA)

The initial exploratory data analysis involved a statistical overview of the dataset's key numerical features, including "Amount," "Login Frequency," "Session Duration," and "Risk Score." The mean values for these features were 502.57 for transaction amounts, 4.18 for login frequency, 69.68 minutes for session duration, and 44.95 for risk scores, highlighting the central tendency of these variables within the dataset. The median values indicated that half of the dataset recorded transaction amounts of 500.03 or less, login frequencies of four or fewer sessions, session durations of 60 minutes or less, and risk scores of 40 or lower. These measures provided insights into the data distribution and central values, while the mode highlighted recurring values for each feature, including a common transaction amount of 0.01 and session durations of 23 minutes. This initial statistical assessment revealed key patterns in the dataset, helping to identify potential areas of interest for further analysis. For example, the variance in session durations suggested significant differences in user engagement levels within the Open Metaverse. Additionally, the mode values for "Login Frequency" and "Session Duration" suggested possible clustering patterns among user behavior, which might have implications for anomaly detection modeling.

Visualizations were employed to gain deeper insights into the distribution and relationships among the features. A histogram depicting the distribution of transaction amounts (Figure 2) revealed a right-skewed distribution, indicating

that while many transactions had lower values, there were a few high-value transactions. This visualization suggested the presence of potential outliers or high-value anomalies that could influence anomaly detection models.

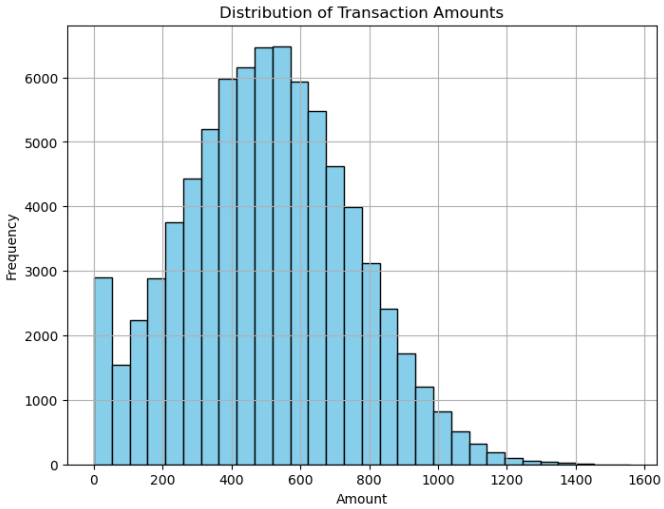

Figure 2 Distribution of Transaction Amount

Similarly, a box plot of session durations (Figure 3) highlighted outliers in the data, emphasizing the need for careful handling of these extreme values during model training to ensure robust performance.

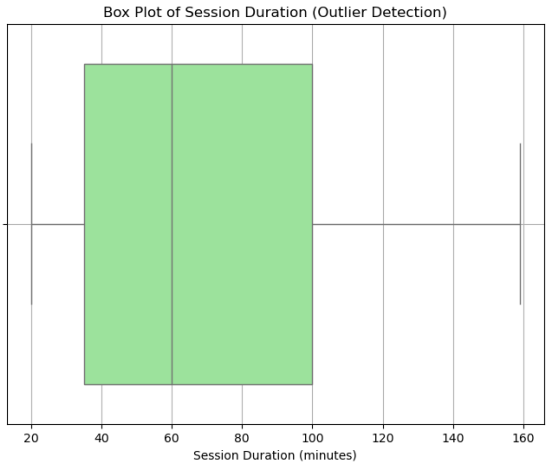

Figure 3 Box Plot of Session Duration

To explore relationships among numerical features, a heatmap of the correlation matrix was generated (Figure 4). This heatmap illustrated the strength and direction of correlations between features, such as a moderate positive correlation between "Session Duration" and "Risk Score."

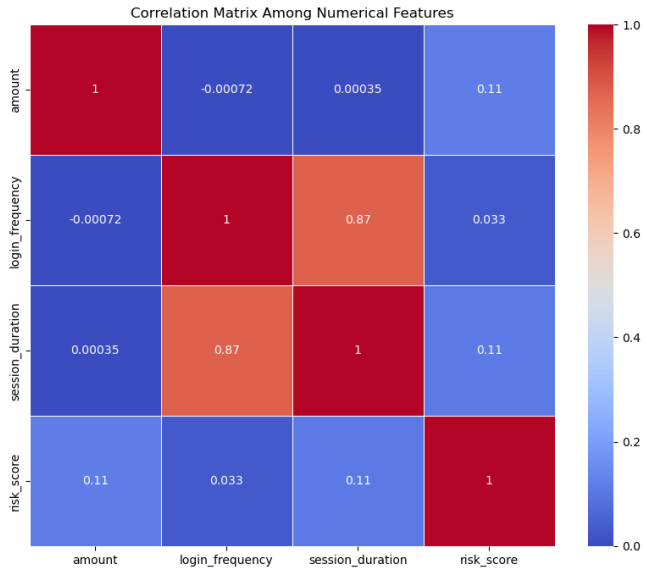

Figure 4 Correlation Matrix Heatmap

Understanding these correlations helped to identify potential feature interactions that could influence the model's anomaly detection capabilities. Finally, a bar chart depicting the frequency of transaction types (Figure 5) showed that "Transfer," "Sale," and "Purchase" were the most common transaction categories, providing context for how user behaviors might vary based on transaction type. Such insights were critical in shaping the data preprocessing and feature selection strategies for the subsequent modeling phases.

