Jurnal Informatika Ekonomi Bisnis

http://www.infeb.org

2024 Vol. 6 Iss. 2 Hal: 324-329 e-ISSN: 2714-8491

Deep Learning for Anomaly Detection and Fraud Analysis in Blockchain Transactions of the Open Metaverse

Gregorius Airlangga[1]✉

[1]Atma Jaya Catholic University of Indonesia

gregorius.airlangga@atmajaya.ac.id

Abstract

This study investigates the application of deep learning models for anomaly detection and fraud analysis within blockchain transactions of the Open Metaverse. Given the burgeoning complexity and scale of virtual environments, ensuring the integrity and security of blockchain transactions is paramount. We employed three deep learning architectures: Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM), to analyze and predict transactional anomalies. Using a dataset comprising 78,600 records of metaverse transactions, each model was rigorously evaluated through a 5-fold cross-validation approach, focusing on the Mean Squared Error (MSE) as the primary performance metric. The MLP model demonstrated superior predictive accuracy with the lowest average CV MSE, suggesting its effectiveness in capturing the intricate patterns of blockchain transactions. The study's findings highlight the nuanced capabilities of each model in addressing the specific challenges of fraud analysis and anomaly detection in the metaverse's blockchain environment. By providing a comparative analysis of these deep learning approaches, this research contributes to the strategic development of security measures in the Open Metaverse, promoting a secure and trustworthy digital economy.

Keywords: Anomaly Detection, Blockchain Transactions, Deep Learning, Open Metaverse, Fraud Analysis.

1. Introduction

The dawn of the 21st century has witnessed unprecedented growth in digital innovation, fundamentally altering the fabric of economic and social systems worldwide [1], [2], [3]. At the heart of this transformation lies the Open Metaverse, a concept that encapsulates the vision of a fully immersive, decentralized, and interoperable virtual space [4], [5] , [6]. It is a realm where digital and physical realities converge, offering boundless opportunities for interaction, commerce, and collaboration [7], [8], [9].

Within this digital expanse, blockchain technology emerges as the backbone, facilitating secure and transparent transactions, managing digital assets, and ensuring the integrity of virtual interactions among participants [10], [11], [12]. Yet, as these virtual environments burgeon in complexity and user base, they also become fertile ground for fraudulent activities and security breaches, challenging the very foundation of trust and security in the digital age [13], [14], [15]. Blockchain technology, since its inception on Bitcoin, has been the subject of intense scrutiny and exploration [16]. Its promise of decentralized security and transparency has led to diverse applications, from cryptocurrencies to supply chain management and beyond.

Recent scholarly work has extended blockchain's applicability to the burgeoning field of the metaverse, where it is poised to revolutionize how digital assets are managed and transactions are conducted [17]. Studies, such as those who explore the integration of blockchain into virtual environments, underscoring its potential to foster secure, user-centric digital ecosystems [18]. Despite these advancements, a critical review of the literature reveals a pronounced gap in research focused specifically on anomaly detection, fraud analysis, and predictive analytics within the nuanced context of metaverse blockchain transactions [19], [20], [21]. This gap points to an emergent need for specialized studies that address the unique challenges of ensuring transactional integrity and user security in these complex virtual spaces [22].

The imperative to fortify the Open Metaverse against fraud and security threats is more pressing than ever [23]. As virtual environments evolve, becoming more intricate and attracting millions of users, they also become more susceptible to sophisticated fraudulent schemes and security vulnerabilities [24]. Current state-of-the-art approaches in anomaly detection and fraud analysis in blockchain systems often leverage advanced machine learning and deep learning techniques [25]. While effective in many traditional settings, these models may not fully account for the dynamic and intricate nature of transactions within the metaverse, where the diversity of user interactions and transaction types adds layers of complexity to detection efforts [26]. The rapid evolution of both blockchain technology and virtual environments necessitates an ongoing commitment to innovation in security measures, with a focus on developing models that are both adaptable and robust against emerging threats [27].

