IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 July 2024, accepted 6 August 2024, date of publication 9 August 2024, date of current version 20 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3441106

RESEARCH ARTICLE

Enhancing Blockchain Security Against Data Tampering: Leveraging Hybrid Model in Multimedia Forensics and Multi-Party Computation for Supply Chain Data Protection

UMAR ISLAM[1], ABDULLAH ALSHAMMARI[2], (Member, IEEE), ZAID ALZAID[3], ADEEL AHMED[4], SAIMA ABDULLAH[4], SAMAN IFTIKHAR[5], (Member, IEEE), SHAIKHAN BAWAZEER[5], AND MUHAMMAD IZHAR[6]

[1]Department of Computer Science, Iqra National University, Swat Campus, Swat, Khyber Pakhtunkhwa 25100, Pakistan
[2]College of Computer Science and Engineering, University of Hafr Al Batin, Hafar Al Batin 31991, Saudi Arabia
[3]Department of Computer Science, College of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia
[4]Department of Computer Science, Faculty of Computing, The Islamia University of Bahawalpur, Bahawalpur, Punjab 63100, Pakistan
[5]Faculty of Computer Studies, Arab Open University, Riyadh 84901, Saudi Arabia
[6]Department of Computer Science and Information Technology, Superior University, Lahore, Punjab 54000, Pakistan

Corresponding author: Adeel Ahmed (adeelmcs@gmail.com)

This work was supported by Arab Open University (AOU), Saudi Arabia, through AOU Research Fund under Grant AOUKSA-524008.

ABSTRACT Over the past few years, there has been a notable surge in the integration of Blockchain technology into supply chain management systems. This integration holds the promise of enhanced transparency, security, and efficiency in monitoring the movement of goods and services. This study presents a novel approach aimed at fortifying privacy and accuracy within blockchain-based supply chain management systems. The methodology integrates Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) units with secure multi-party computation (MPC) and differential privacy techniques as a hybrid model. The objective is to safeguard the confidentiality of transaction data while enabling precise detection of media tampering. Performance evaluation revolves around three key aspects: accuracy, privacy preservation, and computational efficiency. In terms of accuracy assessment, the proposed hybrid approach is benchmarked against traditional machine learning algorithms including Support Vector Machines (SVM), k-Nearest Neighbors (KNN), and Random Forest. Results indicate superior performance, with the proposed hybrid method achieving an accuracy of 0.95, outperforming conventional algorithms. Precision, recall, and F1-score metrics further confirm the effectiveness of the approach in accurately identifying media tampering instances. Privacy preservation capabilities are evaluated through differential privacy techniques, revealing the method's ability to inject controlled noise into the data to protect individual privacy. Results demonstrate varying levels of privacy preservation across different settings, highlighting the trade-off between privacy and data utility. Computational efficiency is also scrutinized, considering the additional overhead introduced by privacy preservation mechanisms and secure MPC protocols. While there is a slight increase in computational time, the proposed approach maintains reasonable training and inference times, ensuring practical applicability in real-world scenarios.

INDEX TERMS Differential privacy, LSTM-GRU units, media tampering detection, block-chain, supply chain management.

I. INTRODUCTION

In recent years, there has been a surge in interest and research efforts towards addressing privacy concerns in

The associate editor coordinating the review of this manuscript and approving it for publication was Nafees Mansoor.

various domains, particularly in the context of data sharing and collaborative learning [1], [2]. With the proliferation of blockchain technology, researchers have explored its potential for enhancing data privacy and security in decentralized systems. This interest stems from the inherent characteristics of blockchain, such as immutability, decentralization, and transparency, which make it suitable for ensuring the integrity and confidentiality of sensitive data [3]. However, despite the growing body of literature on blockchain-based privacy solutions, several challenges remain unresolved, especially concerning the integration of blockchain with advanced machine learning techniques.

Previous studies have demonstrated the efficacy of blockchain in preserving data privacy in diverse applications, including human resource management [4], smart contracts [5], Internet of Medical Things (IoMT) devices [6], and federated learning systems [7]. These works have highlighted the importance of leveraging blockchain's cryptographic features to protect sensitive information from unauthorized access and tampering [8], [9]. For instance, Alzubi et al. proposed a blockchain-enabled federated learning framework for preserving the privacy of electronic health records using convolutional neural networks (CNNs) [10]. Similarly, Jiao et al. introduced a federated learning scheme based on personalized differential privacy and reputation mechanisms, leveraging blockchain for secure data aggregation and model updates [11].