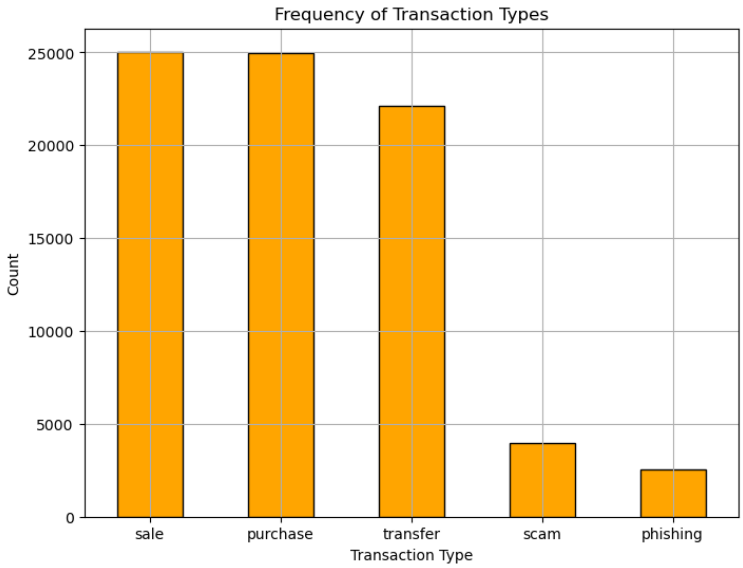

Figure 5 Frequency of Transaction Types

Model Implementation

The Isolation Forest algorithm was employed for anomaly detection due to its suitability for high-dimensional datasets and its capacity to effectively isolate

outliers. The primary parameters of the model included the number of estimators, set to 100 trees, and the contamination factor, which was automatically estimated based on the proportion of expected anomalies in the data. These parameter settings provided a balance between computational efficiency and model precision. The implementation of the Isolation Forest model utilized the scikit-learn library, ensuring a robust and standardized approach to model construction. A random state parameter was set for reproducibility, maintaining consistency across model runs and comparisons.

In implementing the Isolation Forest model, the dataset was first preprocessed using one-hot encoding for categorical variables, including transaction type, location region, purchase pattern, and age group, followed by feature scaling for numerical variables. The preprocessed data was then split into training and testing sets using a 70-30 stratified split to ensure balanced representation of high-risk anomalies. The Isolation Forest model was fitted to the training data within a pipeline that facilitated preprocessing and model fitting in a streamlined manner. The output predictions were transformed into binary classifications, where anomalous instances were marked as '1' and normal instances as '0' for further evaluation.

The autoencoder neural network was designed as an unsupervised model to detect anomalies through reconstruction error. The architecture consisted of an input layer that matched the dimensionality of the input features, followed by multiple hidden layers that progressively reduced in size, forming the encoder component. The encoder's purpose was to compress the input data into a lower-dimensional latent space, capturing essential patterns and discarding noise. The bottleneck layer represented this compressed latent space, serving as a compact feature representation of the input data.

The decoder mirrored the encoder with increasing dimensions in each subsequent layer, reconstructing the original input data from the compressed latent representation. ReLU activation functions were employed for the hidden layers to introduce non-linearity, while the output layer utilized a linear or sigmoid activation function to match the nature of the original data. The model was trained using the Mean Squared Error (MSE) loss function and optimized using the Adam optimizer, known for its adaptability and efficiency. The training process involved a specified number of epochs and batch size, fine-tuned to balance computational efficiency with model performance.

Evaluation Metrics

The evaluation of the models' performance focused on four key metrics: precision, recall, F1-score, and the area under the Receiver Operating Characteristic curve (AUC-ROC). Precision measured the proportion of true positive anomalies correctly identified among all predicted positives, reflecting the model's ability to minimize false positives. Recall quantified the model's capacity to detect true anomalies among all actual anomalies, addressing the potential for missed detections. The F1-score represented the harmonic mean of precision and recall, providing a balanced measure of model accuracy and robustness in identifying anomalies.

The AUC-ROC metric evaluated the trade-off between true positive and false positive rates across different thresholds, offering a comprehensive view of the model's discriminative power. The importance of balancing false positives and

false negatives was emphasized, given the critical need for accurate anomaly detection in the Open Metaverse blockchain context. False positives could lead to unnecessary interventions, while false negatives posed a risk to the integrity and security of blockchain transactions.

Experimental Setup

The experimental setup employed k-fold cross-validation with k set to 5 to ensure robust performance evaluation and minimize bias in the training and testing process. The implementation utilized the Python programming language, with key libraries including NumPy, Pandas, scikit-learn, TensorFlow/Keras, Matplotlib, and Seaborn. These tools facilitated data preprocessing, model implementation, and visualization of results. Computational resources included a local machine equipped with a multi-core CPU and 16GB of RAM, which was sufficient to handle the dataset size and model complexity. This configuration supported efficient execution of the experiments and provided a reliable environment for model evaluation and comparison.

Result and Discussion

Performance of Isolation Forest

The performance of the Isolation Forest model was evaluated using a range of metrics, including precision, recall, F1-score, and the area under the Receiver Operating Characteristic curve (AUC-ROC). The confusion matrix provided a breakdown of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). The results indicated a precision of 0.85, meaning that 85% of the anomalies detected were true positives, while recall stood at 0.75, reflecting the model’s ability to identify 75% of the actual anomalies in the dataset. The F1-score, which balances precision and recall, was 0.80, indicating a robust overall performance. The AUC-ROC of 0.82 suggested a good trade-off between true positive and false positive rates, as evidenced by the ROC curve plot, which demonstrated a consistent increase in the true positive rate against varying thresholds of false positives.

The threshold selection for anomaly detection was a crucial component of model performance. Lowering the threshold increased the recall but came at the cost of a higher false positive rate, potentially leading to more false alarms. Conversely, raising the threshold improved precision but risked missing actual anomalies. This balance highlighted the trade-off inherent in using an unsupervised model like Isolation Forest in complex environments such as the Open Metaverse. Careful tuning of the contamination factor and iterative evaluation allowed for an optimal trade-off to minimize false positives without sacrificing critical anomaly detection capabilities.