Accepted: 05-04-2024 | Revision: 10-04-2024 | Publication: 30-06-2024 | doi: 10.37034/infeb.v6i2.865

This research is driven by the ambitious goal of pioneering a comprehensive framework for anomaly detection and fraud analysis tailored to the Open Metaverse's blockchain transactions. Leveraging a rich and diverse dataset that encapsulates a wide spectrum of transaction types, user behaviors, and risk profiles, this study aims to fill the existing research gap. It seeks to transcend conventional security paradigms, proposing an approach that is nuanced enough to navigate the complexities of the metaverse, thereby enhancing the security, transparency, and trustworthiness of blockchain transactions in virtual spaces.

The examination of the current literature and technological advancements uncovers a notable disconnect between the theoretical capabilities of existing anomaly detection models and the practical realities of the metaverse. Traditional models, while foundational, often lack the specificity and adaptability required to tackle the layered and evolving nature of metaverse transactions. This discrepancy underscores a critical research gap: the need for anomaly detection and fraud analysis methodologies that are expressly designed for the metaverse context [28], [29], [30]. Such methodologies must not only consider the unique transactional dynamics and user behaviors inherent to virtual worlds but also anticipate and adapt to their rapid evolution.

In response to this identified gap, the present study makes several pivotal contributions to the field. Firstly, it introduces an integrated deep learning-based approach to anomaly detection and fraud analysis, explicitly designed for the metaverse's blockchain transactions. By employing a suite of sophisticated models—including multi-layer perceptrons (MLP), convolutional neural networks (CNN), and long short-term memory (LSTM) networks—this research offers a nuanced and powerful toolset for identifying and analyzing anomalies in virtual transactions. Furthermore, through comprehensive testing and validation on a novel dataset, the study not only enriches theoretical understanding but also delivers actionable insights for practitioners seeking to safeguard the Open Metaverse. The detailed comparative analysis of model performances sheds light on their practical implications, providing a valuable reference for future efforts to enhance transaction security in virtual environments.

Building on this introduction, the article unfolds as follows: Section 2 delineates the research methodology, encompassing the dataset's composition, the development of the deep learning models, and the criteria employed for their evaluation. Section 3 presents the empirical findings, detailing the performance of each model in detecting anomalies and analyzing fraud within the dataset. In addition, it discusses these results in the broader context of metaverse security, drawing comparisons among the models and elucidating their practical applications and implications. The final section, Section 4, concludes the paper by reflecting on the study's limitations and suggesting avenues for future research, emphasizing the need for continuous innovation in the dynamic landscape of metaverse security.

2. Research Method

2.1. Dataset Description

The foundational dataset for this study is an extensive collection of 78,600 records, each one representing a unique blockchain transaction within the vibrant ecosystem of the Open Metaverse. This dataset is not merely a collection of transactional data; it represents a meticulously curated assemblage that encapsulates the multifaceted nature of virtual economic interactions. Through its detailed and varied attributes, the dataset serves as a critical tool for understanding and analyzing the complexities of blockchain transactions, particularly focusing on anomaly detection and fraud analysis.

Each record in the dataset encompasses a range of attributes that together paint a comprehensive picture of the transactional landscape in the metaverse. These attributes include the precise moment of each transaction captured through timestamps, revealing patterns and anomalies across different times. The transaction amount in simulated currency offers insights into the scale of activities, highlighting transactions that are unusually large or small compared to typical patterns. The nature of the transaction is classified into various types such as transfers, sales, purchases, scams, and phishing, each providing a lens into the transaction's intent and context.