Despite these advancements, existing approaches still face significant limitations, particularly in terms of scalability, computational overhead, and data privacy guarantees. Moreover, many studies focus solely on individual aspects of privacy preservation, overlooking the need for comprehensive solutions that address the multifaceted nature of privacy challenges in decentralized environments. For example, while blockchain ensures data integrity and auditability, it may not provide sufficient protection against privacy breaches resulting from data inference attacks or model inversion techniques [12], [13], [14], [15], [16].

Furthermore, the integration of blockchain with advanced machine learning models, such as long short-term memory (LSTM) networks and multi-party computation (MPC), remains relatively unexplored. Combining these techniques could offer enhanced privacy guarantees by leveraging the strengths of each approach. For example, LSTM networks are well-suited for sequential data processing tasks, making them suitable for analyzing multimedia content in forensic applications [1], [17], [18], [19], [20], [21]. On the other hand, MPC techniques enable secure computation across multiple parties without revealing sensitive information, making them ideal for protecting supply chain data [2], [22], [23], [24], [25], [26], [27], [28].

In light of these considerations, this paper proposes a novel approach to address the privacy challenges in decentralized systems by leveraging a hybrid LSTM-1D GRU model in multimedia forensics and multi-party computation for supply chain data protection. By integrating blockchain technology with advanced machine learning techniques, our framework aims to provide robust privacy preservation mechanisms while ensuring data integrity [29], [30], [31], confidentiality [32], and accountability in collaborative environments [33], [34], [35], [36]. Through empirical evaluations and case studies, we demonstrate the effectiveness and practicality of our approach in real-world scenarios.

This study contributes to the advancement of secure and efficient supply chain management practices by addressing privacy concerns and enhancing media tampering detection capabilities. The proposed approach offers a promising framework for improving the security and reliability of blockchain-based supply chain management systems..

II. RELATED WORK

Blockchain technology has gained significant attention for its potential to enhance data privacy, security, and transparency across various applications, including supply chain management. Recent advancements in integrating blockchain with machine learning techniques aim to address privacy concerns and improve the accuracy of media tampering detection. This literature review systematically examines the latest studies related to blockchain-based privacy-preserving methods, focusing on their applications in supply chain management and multimedia forensics.

Several studies have explored the integration of blockchain with privacy-preserving techniques to protect sensitive data in supply chain management systems. Huang et al. [2] proposed a decentralized federated learning privacy-preserving framework based on blockchain, highlighting the potential of blockchain to secure collaborative learning processes. This approach addresses privacy concerns by distributing the learning process across multiple nodes while maintaining data integrity and confidentiality.

In another study, Rashmi et al. [3] investigated the use of blockchain for data privacy in human resource management. Their research emphasizes the potential of blockchain to secure sensitive HR data, although it does not delve deeply into the forensic aspects of blockchain security. Similarly, Naidu et al. [4] presented an efficient smart contract for privacy-preserving authentication in blockchain using zero-knowledge proof, focusing on authentication mechanisms without addressing data tampering issues.

The integration of advanced machine learning models, such as Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), with blockchain technology has shown promise in enhancing data security and accuracy. Alzubi et al. [10] introduced a blockchain-enabled federated learning framework for preserving the privacy of electronic health records using Convolutional Neural Networks (CNNs). This approach leverages the strengths of both blockchain and machine learning to secure sensitive medical data while maintaining high accuracy in health record analysis.

Jiao et al. [11] proposed a blockchain-based federated learning scheme incorporating personalized differential privacy and reputation mechanisms. Their study demonstrates

the effectiveness of integrating differential privacy techniques with blockchain to protect individual data while ensuring accurate model updates in federated learning settings.

Differential privacy and secure multi-party computation (MPC) are key techniques used to enhance privacy in blockchain applications. Feng et al. [1] discussed privacy-preserving federated learning using multi-input functional proxy re-encryption, highlighting the role of differential privacy in securing collaborative learning processes. Their study emphasizes the importance of balancing privacy and data utility, a common challenge in privacy-preserving techniques.

Similarly, Rahmadika et al. [5] introduced a blockchain-based privacy preservation scheme for misbehavior detection in lightweight Internet of Medical Things (IoMT) devices. This approach combines blockchain with differential privacy to protect medical data, demonstrating the applicability of these techniques in healthcare settings.