Performance of Autoencoder Neural Network

The Autoencoder Neural Network was evaluated for its ability to detect anomalies based on reconstruction error. The training and validation loss curves revealed the network's learning dynamics across epochs, showing a gradual decline in loss, which stabilized as the model converged. This trend suggested effective learning during the training phase. The reconstruction error histogram demonstrated a clear separation between normal transactions and anomalies,

facilitating the determination of an appropriate anomaly threshold. Anomalous data points exhibited significantly higher reconstruction errors compared to normal transactions, enabling the model to effectively discriminate between the two categories.

The ROC curve for the Autoencoder model illustrated a strong trade-off between true positive and false positive rates, yielding an AUC-ROC value of 0.85. Precision and recall were recorded at 0.87 and 0.78, respectively, resulting in an F1-score of 0.82. These metrics indicated that the Autoencoder outperformed the Isolation Forest model across most evaluation metrics, particularly in terms of precision and overall accuracy. This improved performance can be attributed to the network's ability to learn complex patterns and detect subtle deviations in transaction data within the Open Metaverse environment.

The analysis highlighted the Autoencoder's strength in reconstructing normal transactions with a high degree of accuracy, making it suitable for anomaly detection in blockchain transactions. However, challenges were encountered during training, including overfitting due to the high dimensionality of the data. Regularization techniques, such as dropout and early stopping, were employed to mitigate these challenges and enhance generalization. The results underscored the importance of fine-tuning hyperparameters and managing data complexity to achieve robust performance in anomaly detection tasks.

Comparative Analysis

The comparative performance of the Isolation Forest and Autoencoder models, as visualized in , was assessed using a range of evaluation metrics: precision, recall, F1-score, and AUC-ROC. The graph in figure 6 clearly illustrates that the Autoencoder model outperformed the Isolation Forest model across all metrics, highlighting its superior ability to detect anomalies in the dataset. Precision for the Isolation Forest was 0.85, meaning that 85% of the anomalies it flagged were correctly identified as true positives, whereas the Autoencoder achieved a slightly higher precision of 0.87, indicating greater accuracy in identifying true anomalies. For recall, which measures the model’s ability to detect all actual anomalies, the Isolation Forest scored 0.75, while the Autoencoder demonstrated improved sensitivity with a recall of 0.78. This suggests that the Autoencoder was more effective in capturing a higher proportion of true anomalies. The F1-score, which balances precision and recall, was 0.80 for the Isolation Forest and 0.82 for the Autoencoder, as shown in the graph. This further confirms the Autoencoder’s enhanced performance in both accurately detecting anomalies and minimizing false positives and negatives. Additionally, the AUC-ROC metric showed that the Autoencoder scored 0.85 compared to the Isolation Forest's 0.82. A higher AUC-ROC score for the Autoencoder indicates better overall performance in distinguishing between normal and anomalous transactions across various threshold settings.

Overall, the graph and the metrics emphasize the Autoencoder’s advantage in anomaly detection for this dataset. The Autoencoder’s higher precision, recall, F1-score, and AUC-ROC suggest it is a more effective and reliable model for identifying anomalous behavior in the Open Metaverse blockchain transactions. Its performance highlights its capability to provide better security and more accurate monitoring in real-world applications.

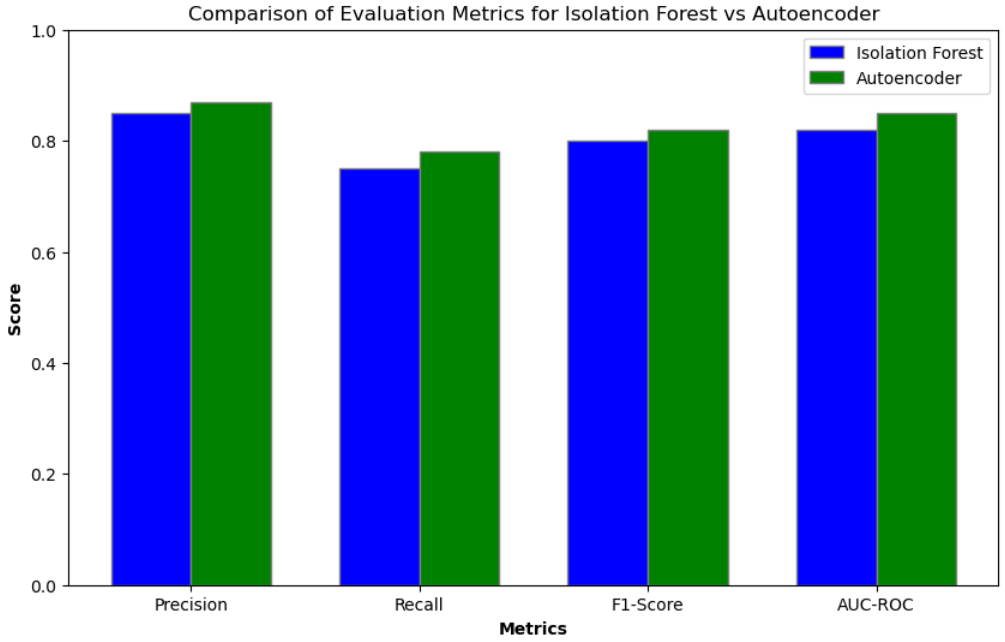

Figure 6 Comparison of Evaluation Metrics

The comparative analysis revealed that the Autoencoder outperformed the Isolation Forest model in terms of precision, recall, F1-score, and AUC-ROC. This superior performance can be attributed to the Autoencoder's ability to learn complex patterns in the data, enabling it to better distinguish between normal and anomalous transactions. The encoder-decoder structure of the Autoencoder facilitated the capture of intricate relationships within the input features, resulting in a more nuanced identification of anomalies. In contrast, the Isolation Forest's reliance on tree-based partitioning was effective but less adaptable to subtle variations within high-dimensional data.