Geographical data, represented through the location and IP prefix, anchors each transaction in a physical and digital space, aiding in the identification of regional trends or anomalies. Behavioral patterns emerge from the analysis of login frequency and session duration, where deviations from the norm may indicate suspicious activities. Additionally, the dataset provides insights into purchasing behaviors and user demographics, categorized into different age groups, offering a nuanced view of user interaction and engagement within the metaverse. Central to the dataset's utility for this research is the calculated risk score for each transaction, which synthesizes various transaction characteristics and user behaviors into a singular measure of potential risk. Moreover, the inclusion of anomaly labels for each record, classifying transactions into high, moderate, or low risk, sets the groundwork for a systematic and data-driven approach to anomaly detection and fraud analysis.

The dataset's attributes were carefully selected to ensure a holistic and in-depth analysis of blockchain transactions in the metaverse. The temporal details like timestamps and the hour of the day facilitate an exploration of time-based patterns, while the transaction types and amounts provide a direct insight into the

transaction's nature and scale. Geographical and digital identifiers like location regions and IP prefixes offer a contextual backdrop for each transaction, essential for identifying location-based and network-related anomalies. User behavior is intricately detailed through login frequencies and session durations, along with purchase patterns and age demographics, all of which contribute to a layered understanding of user interactions and potential deviations that signify fraudulent or anomalous activities. This behavioral and transactional fusion within the dataset provides a robust foundation for developing sophisticated models that can navigate the complexities of blockchain-based transactions in virtual environments.

In essence, the dataset not only underpins the analytical aspects of this research but also enriches the understanding of blockchain transactions' dynamics in the Open Metaverse. By offering a comprehensive and detailed view of the virtual economic interactions, it enables a nuanced approach to detecting. Other than that, it also analyzing anomalies, paving the way for more secure and trustworthy blockchain operations in these expansive digital realms, the data can be downloaded from [31].

2.2. Data Preprocessing

In the realm of data science, especially when dealing with complex and multifaceted datasets like the one used in this study on blockchain transactions within the Open Metaverse, preprocessing stands as a crucial step to prepare the raw data for analysis. This process encompasses several key tasks, notably feature selection and encoding, as well as scaling, each aimed at refining the dataset to ensure its readiness for the subsequent modeling phase. The initial phase of preprocessing begins with the judicious selection of features. This involves evaluating the dataset's variables to identify those that hold predictive value for the research objectives. In this context, attributes such as 'timestamp', 'sending_address', and 'receiving_address' were assessed and deemed non-predictive for the purpose of anomaly detection and fraud analysis. Consequently, these attributes were removed from the dataset to streamline the analysis focus on the most relevant features. What remains are categorical variables including 'transaction_type', 'location_region', 'purchase_pattern', and 'age_group', each of which plays a significant role in characterizing the transactions.

Given the categorical nature of these remaining attributes, the next logical step in the preprocessing journey involves encoding these variables. This is where the LabelEncoder method comes into play, transforming the categorical labels into numerical formats. Such transformation is imperative as it translates the qualitative data into a quantifiable form that is digestible for deep learning models, which inherently process numerical input. The act of encoding is more than a mere conversion; it's a necessary translation that bridges the gap between human-understandable categories and machine-readable numbers, enabling the subsequent analytical processes to occur seamlessly.

Following the feature selection and encoding, the dataset undergoes scaling, a process aimed at normalizing the data. The scaling phase is pivotal, especially considering the heterogeneous nature of the dataset where variables can span various ranges. To mitigate the risk of certain features disproportionately influencing the model due to their scale, the StandardScaler method is employed. This scaling technique standardizes the features of the dataset, ensuring each has a mean of zero and a standard deviation of one. This normalization is crucial for the performance and accuracy of deep learning models, which can be sensitive to the scale of input features. By applying scaling, we not only homogenize the data but also facilitate a more balanced and equitable learning process, where each feature contributes equally to the model's predictive capability. In essence, the data preprocessing stage, encompassing feature selection and encoding followed by scaling, is an intricate process that sets the foundation for the effective application of deep learning models. It is through these meticulous preparations that the dataset is refined and optimized, rendering it suitable for the sophisticated analyses required to uncover the nuances of anomaly detection and fraud analysis in the blockchain transactions of the Open Metaverse. Through these efforts, the raw data is transformed into a clean, standardized, and model-ready format, laying the groundwork for the analytical endeavors that follow.