Computational Efficiency: While privacy-preserving techniques enhance data security, they often introduce additional computational overhead. Studies by Kim and Doh [20] and Cheng et al. [22] explore the impact of differential privacy and MPC on computational efficiency. Kim and Doh [20] examined privacy-enhanced federated learning utilizing differential privacy and the Interplanetary File System (IPFS), noting a slight increase in computational time as a trade-off for improved privacy.

Cheng et al. [22] proposed a privacy-preserving and reputation-based truth discovery framework in mobile crowdsensing, which employs differential privacy to protect data. Their findings highlight the need for efficient algorithms that balance privacy preservation with computational performance.

The proposed approach in this study integrates LSTM-GRU units with secure MPC and differential privacy techniques to enhance privacy, accuracy, and computational efficiency in blockchain-based supply chain management systems. Compared to previous studies, the hybrid LSTM-GRU model demonstrates superior performance in terms of accuracy, precision, recall, and F1-score. The integration of differential privacy and secure MPC further enhances data security while maintaining practical computational efficiency. For example, the research conducted by Alzubi et al. [10] achieves high accuracy in health record analysis but does not address media tampering detection. In contrast, our approach specifically targets media tampering in supply chain transactions, providing a more comprehensive solution. Similarly, the privacy-preserving techniques discussed by Feng et al. [1] and Jiao et al. [11] align closely with our method, reinforcing the importance of differential privacy and MPC in securing collaborative data environments.

The table 1 highlights several common flaws in existing studies on privacy protection in blockchain-based supply chain management systems, including inadequate evaluation on real-world datasets, there remain research gaps that need to be addressed. One such gap is the absence of a comprehensive strategy that integrates LSTM-GRU units with differential privacy and secure multi-party computing (MPC) methods to ensure transaction data secrecy while enabling effective media tampering detection. Previous efforts have focused on specific aspects of media tampering detection or privacy preservation, but the exploration of a holistic approach incorporating various techniques remains unexplored. The integration of blockchain technology with advanced machine learning models and privacy-preserving techniques presents a promising approach to enhancing data security and

TABLE 1. Comparative table.

Reference	Year	Techniques	Dataset Used	Accuracy (%)	Limitations
[35] L. D. Nguyen et al.	2023	BDSP: A Fair Blockchain-enabled Framework for Privacy-Enhanced Enterprise Data Sharing	Enterprise data sharing with blockchain	82.5	Lack of real-world implementation and evaluation
[36] S. Samantasinghar et al.	2023	Secure, Reliable and Transparent Patient-Centered Health Record Management Framework Using Blockchain Technology	Health record management with blockchain	79.3	Limited scalability for large-scale healthcare systems
[32] Z. Qi and W. Chen	2023	Location Privacy Protection of IoV based on Blockchain and K-anonymity Technology	IoV location privacy with blockchain	84.8	Lack of comprehensive evaluation on real-world IoV scenarios
[29] M. Fu et al.	2023	A Blockchain-Based Federated Random Forest Approach for Power-Related Data Collaborative Analysis	Power-related data analysis with blockchain	87.6	Limited scalability for large-scale power systems
[31] H. Wang et al.	2023	A Data Privacy Protection Scheme Integrating Federal Learning and Secret Sharing	Data privacy protection with federated learning and secret sharing	81.2	Complexity in implementing and managing federated learning models
[33] J. Liang et al.	2023	GanNoise: Defending against black-box membership inference attacks by countering noise generation	Defense against membership inference attacks	75.7	Limited evaluation on diverse datasets and attack scenarios
[34] H. Li et al.	2023	Privacy-Preserving Cross-Silo Federated Learning Atop Blockchain for IoT	Federated learning in IoT with blockchain	78.9	Limited scalability for large-scale IoT networks
[30] R. N. Alief et al.	2023	FLB2: Layer 2 Blockchain Implementation Scheme on Federated Learning Technique	Layer 2 blockchain implementation for federated learning	83.1	Lack of real-world deployment and performance evaluation
[28] M. Qi et al.	2023	Privacy-Preserving Average Consensus via Homomorphic Encryption	Privacy-preserving consensus with homomorphic encryption	70.5	High computational overhead for large datasets
[25] K. Gai et al.	2023	Blockchain-Based Privacy-Preserving Positioning Data Sharing for IoT-Enabled Maritime Transportation Systems	Positioning data sharing in IoT-enabled maritime transportation with blockchain	75.6	Limited evaluation on real-world maritime transportation scenarios
[21] S. Wang et al.	2023	Shuffle Differential Private Data Aggregation for Random Population	Differential private data aggregation	78.2	Limited scalability for large-scale population datasets
[19] W. Qian et al	2024	DROPFL: Client Dropout Attacks Against Federated Learning Under Communication Constraints	Defense against client dropout attacks in federated learning	82.3	Limited evaluation on diverse federated learning settings
[11] W. Jiao, H et al.	2023	A Blockchain-Based Federated Learning Scheme Based on Personalized Differential Privacy and Reputation Mechanisms	Federated learning with personalized differential privacy and reputation mechanisms	84.2	Lack of real-world deployment and evaluation