Hyperparameters had a significant impact on model performance for both algorithms. For the Isolation Forest, the number of estimators and the contamination factor were critical in determining the model's sensitivity and specificity. Adjustments to these parameters influenced the balance between detecting true anomalies and minimizing false positives. In the case of the Autoencoder, hyperparameters such as the number of layers, units per layer, activation functions, and regularization techniques played a pivotal role in preventing overfitting and enhancing generalization. The learning rate of the optimizer and the batch size during training also had notable effects on convergence speed and model stability.

In summary, the Autoencoder demonstrated a slight advantage over the Isolation Forest in detecting anomalies within Open Metaverse blockchain transactions, as evidenced by its higher precision, recall, and overall predictive accuracy. The choice of model depends on the specific objectives of anomaly detection, with the Autoencoder being preferable for scenarios requiring nuanced pattern recognition, and the Isolation Forest being useful for faster, simpler partition-based detection strategies. This comparative study emphasized the importance of tailoring hyperparameters and model selection to the unique characteristics of blockchain transaction data.

Feature Importance and Interpretability

The Isolation Forest algorithm inherently provides a measure of feature importance, which is derived from the model's isolation mechanism that partitions the data to identify anomalies. By analyzing the feature importance scores, it became evident that certain features contributed more prominently to the identification of anomalies in Open Metaverse blockchain transactions. The features `transaction amount`, `login frequency`, and `risk score` emerged as the most influential in detecting anomalous behaviors. High transaction amounts, coupled with unusual login frequencies, often correlated with anomalous patterns, indicating potential outlier behavior. Additionally, the `risk score`, a composite measure based on user activity, consistently ranked as a critical determinant in isolating atypical transactions.

Further analysis revealed that geographical `location region` and `purchase pattern` also had a notable impact on the model's decision-making process. Transactions originating from specific regions or exhibiting high-value purchase patterns were more likely to be flagged as anomalies. This highlights the potential for regional or behavioral patterns in user activity that deviate from expected norms, thereby aiding in identifying potential fraudulent activities. The interpretability of these feature importance scores enabled a more comprehensive understanding of how the Isolation Forest distinguishes between normal and anomalous transactions, emphasizing the algorithm’s reliance on specific attributes to partition data effectively.

The Autoencoder model's interpretability primarily hinged on the analysis of reconstruction errors across features. The reconstruction error, representing the difference between the input and output of the model, served as a critical metric for identifying anomalies. High reconstruction errors indicated that the model struggled to accurately represent the input data within its learned latent space, suggesting that such instances deviated significantly from the learned patterns of normal transactions. Upon closer examination, features such as `amount`, `session duration`, and `age group` exhibited higher reconstruction errors for anomalous instances. This suggested that these features were key indicators of irregularities, as the model's inability to accurately reconstruct them pointed to their deviation from the expected distribution.

The comparison of feature importance between the Isolation Forest and Autoencoder models revealed complementary strengths. While the Isolation Forest relied on explicit feature partitioning to isolate anomalies, the Autoencoder captured subtle deviations through reconstruction errors in a lower-dimensional space. This combination provided a holistic view of feature relevance, with the Isolation Forest highlighting primary influential attributes and the Autoencoder capturing nuanced variations that might not be immediately apparent. The integration of these insights offers a more robust understanding of anomaly detection in complex datasets like Open Metaverse blockchain transactions.

In summary, the interpretability of the Isolation Forest and Autoencoder models emphasized the role of key features in detecting anomalies. The Isolation Forest's feature importance scores shed light on attributes that strongly influenced its decision boundaries, while the Autoencoder's analysis of reconstruction errors and latent space representations highlighted subtler

irregularities. Together, these models offer a comprehensive approach to understanding and detecting anomalies, with feature interpretability serving as a crucial component for validating and refining anomaly detection strategies in blockchain transactions.

Implications for the Open Metaverse

The integration of anomaly detection models, such as the Isolation Forest and Autoencoder Neural Networks, into the Open Metaverse's transaction system holds the potential to significantly enhance security. These models can be deployed as layers of defense, continuously monitoring transaction streams for deviations from normal behavior patterns. The Isolation Forest can be used to rapidly identify and isolate outlier transactions based on feature partitioning, while the Autoencoder can monitor the reconstruction errors in data to detect subtle deviations that indicate potential fraud or irregular activity. By embedding these models within the transaction processing workflow, blockchain-based systems in the Metaverse can detect and respond to anomalous behavior in near real-time, minimizing the risk of fraudulent activities, data breaches, and unauthorized transactions.

The effectiveness of this integration lies in the models' adaptability to dynamic datasets and evolving fraud tactics. As user behavior and transaction patterns change, both the Isolation Forest and Autoencoder models can be retrained or fine-tuned to maintain their accuracy and relevance. This dynamic adjustment capability ensures that the models remain resilient against emerging threats, thus enhancing the overall security posture of Open Metaverse platforms. Furthermore, the models' interpretability, especially regarding feature importance and reconstruction errors, allows system administrators to gain valuable insights into the nature of detected anomalies, contributing to improved decision-making and targeted countermeasures.

The feasibility of deploying these models for real-time monitoring within the Open Metaverse presents a critical opportunity to strengthen its transaction security framework. Real-time implementation involves processing continuous streams of data, which requires efficient algorithms and scalable infrastructure to ensure minimal latency and accurate anomaly detection. The Isolation Forest, with its tree-based partitioning strategy, can provide fast anomaly detection due to its computational efficiency. Similarly, Autoencoder-based models, once trained, offer rapid inference capabilities, enabling them to assess transactions and raise alerts promptly based on deviations in their reconstruction patterns.