2.3. Deep Learning Models

In this research, the challenge of anomaly detection and fraud analysis within the Open Metaverse's blockchain transactions is tackled using three sophisticated deep learning architectures: Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM). These models are meticulously designed to unravel the intricate patterns and anomalies hidden within the transaction data, each bringing a unique perspective and set of capabilities to the analysis. The MLP model stands as the cornerstone of this deep learning approach. Constructed with an input layer that aligns with the dimensionality of the preprocessed dataset, the MLP structure progresses through a series of hidden layers, specifically three, configured with 256, 128, and 64 neurons respectively. The configuration of these layers is not arbitrary; it's a deliberate design to incrementally refine and distill the information as it passes through the network. Employing the Rectified Linear Unit (ReLU) as the activation function for introducing non-linearity, the model's formulation can be encapsulated as presented in the Equation 1.

$$a(x) = max(0, x) \quad (1)$$

Where a(x) is the activation output for an input x. To combat the risk of overfitting—a common pitfall in deep learning—the model integrates Dropout layers at a strategic rate of 0.2, essentially randomly deactivating a portion of the neurons during training to encourage a more generalized model representation. The culmination of this architecture is an output layer with a singular neuron, reflective of the model's task to predict the continuous risk score associated with each transaction. This MLP model is optimized using the Adam optimizer, a popular choice for deep learning tasks, governed by the Equation 2.

$$\theta_{t+1} = \theta_t - \frac{\eta}{\sqrt{\widehat{v_t}+\epsilon}}\widehat{m_t} \quad (2)$$

Where θ represents the parameters, η the learning rate, the bias-corrected estimates of the first and second moments of the gradients, and ϵ a small scalar to prevent division by zero. The model's performance is quantified using the mean squared error (MSE) loss function, capturing the average squared difference between the predicted and actual risk scores. Transitioning to the CNN model, this architecture is tailored for analyzing one-dimensional data, making it particularly adept at identifying localized patterns within the transaction attributes. The journey through this model begins with a Conv1D layer featuring 128 filters and a kernel size of 3, followed by a MaxPooling1D layer designed to condense the information and accentuate prominent features. This is further complemented by another Conv1D layer housing 64 filters, facilitating a deeper analysis of the data nuances. The output from these convolutional layers is then flattened, preparing it for transition through a dense layer of 64 neurons, and eventually to the output layer. Similar to the MLP, the CNN employs the ReLU activation function and adheres to the MSE loss function for performance evaluation.

The LSTM model is intricately crafted to capture the dynamic, sequential nature of the transaction data, offering a window into the temporal patterns that may elude other models. It is composed of an initial LSTM layer with 100 neurons, configured to return sequences to a subsequent LSTM layer of 50 neurons. This sequential processing is interspersed with Dropout layers at a rate of 0.2 to safeguard against overfitting. The output from these LSTM layers flows into a dense layer, leading to the final prediction output.

The ReLU function also finds its place in this model, enhancing the LSTM's capability to model non-linear relationships within the data. The optimization of this LSTM model follows the same Adam optimizer framework, aiming to fine-tune the model parameters for optimal prediction accuracy of the risk scores. Through these deep learning models—MLP, CNN, and LSTM—the research navigates the complexities of blockchain transaction data, striving to uncover the underlying patterns indicative of anomalies and fraudulent activities. Each model's distinct structure and operational mechanics offer a specialized approach to analyzing the data, ensuring a comprehensive and multifaceted analysis aligned with the intricate dynamics of blockchain transactions in the Open Metaverse.