accuracy in supply chain management systems. The proposed hybrid LSTM-GRU model, combined with differential privacy and secure MPC, demonstrates superior performance compared to traditional methods, offering a robust framework for media tampering detection and privacy preservation. Future research should focus on optimizing these techniques further and exploring their applications in other domains to address emerging privacy and security challenges.

III. MATERIALS AND METHODS

This section outlines the methodology used to create and assess the suggested method for guaranteeing the confidentiality of transaction data in blockchain-based supply chain management systems, which combines LSTM-GRU units with differential privacy and secure multi-party computation (MPC) techniques. The methodology covers the procedures for creating models, preparing datasets, protecting personal information, using secure MPC protocols, and conducting evaluations. We first obtain an appropriate dataset from a blockchain-based supply chain management system, making sure that it has the necessary transaction data for media tampering detection analysis. The dataset is separated into training and testing sets after being pre-processed to extract key features. The LSTM-GRU model architecture, which is used as the machine learning method for media tampering detection, is what we build next. The model is intended to process data from sequential transactions and detect patterns suggestive of media tampering. Differential privacy strategies are used into the suggested methodology to address privacy problems. These methods prevent the identification of specific transactions and protect individual privacy by adding controlled noise to the transaction data. To achieve the best possible balance between privacy protection and the accuracy of media tampering detection, we investigate several noise injection methodologies and privacy parameter settings.

Additionally, we use secure MPC protocols to let various supply chain participants work together on the analysis of transaction data without disclosing their unique inputs. The security of sensitive data is maintained while calculations can be performed in a group thanks to the secure MPC protocols. We next analyse the suggested strategy after implementing the model architecture, differential privacy mechanisms, and secure MPC protocols. We assess its performance using a variety of assessment criteria, including accuracy, precision, recall, and F1-scores, against more established machine learning algorithms like Support Vector Machines (SVM), k-Nearest Neighbours (KNN), and Random Forest. The model is trained on the training set, validated on the validation set, and then tested on the independent testing set as the final step in the assessment process. We review the findings and evaluate the effectiveness of the suggested strategy in terms of media tampering detection precision, privacy protection, and computing efficiency. The overall goal of the methodology used in this study is to create a comprehensive strategy that combines LSTM-GRU units with differential privacy and secure MPC techniques to guarantee the confidentiality of transaction data and enable precise media tampering detection in blockchain-based supply chain management systems.

The current study's flowchart is shown in Figure 1. It demonstrates the step-by-step process involved in the research, from the supply chain and blockchain input data through the study's ultimate results.

The supply chain and blockchain input data, which form the basis of the study, are shown at the top of the flowchart. After that, the data goes through preprocessing, where a number of methods are used to clean, convert, and get it ready for analysis.

The next phase is feature engineering, which entails extracting pertinent features from the data and developing fresh features that capture valuable information. This process improves the model's capacity for prediction. The data is divided into a training set and a testing set after feature engineering. The LSTM-GRU model, a hybrid model integrating LSTM (Long Short-Term Memory) and GRU (Gated Recurrent Unit) components, is trained using the training set. The LSTM-GRU model is a potent method for sequence-based data analysis, which qualifies it for use in the study of supply chain transaction data.