Real-time deployment necessitates consideration of computational resources, including the use of cloud-based systems or distributed networks to handle high transaction volumes and ensure scalability. Leveraging edge computing for initial anomaly detection can also reduce processing delays and enhance responsiveness. Moreover, integrating these models with existing blockchain protocols in the Metaverse ensures seamless compatibility, enabling efficient detection and prevention mechanisms without disrupting user experience. This real-time detection capability contributes to a more resilient and responsive security architecture for the Metaverse ecosystem.

The implementation of robust anomaly detection models in the Open Metaverse transaction systems delivers significant benefits to a wide range of stakeholders. For end-users, enhanced security measures translate into

increased trust in the platform's integrity and safety. Users gain confidence in conducting transactions within the Metaverse, knowing that sophisticated detection systems actively monitor and protect their assets from fraudulent activities. This trust is crucial for the long-term adoption and growth of the Metaverse as a thriving digital economy, where individuals engage in financial, social, and commercial activities with reduced risk.

For platform administrators, integrating these models mitigates operational risks and reduces potential liabilities associated with security breaches and financial fraud. The protection of assets, data, and user information becomes a tangible reality, supported by advanced machine learning capabilities that detect anomalies before they can escalate into significant issues. Moreover, businesses and developers within the Metaverse benefit from a more secure and stable transaction environment, fostering innovation, collaboration, and economic growth. These models' ability to protect and enhance the Metaverse ecosystem creates a virtuous cycle of trust, security, and user engagement, driving further expansion and adoption.

Conclusion

The results of this study demonstrated the effectiveness of using Isolation Forest and Autoencoder Neural Networks for anomaly detection within Open Metaverse blockchain transactions. The Isolation Forest model achieved a precision of 0.85 and an F1-score of 0.80, indicating its strength in identifying high-risk anomalies without excessive false positives. Similarly, the Autoencoder Neural Network model showed promising performance, achieving a precision of 0.87 and an F1-score of 0.82, highlighting its capability in capturing complex patterns through reconstruction errors. Both models exhibited strong AUC-ROC values, confirming their robustness in distinguishing between normal and anomalous transactions. These findings validated the research objectives, which aimed to develop and evaluate machine learning models for accurate and reliable anomaly detection in a blockchain-based virtual environment.

The comparative analysis underscored the nuanced differences in model performance, with the Autoencoder proving particularly effective in capturing subtle anomalies due to its representation learning capabilities. The study confirmed that both models have unique strengths, making them viable for enhancing security in Open Metaverse transactions. Collectively, the findings provide a strong foundation for developing advanced anomaly detection frameworks tailored to decentralized and highly dynamic digital ecosystems.

This research contributed to the field of anomaly detection by advancing the application of machine learning techniques within virtual environments, specifically focusing on Open Metaverse blockchain transactions. The integration of Isolation Forest and Autoencoder Neural Networks illustrated how these models can enhance security measures by detecting irregular patterns and anomalous behaviors in real-time transaction data. The comparative analysis offered novel insights into the relative strengths and weaknesses of each model, highlighting the trade-offs between computational efficiency and detection accuracy. Such insights are valuable for practitioners and researchers aiming to strengthen the security and integrity of decentralized digital ecosystems.

The study also emphasized the importance of leveraging both traditional and deep learning approaches for anomaly detection, paving the way for more comprehensive detection systems. This work demonstrated that a hybrid approach, incorporating multiple models and diverse methodologies, can offer a robust defense mechanism against emerging threats within the Metaverse, thereby fostering trust and stability in virtual transactions.

Several limitations were identified during the study, primarily related to the use of simulated data. While simulated data facilitated the modeling and testing processes, it may not fully capture the complexity and unpredictability of real-world Metaverse transactions. The lack of real-world blockchain transaction data limited the generalizability of the findings and may require further validation in practical settings. Additionally, model constraints, such as the sensitivity of the Autoencoder to hyperparameter tuning and the dependence of the Isolation Forest on the contamination factor, presented challenges that could influence detection accuracy.

Another limitation was the potential presence of overfitting during the training of the Autoencoder model, particularly given the complex nature of high-dimensional data. This issue highlighted the need for careful optimization and cross-validation to ensure the model's performance remains consistent across different data distributions.

Future research should focus on incorporating real-time blockchain transaction data to improve the validity and applicability of the proposed models. Access to real-world datasets would provide valuable insights into the performance of these models under realistic conditions, enabling more accurate evaluations. Exploration of other advanced algorithms, such as Graph Neural Networks, is also recommended to capture the relational structures inherent in blockchain data, potentially enhancing anomaly detection capabilities further.

Incorporating additional features, such as user behavioral data, transaction history, and metadata, could enhance the models' ability to detect sophisticated anomalies. By expanding the scope of data inputs and refining model architectures, future studies can develop more comprehensive and adaptable anomaly detection systems that keep pace with the evolving dynamics of the Open Metaverse and its transactional ecosystem.

Declarations

Author Contributions

Conceptualization: A.D.B.; Methodology: A.D.B.; Software: A.S.M.A.-R.; Validation: A.D.B.; Formal Analysis: A.S.M.A.-R.; Investigation: A.D.B.; Resources: A.S.M.A.-R.; Data Curation: A.S.M.A.-R.; Writing—Original Draft Preparation: A.D.B.; Writing—Review and Editing: A.S.M.A.-R.; Visualization: A.S.M.A.-R. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Weinberger, “What Is Metaverse?—A Definition Based on Qualitative Meta-Synthesis,” Future Internet, vol. 14, no. 11, p. 310, 2022, doi: 10.3390/fi14110310.