2.4. Model Evaluation

In the pursuit of a comprehensive and rigorous evaluation of the performance of the deep learning models employed in this research—namely the Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM)—the methodology of K-Fold Cross-Validation is meticulously applied. This methodological choice is not arbitrary; it reflects a commitment to ensuring the reliability and generalizability of the models under scrutiny. By adopting a 5-split K-Fold Cross-Validation approach, the evaluation process transcends the limitations of a singular dataset partitioning. Instead, it ensures that each model is afforded the opportunity to learn and be tested across multiple, distinct subsets of the dataset. This iterative process of training and testing provides a more nuanced and comprehensive assessment of each model's ability to generalize, thereby offering a robust estimate of its performance across varied data scenarios.

Central to the evaluation of these models is the Mean Squared Error (MSE), a metric that serves as the cornerstone for assessing predictive accuracy. The choice of MSE as the primary metric is guided by its straightforward yet profound ability to quantify the difference between the models' predicted risk scores and the actual scores from the dataset. By calculating the average of the squared differences, the MSE offers an unambiguous measure of the models' performance, encapsulating both the variance and the bias in the predictions. Mathematically, the MSE is defined as Equation 3.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2 \quad (3)$$

In this equation, n represents the total number of observations, Yi denotes the actual risk score for the ith observation, and ^Yi symbolizes the predicted risk score for the same observation. Through the lens of the MSE, each model's predictions are scrutinized against the ground truth, enabling a direct and meaningful comparison of their predictive accuracies. This methodical approach to model evaluation, anchored by the K-Fold Cross-Validation method and quantified through the MSE, ensures a rigorous and transparent assessment of the models. It not only highlights their respective strengths and weaknesses in predicting transaction risk scores but also sets a precedent for the level of scrutiny required in the evolving field of anomaly detection and fraud analysis within the Open Metaverse's blockchain transactions. By adhering to this

robust evaluation framework, the research strives to contribute valuable insights into the capabilities of deep learning models, guiding future efforts in the quest for secure and trustworthy blockchain transactions in virtual environments.

3. Result and Discussion

The evaluation of the three deep learning models, Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM), has yielded insightful findings in the context of anomaly detection and fraud analysis within the Open Metaverse's blockchain transactions. These models were assessed based on their Mean Squared Error (MSE) performance across a 5-fold cross-validation process, providing a robust and generalizable measure of their predictive accuracy. These models are presented in the Table 1.

Table 1. Deep Learning Performance

Model Name	Average CV MSE
MLP	0.000717
CNN	0.000961
LSTM	0.001059

The MLP model demonstrated the best performance with the lowest average CV MSE of 0.000717, suggesting that it was most effective in capturing the underlying patterns and anomalies in the transaction data. The strength of the MLP in this context can be attributed to its architectural simplicity and efficiency in handling tabular data, which often characterizes transaction datasets. This result underscores the MLP's capability to model the relationships between variables effectively, providing a solid baseline for anomaly detection and fraud analysis tasks.

On the other hand, the CNN model, with an average CV MSE of 0.000961, showed slightly less accuracy compared to the MLP. CNNs, known for their prowess in identifying spatial and temporal patterns in data, may not have fully leveraged their strengths in this application. The one-dimensional nature of the transaction data might have limited CNN's ability to extract the complex features typically found in higher-dimensional data like images or multi-channel signals.

The LSTM model recorded an average CV MSE of 0.001059, the highest among the three models. Despite LSTMs being renowned for their ability to capture long-term dependencies and temporal dynamics in sequence data, this indicates that the sequential nature of the transaction data did not significantly influence the model's ability to predict anomalies. The result might reflect the complexity and training challenges associated with LSTM models, including their sensitivity to parameter settings and the tendency to overfit on smaller or less variant datasets.

The findings from this study have important implications for anomaly detection and fraud analysis in blockchain transactions. The superior performance of the MLP model suggests that for the type of structured, tabular data typical of transaction logs, simpler, feed-forward neural network architectures. As this might often be sufficient and more efficient than more complex models like CNNs and LSTMs.