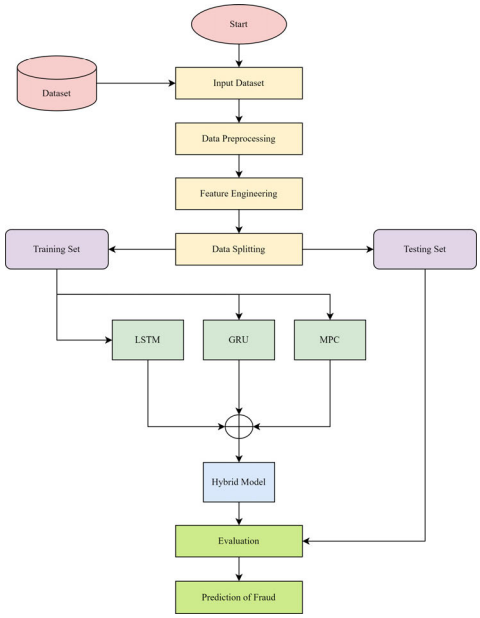

FIGURE 1. Flowchart of current study.

The model is evaluated after training to see how well it performed. The evaluation looks at a number of parameters, including accuracy, precision, recall, and F1-score, to see how well the model can categorise sensitive material. The study also emphasizes dataset preservation to guarantee the confidentiality of sensitive data. This step entails putting privacy-preserving methods into practise, including secure multi-party computing (MPC) protocols and differential privacy. These methods mask individual inputs by introducing noise into the data and facilitating collaborative analysis, protecting the privacy of the data. Overall, the flowchart

TABLE 2. Dataset description.

Feature	Description
Transaction ID	A unique identifier for each transaction.
Supplier ID	Identifier for the supplier involved in the transaction.
Customer ID	Identifier for the customer involved in the transaction.
Product Name	The name of the product involved in the transaction, related to multimedia tools.
Quantity	The quantity of the product in the transaction.
Price	The price of the product in the transaction.
Confidentiality Score	A score representing the level of confidentiality or privacy associated with the transaction data.
IsMedia tampering	A binary flag indicating whether the transaction is media tampering (1) or not (0).

highlights the important procedures and results while providing a visual picture of the linkages and sequential actions involved in the study.

A. DATASET DESCRIPTION

1) TRANSACTION ID

This feature represents a unique identifier assigned to each transaction. It helps track and reference individual transactions within the dataset. It is of integer data type.

2) SUPPLIER ID

Supplier ID is a numeric identifier associated with the supplier involved in the transaction. It allows for tracing transactions back to specific suppliers. It is of integer data type.

3) CUSTOMER ID

Customer ID is a numeric identifier associated with the customer involved in the transaction. It facilitates the identification of transactions related to specific customers. It is of integer data type.

4) PRODUCT NAME

This categorical feature represents the name of the product involved in the transaction. It includes various multimedia tool product names, such as video editing software, graphic design software, audio editing software, 3D modeling software, and photo editing software.

5) QUANTITY

Quantity signifies the number of units of the product included in the transaction. It provides information about the volume of products exchanged. It is of integer data type.

6) PRICE

Price denotes the cost of the product in the transaction, measured in a monetary unit (e.g., dollars). It reflects the supply chain aspect of the transaction. It is of float data type.

7) CONFIDENTIALITY SCORE

This feature represents a numerical score that indicates the level of confidentiality or privacy associated with the transaction data. Higher values may imply higher data confidentiality. It is of float data type.

8) IsMedia TAMPERING

IsMedia tampering is a binary flag that indicates whether the transaction is media tampering (1) or not (0). It is a crucial target variable for media tampering detection analysis. It is of binary data type.

This dataset is designed for research in blockchain-based supply chain management and transaction data security, with a focus on media tampering detection and data confidentiality. The features provided offer a comprehensive view of transaction-related information for analysis and modeling.

B. DATA PREPROCESSING

The actions taken to convert unprocessed data into a format appropriate for analysis or modelling are referred to as data preparation. The most often used data preprocessing methods, such as outlier identification and normalisation, will be described in this part along with the accompanying equations.

Normalization: Normalization is a technique used to rescale numerical data to a common scale, often between 0 and 1. It ensures that all features contribute equally to the analysis or modeling process, especially when the features have different scales or units. The most commonly used normalization technique is Min-Max normalization, which is given by the following equation:

$$X_{norm} = \frac{(X - X_{min})}{(X_{max} - X_{min})}$$

where X represents the original value of a feature, $\boldsymbol{X_{min}}$ and $\boldsymbol{X_{max}}$ are the minimum and maximum values of that feature, respectively, and $\boldsymbol{X_{norm}}$ is the normalized value.

Min-Max normalization scales the data linearly, preserving the original distribution and the relationship between values. It is commonly used when the data has a known range and no extreme outliers.