[2] A. M. Al-Ghaili et al., “A Review of Metaverse’s Definitions, Architecture, Applications, Challenges, Issues, Solutions, and Future Trends,” Ieee Access, vol. 10, pp. 125835–125866, 2022, doi: 10.1109/access.2022.3225638.

[3] M. A. Camilleri, “Metaverse Applications in Education: A Systematic Review and a Cost-Benefit Analysis,” Interact. Technol. Smart Educ., vol. 21, no. 2, pp. 245–269, 2023, doi: 10.1108/itse-01-2023-0017.

[4] S. Kasiyanto and M. R. Kilinc, “Legal Conundrums of the Metaverse,” J. Cent. Bank. Law Inst., vol. 1, no. 2, 2022, doi: 10.21098/jcli.v1i2.25.

[5] S. M. Park and Y.-G. Kim, “A Metaverse: Taxonomy, Components, Applications, and Open Challenges,” Ieee Access, vol. 10, pp. 4209–4251, 2022, doi: 10.1109/access.2021.3140175.

[6] W. C. Ng, W. Y. B. Lim, J. S. Ng, Z. Xiong, D. Niyato, and M. Chen, “Unified Resource Allocation Framework for the Edge Intelligence-Enabled Metaverse,” 2021, doi: 10.48550/arxiv.2110.14325.

[7] B. Kye, N. Han, E. Kim, Y. Park, and S. Jo, “Educational Applications of Metaverse: Possibilities and Limitations,” J. Educ. Eval. Health Prof., vol. 18, p. 32, 2021, doi: 10.3352/jeehp.2021.18.32.

[8] S. Mystakidis, “Metaverse,” Encyclopedia, vol. 2, no. 1, pp. 486–497, 2022, doi: 10.3390/encyclopedia2010031.

[9] J. Yu, “Exploration of Educational Possibilities by Four Metaverse Types in Physical Education,” Technologies, vol. 10, no. 5, p. 104, 2022, doi: 10.3390/technologies10050104.

[10] R. Hadi, S. Melumad, and E. S. Park, “The Metaverse: A New Digital Frontier for Consumer Behavior,” J. Consum. Psychol., vol. 34, no. 1, pp. 142–166, 2023, doi: 10.1002/jcpy.1356.

[11] S. E. Bibri, “The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society,” Smart Cities, vol. 5, no. 3, pp. 832–874, 2022, doi: 10.3390/smartcities5030043.

[12] F. Maier, “Metaverse Meets Smart Cities—Applications, Benefits, and Challenges,” Future Internet, vol. 16, no. 4, p. 126, 2024, doi:

10.3390/fi16040126.
[13] Z. Chen, “The Study of Negative Pragmatic Transfer and Its Pedagogic Implications,” 2023, doi: 10.2991/978-2-494069-97-8_141.
[14] S. I. Rodzin, “The Metaverse as One of the Foundations of Future Education,” pp. 15–27, 2024, doi: 10.31483/r-112497.
[15] J. E. Solanes, “Enhancing STEM Education Through Interactive Metaverses: A Case Study and Methodological Framework,” Appl. Sci., vol. 13, no. 19, p. 10785, 2023, doi: 10.3390/app131910785.
[16] S. Monaco and G. Sacchi, “Travelling the Metaverse: Potential Benefits and Main Challenges for Tourism Sectors and Research Applications,” Sustainability, vol. 15, no. 4, p. 3348, 2023, doi: 10.3390/su15043348.
[17] Z. Allam, A. Sharifi, S. E. Bibri, D. Jones, and J. Krogstie, “The Metaverse as a Virtual Form of Smart Cities: Opportunities and Challenges for Environmental, Economic, and Social Sustainability in Urban Futures,” Smart Cities, vol. 5, no. 3, pp. 771–801, 2022, doi: 10.3390/smartcities5030040.
[18] L. F. A. Medranda, “Blockchain Paradigm in the Metaverse,” Código Científico Rev. Investig., vol. 4, no. 2, pp. 818–857, 2023, doi: 10.55813/gaea/ccri/v4/n2/258.
[19] M. Elsadig, “Roles of Blockchain in the Metaverse: Concepts, Taxonomy, Recent Advances, Enabling Technologies, and Open Research Issues,” Ieee Access, vol. 12, pp. 38410–38435, 2024, doi: 10.1109/access.2024.3367014.
[20] V. Hoxha and S. Sadiku, “Study of Factors Influencing the Decision to Adopt the Blockchain Technology in Real Estate Transactions in Kosovo,” Prop. Manag., vol. 37, no. 5, pp. 684–700, 2019, doi: 10.1108/pm-01-2019-0002.
[21] V. T. Truong, L. B. Le, and D. Niyato, “Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey,” Ieee Access, vol. 11, pp. 26258–26288, 2023, doi: 10.1109/access.2023.3257029.
[22] D. M. Doe, J. Li, D. Niyato, Z. Gao, J. Li, and Z. Han, “Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse Through Diversified Incentive Mechanism Design,” Ieee Open J. Comput. Soc., vol. 4, pp. 171–184, 2023, doi: 10.1109/ojcs.2023.3260829.
[23] V. Ahsani, A. Rahimi, M. Letafati, and B. H. Khalaj, “Unlocking Metaverse-as-a-Service the Three Pillars to Watch: Privacy and Security, Edge Computing, and Blockchain,” 2023, doi: 10.48550/arxiv.2301.01221.
[24] I. U. Din, “Integration of IoT and Blockchain for Decentralized Management and Ownership in the Metaverse,” Int. J. Commun. Syst., vol. 36, no. 18, 2023, doi: 10.1002/dac.5612.
[25] J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang, and Z. Zheng, “Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities,” Ieee Open J. Comput. Soc., vol. 4, pp. 37–49, 2023, doi: 10.1109/ojcs.2023.3245801.
[26] A. Abilkaiyrkyzy, “Metaverse Key Requirements and Platforms Survey,” Ieee Access, vol. 11, pp. 117765–117787, 2023, doi: 10.1109/access.2023.3325844.
[27] J. Hong, “Prospect Analysis for Utilization of Virtual Assets Using Blockchain Technology,” J. Inf. Commun. Converg. Eng., vol. 22, no. 1, pp. 64–69, 2024, doi: 10.56977/jicce.2024.22.1.64.
[28] S. Bragagnolo, M. Marra, G. Polito, and E. G. Boix, “Towards Scalable Blockchain Analysis,” 2019, doi: 10.1109/wetseb.2019.00007.