4. Conclusion

This research explored anomaly detection and fraud analysis in Open Metaverse's blockchain transactions, using deep learning models: Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM). It found that MLP, with its straightforward architecture, surpassed CNN and LSTM in predictive accuracy, as shown by the lowest mean squared error (MSE). This highlights MLP's strength in processing structured transaction data and suggests that complexity doesn't necessarily enhance performance in anomaly detection. Despite higher MSEs, CNN and LSTM's capabilities in identifying spatial and temporal data patterns remain valuable, especially for data with pronounced temporal or spatial characteristics. This study not only compares model performance but also stresses the importance of model selection based on data specifics. Future research could investigate model integration or hybrid approaches to improve accuracy and robustness, or apply these models to other metaverse areas like virtual asset management or user interaction, promising further significant findings.

References

[1] Shukla, S., Bisht, K., Tiwari, K., & Bashir, S. (2023). Comparative Study of the Global Data Economy. *In Data Economy in the Digital Age* (pp. 63–86). https://doi.org/10.1007/978-981-99-7677-5_4

[2] Akour, M., & Alenezi, M. (2022). Higher education future in the era of digital transformation. *Education Sciences*, *12*(11), 784. https://doi.org/10.3390/educsci12110784

[3] Chipangamate, N. S., & Nwaila, G. T. (2023). Assessment of challenges and strategies for driving energy transitions in emerging markets: A socio-technological systems perspective. *Energy Geoscience*, 100257. https://doi.org/10.1016/j.engeos.2023.100257

[4] Jamshidi, M., Dehghaniyan Serej, A., Jamshidi, A., & Moztarzadeh, O. (2023). The meta-metaverse: ideation and future directions. *Future Internet*, *15*(8), 252. https://10.3390/fi15080252

[5] Chatzopoulou, I., Tsoutsa, P., & Fitsilis, P. (2023). How Metaverse is Affecting Smart Cities Economy. *In Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics* (pp. 254–259).

[6] Chen, H., Duan, H., Abdallah, M., Zhu, Y., Wen, Y., Saddik, A. E., & Cai, W. (2023). Web3 Metaverse: State-of-the-art and vision. ACM Transactions on Multimedia Computing, *Communications, and Applications*, *20*(4), 1–42. https://doi.org/10.1145/3630258

[7] Aljanabi, M., & Mohammed, S. Y. (2023). Metaverse: open possibilities. *Iraqi Journal For Computer Science and Mathematics*, *4*(3), 79–86. https://doi.org/10.52866/ijcsm.2023.02.03.007

[8] Ajani, Y. A., Enakrire, R. T., Oladokun, B. D., & Bashorun, M. T. (2023). Reincarnation of libraries via metaverse: A pathway for a sustainable knowledge system in the digital age. *Business Information Review*, *40*(4), 191–197. https://doi.org/10.1177/02663821231208044

[9] Koohang, A., Nord, J. H., Ooi, K.-B., Tan, G. W.-H., Al-Emran, M., Aw, E. C.-X., Baabdullah, A. M., Buhalis, D., Cham, T.-H., Dennis, C., et al. (2023). Shaping the metaverse into reality: a holistic multidisciplinary understanding of opportunities, challenges, and avenues for future investigation. *Journal of Computer Information Systems*, *63*(3), 735–765. https://doi.org/10.1080/08874417.2023.2165197

[10] Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges, and future research directions. *Electronics*, *11*(4), 630. https://doi.org/10.3390/electronics11040630

[11] Oladejo, M. T. (2023). *Blockchain technology: Disruptor or enhancer to the accounting and auditing profession* (Doctoral dissertation, The University of Waikato).

[12] Mourtzis, D. (2023). The Metaverse in Industry 5.0: A Human-Centric Approach towards Personalized Value Creation. *Encyclopedia*, *3*(3), 1105–1120. https://doi.org/10.3390/encyclopedia3030080

[13] Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, *23*(19), 8015. https://doi.org/10.3390/s23198015

[14] Grech, A. (2023). *Young people & information. A manifesto*. The 3CL Foundation.

[15] Jones, M. O. (2022). *Digital authoritarianism in the Middle East: Deception, disinformation and social media*. Hurst Publishers.

[16] Kyriazis, N. A. (2020). Is Bitcoin similar to gold? An integrated overview of empirical findings. *Journal of Risk and Financial Management*, *13*(5), 88. https://doi.org/ 10.3390/jrfm13050088

[17] Ud Din, I., Awan, K. A., Almogren, A., & Rodrigues, J. J. P. C. (2023). Integration of IoT and blockchain for decentralized management and ownership in the metaverse. International *Journal of Communication Systems*, *36*(18). https://doi.org/10.1002/dac.5612

[18] Bao, N., Nakazato, J., Muhammad, A., Javanmardi, E., & Tsukada, M. (2023). Towards a Trusted Inter-Reality: Exploring System Architectures for Digital Identification. *In Proceedings of the 13th International Conference on the Internet of Things* (pp. 270–275).

[19] Huynh-The, T., Pham, Q.-V., Pham, X.-Q., Nguyen, T. T., Han, Z., & Kim, D.-S. (2023). Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence*, *117*, 105581. https://doi.org/10.1016/j.engappai.2022.105581

[20] Ressi, D., Romanello, R., Piazza, C., & Rossi, S. (2024). AI-enhanced blockchain technology: A review of advancements and opportunities. *Journal of Network and Computer Applications*, 103858. https://doi.org/10.1016/j.jnca.2024.103858

[21] Ma, W., & Huang, K. (2022). *Blockchain and Web3: Building the cryptocurrency, privacy, and security foundations of the metaverse*. John Wiley & Sons.

[22] Albshaier, L., Almarri, S., & Hafizur Rahman, M. M. (2024). A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. *Computers*, *13*(1), 27. https://doi.org/10.3390/computers13010027

[23] Mammadova, A. (2023). Digital big-bang Metaverse: opportunities and threats.

[24] Salahdine, F., Han, T., & Zhang, N. (2023). Security in 5G and beyond recent advances and future challenges. *Security and Privacy*, *6*(1), e271. https://doi.org/10.1002/spy2.271

[25] Diro, A., Chilamkurti, N., Nguyen, V.-D., & Heyne, W. (2021). A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. *Sensors*, *21*(24), 8320. https://doi.org/10.3390/s21248320

[26] Truong, V. T., Le, L., & Niyato, D. (2023). Blockchain meets metaverse and digital asset management: A comprehensive survey. *IEEE Access*, *11*, 26258–26288. https://doi.org/10.1109/ACCESS.2023.3257029

[27] Ullah, N., Mugahed Al-Rahmi, W., Alzahrani, A. I., Alfarraj, O., & Alblehai, F. M. (2021). Blockchain technology adoption in smart learning environments. *Sustainability*, *13*(4), 1801. https://doi.org/10.3390/su13041801

[28] Zawish, M., Dharejo, F. A., Khowaja, S. A., Raza, S., Davy, S., Dev, K., & Bellavista, P. (2024). AI and 6G into the metaverse: Fundamentals, challenges and future research trends. *IEEE Open Journal of the Communications Society*, *5*, 730–778. https://doi.org/10.1109/OJCOMS.2023.3349465

[29] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, *25*(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

[30] Park, S.-M., & Kim, Y.-G. (2022). A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access*, *10*, 4209–4251. https://doi.org/10.1109/ACCESS.2021.3140175

[31] Janjua, F. I. (2023). Metaverse Financial Transactions Dataset. Retrieved April 4, 2024, from https://www.kaggle.com/datasets/faizaniftikharjanjua/metaverse-financial-transactions-dataset