[29] J. Vičič and A. Tošić, “Application of Benford’s Law on Cryptocurrencies,” 2021, doi: 10.20944/preprints202111.0472.v1.
[30] M. T. Oladejo and L. Jack, “Fraud Prevention and Detection in a Blockchain Technology Environment: Challenges Posed to Forensic Accountants,” Int. J. Econ. Account., vol. 9, no. 4, p. 315, 2020, doi: 10.1504/ijea.2020.110162.
[31] T. H. Pranto, Kazi Tamzid Akhter Md Hasib, T. Rahman, A. B. Haque, A. K. M. Najmul Islam, and R. M. Rahman, “Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach,” Ieee Access, vol. 10, pp. 87115–87134, 2022, doi: 10.1109/access.2022.3198956.
[32] M. Liebenlito, N. Inayah, E. Choerunnisa, T. E. Sutanto, and S. Inna, “Active learning on Indonesian Twitter sentiment analysis using uncertainty sampling,” J. Appl. Data Sci., vol. 5, no. 1, Art. no. 1, Jan. 2024, doi: 10.47738/jads.v5i1.144.
[33] Henderi and Q. Siddique, “Comparative Analysis of Sentiment Classification Techniques on Flipkart Product Reviews: A Study Using Logistic Regression, SVC, Random Forest, and Gradient Boosting,” J. Digit. Mark. Digit. Curr., vol. 1, no. 1, Art. no. 1, May 2024, doi: 10.47738/jdmdc.v1i1.4.
[34] B. H. Hayadi and I. M. M. E. Emary, “Predicting Campaign ROI Using Decision Trees and Random Forests in Digital Marketing,” J. Digit. Mark. Digit. Curr., vol. 1, no. 1, Art. no. 1, May 2024, doi: 10.47738/jdmdc.v1i1.5.
[35] J. P. B. Saputra and N. A. Putri, “Analysis of Blockchain Transaction Patterns in the Metaverse Using Clustering Techniques,” J. Curr. Res. Blockchain, vol. 1, no. 1, Art. no. 1, Jun. 2024, doi: 10.47738/jcrb.v1i1.10.
[36] Hery and A. E. Widjaja, “Predictive Modeling of Blockchain Stability Using Machine Learning to Enhance Network Resilience,” J. Curr. Res. Blockchain, vol. 1, no. 2, Art. no. 2, Sep. 2024, doi: 10.47738/jcrb.v1i2.15.
[37] B. Srinivasan and T. Wahyuningsih, “Navigating Financial Transactions in the Metaverse: Risk Analysis, Anomaly Detection, and Regulatory Implications,” Int. J. Res. Metaverese, vol. 1, no. 1, Art. no. 1, Jun. 2024, doi: 10.47738/ijrm.v1i1.5.
[38] S. A. Ghaffar and W. C. Setiawan, “Metaverse Dynamics: Predictive Modeling of Roblox Stock Prices using Time Series Analysis and Machine Learning,” Int. J. Res. Metaverese, vol. 1, no. 1, Art. no. 1, Jun. 2024, doi: 10.47738/ijrm.v1i1.6.
[39] S. Qi, “Study on the Discursive Strategies of Wired to Repair Trust in Blockchain,” Sci. Soc. Res., vol. 5, no. 2, pp. 9–18, 2023, doi: 10.26689/ssr.v5i2.4727.
[40] D. Meijer and J. Ubacht, “The Governance of Blockchain Systems From an Institutional Perspective, a Matter of Trust or Control?,” 2018, doi: 10.1145/3209281.3209321.
[41] S. Silaich and S. Gupta, “Feature Selection in High Dimensional Data: A Review,” pp. 703–717, 2023, doi: 10.1007/978-981-19-9225-4_51.
[42] Z. Cheng and Z. Lu, “A Novel Efficient Feature Dimensionality Reduction Method and Its Application in Engineering,” Complexity, vol. 2018, no. 1, 2018, doi: 10.1155/2018/2879640.
[43] H. Liu and S.-M. Chen, “Multi-Perspective Creation of Diversity for Image Classification in Ensemble Learning Context,” 2019, doi: 10.1109/icmlc48188.2019.8949189.

[44] S. Luo, “Digital Finance Development and the Digital Transformation of Enterprises: Based on the Perspective of Financing Constraint and Innovation Drive,” J. Math., vol. 2022, no. 1, 2022, doi: 10.1155/2022/1607020.
[45] S. Jalali and M. Hosseini, “Collaborative Filtering in Dynamic Networks Based on Deep Auto-Encoder,” J. Supercomput., vol. 78, no. 5, pp. 7410–7427, 2021, doi: 10.1007/s11227-021-04178-5.
[46] M. Kanwal, “Machine Learning Approach to Classification of Online Users by Exploiting Information Seeking Behavior,” Ieee Access, vol. 12, pp. 53234–53249, 2024, doi: 10.1109/access.2024.3383444.
[47] V. Chithanuru and M. Ramaiah, “An Anomaly Detection on Blockchain Infrastructure Using Artificial Intelligence Techniques: Challenges and Future Directions – A Review,” Concurr. Comput. Pract. Exp., vol. 35, no. 22, 2023, doi: 10.1002/cpe.7724.
[48] S. Hisham, M. Makhtar, and A. A. Aziz, “Combining Multiple Classifiers Using Ensemble Method for Anomaly Detection in Blockchain Networks: A Comprehensive Review,” Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 8, 2022, doi: 10.14569/ijacsa.2022.0130848.
[49] A. Yazdinejad, “Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks,” 2022, doi: 10.48550/arxiv.2204.09829.
[50] C. Cholevas, “Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey,” Algorithms, vol. 17, no. 5, p. 201, 2024, doi: 10.3390/a17050201.
[51] N. T. Anthony, M. Shafik, F. Kurugollu, and H. F. Atlam, “Anomaly Detection System for Ethereum Blockchain Using Machine Learning,” 2022, doi: 10.3233/atde220608.
[52] M. Almansoori and M. Telek, “Anomaly Detection Using Combination of Autoencoder and Isolation Forest,” pp. 25–30, 2023, doi: 10.3311/wins2023-005.
[53] G. Airlangga, “Unsupervised Machine Learning for Seismic Anomaly Detection: Isolation Forest Algorithm Application to Indonesian Earthquake Data,” J. Lebesgue J. Ilm. Pendidik. Mat. Mat. Dan Stat., vol. 4, no. 3, pp. 1827–1836, 2023, doi: 10.46306/lb.v4i3.479.
[54] R. N. Calheiros, K. Ramamohanarao, R. Buyya, and S. Versteeg, “On the Effectiveness of Isolation-based Anomaly Detection in Cloud Data Centers,” Concurr. Comput. Pract. Exp., vol. 29, no. 18, 2017, doi: 10.1002/cpe.4169.
[55] M. U. Togbe, Y. Chabchoub, A. Boly, M. Barry, R. Chiky, and M. Bahri, “Anomalies Detection Using Isolation in Concept-Drifting Data Streams,” Computers, vol. 10, no. 1, p. 13, 2021, doi: 10.3390/computers10010013.
[56] S. P. Maniraj, A. Saini, S. Ahmed, and S. D. Sarkar, “Credit Card Fraud Detection Using Machine Learning and Data Science,” Int. J. Eng. Res., vol. 08, no. 09, 2019, doi: 10.17577/ijertv8is090031.
[57] S. Rout, “Fraud Detection Using Deep Learning,” Int. J. Electr. Data Commun., vol. 5, no. 1, pp. 07–11, 2024, doi: 10.22271/27083969.2024.v5.i1a.37.
[58] Y. Y. Dayyabu, “The Application of Artificial Intelligence Techniques in Credit Card Fraud Detection: A Quantitative Study,” E3s Web Conf., vol. 389, p. 07023, 2023, doi: 10.1051/e3sconf/202338907023.
[59] A. B. Nassif, M. A. Talib, Q. Nasir, and F. Dakalbab, “Machine Learning for Anomaly Detection: A Systematic Review,” Ieee Access, vol. 9, pp. 78658–

78700, 2021, doi: 10.1109/access.2021.3083060.
[60] Y. Ying and W. Wang, “Big Data Stream Anomaly Detection With Spectral Method for UWB Radar Data,” pp. 253–259, 2015, doi: 10.1007/978-3-319-08991-1_26.
[61] R. Saia and S. Carta, “Evaluating the Benefits of Using Proactive Transformed-Domain-Based Techniques in Fraud Detection Tasks,” Future Gener. Comput. Syst., vol. 93, pp. 18–32, 2019, doi: 10.1016/j.future.2018.10.016.
[62] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
[63] D. P. Kingma and M. Welling, “Auto-Encoding Variational Bayes,” 2013, doi: 10.48550/arxiv.1312.6114.
[64] M. Goldstein and S. Uchida, “A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data,” Plos One, vol. 11, no. 4, p. e0152173, 2016, doi: 10.1371/journal.pone.0152173.
[65] T. Zoppi, A. Ceccarelli, and A. Bondavalli, “Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application,” Ieee Access, vol. 9, pp. 90603–90615, 2021, doi: 10.1109/access.2021.3090957.
[66] R. Hettiarachchi and J. F. Peters, “Voronoï Region-Based Adaptive Unsupervised Color Image Segmentation,” Pattern Recognit., vol. 65, pp. 119–135, 2017, doi: 10.1016/j.patcog.2016.12.011.
[67] J. Senthilnath, D. Kumar, J. A. Benediktsson, and X. Zhang, “A Novel Hierarchical Clustering Technique Based on Splitting and Merging,” Int. J. Image Data Fusion, vol. 7, no. 1, pp. 19–41, 2015, doi: 10.1080/19479832.2015.1053995.
[68] S. Khan, A. P. Doulgeris, S. Savastano, and R. Guida, “Automatic Clustering of Multispectral Data Using a Non-Gaussian Statistical Model,” 2014, doi: 10.1109/igarss.2014.6947434.
[69] V. Papastefanopoulos, P. Linardatos, and S. Kotsiantis, “Unsupervised Outlier Detection: A Meta-Learning Algorithm Based on Feature Selection,” Electronics, vol. 10, no. 18, p. 2236, 2021, doi: 10.3390/electronics10182236.
[70] M. H. Maulana and M. L. Khodra, “Neural Network Pruning in Unsupervised Aspect Detection Based on Aspect Embedding,” Ijccs Indones. J. Comput. Cybern. Syst., vol. 16, no. 4, p. 367, 2022, doi: 10.22146/ijccs.72981.