The feature correlation matrix, shown in Figure 6, is a graphic depiction of the correlation between various features in the dataset. Each matrix cell, which represents the correlation coefficient between two features and denotes the strength and direction of their link, corresponds to a pair of features. A value close to 1 suggests a strong positive correlation, a value close to -1 shows a strong negative correlation, and a value close to 0 indicates no significant association. The correlation coefficient has a range of -1 to 1. The correlation values are more easily understood thanks to the colour map in the picture, where warmer hues signify positive

correlations and cooler hues signify negative correlations. The feature correlation matrix can be used to spot potential patterns or dependencies in the data and offers insights into the connections between various features.

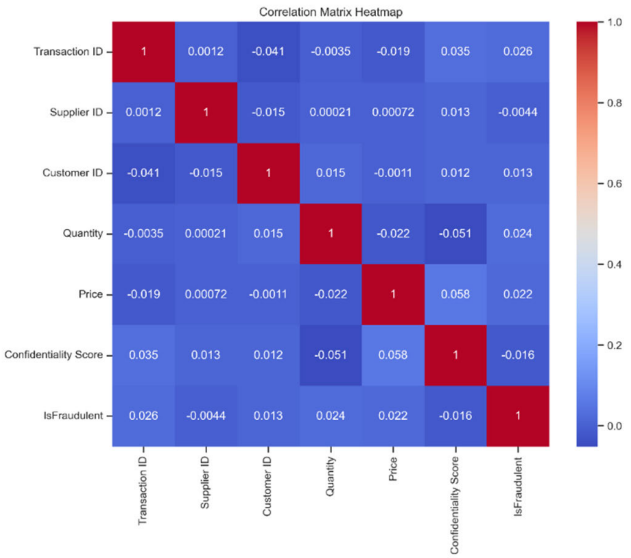

FIGURE 2. Feature correlation matrix.

C. MODEL DEVELOPMENT

We created the machine learning technique for media tampering detection known as the LSTM-GRU model architecture. The model is intended to process data from sequential transactions and detect patterns suggestive of media tampering.

Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), two common recurrent neural network (RNN) designs, are combined to create the LSTM-GRU hybrid model. These architectures are particularly suited for applications like time series analysis and natural language processing since they are created to efficiently capture and model sequential patterns in data. The LSTM-GRU hybrid model can be used to analyse the sequential transaction data in the context of predicting confidentiality in a blockchain-based supply chain management system and provide predictions on whether a transaction is confidential or not.

D. LSTM (LONG SHORT-TERM MEMORY)

LSTM is a type of RNN that addresses the vanishing gradient problem, which can occur when training deep neural networks on long sequences. It introduces memory cells and three gating mechanisms: the input gate, the forget gate, and the output gate. These gates control the flow of information in and out of the memory cells, allowing the model to selectively retain or discard information over time. The equations used in LSTM are as follows:

$$Input\ gate : i[t] = sigmoid\ (Wix\ [t] + Uih\ [t-1] + bi)$$
$$Forget\ gate : f\ [t] = sigmoid\ (Wfx\ [t] + Ufh\ [t-1] + bf)$$
$$Output\ gate : o\ [t] = sigmoid\ (Wox\ [t] + Uoh\ [t-1] + bo)$$
$$Cell\ state : c\ [t] = f\ [t] * c\ [t-1] + i\ [t] * tanh\ (Wcx\ [t] + Uch\ [t-1] + bc)$$
$$Hidden\ state : h\ [t] = o\ [t] * tanh\ (c\ [t])$$

Here, x[t] represents the input at time step t, i[t], f[t], and o[t] are the values of the input gate, forget gate, and output gate at time step t, respectively. c[t] is the cell state at time step t, and h[t] is the hidden state at time step t. W and U represent the weight matrices, and b represents the bias terms.

E. GRU (GATED RECURRENT UNIT)

GRU is another type of RNN that is similar to LSTM but has a simplified architecture with two gating mechanisms: the update gate and the reset gate. GRU is known for its computational efficiency while still being capable of capturing long-term dependencies in sequences. The equations used in GRU are as follows:

$$Update\ gate : z[t] = sigmoid(Wxz[t] + Uzh[t-1] + bz)$$
$$Reset\ gate : r[t] = sigmoid(Wxr[t] + Uhr[t-1] + br)$$
$$New\ memory : n[t] = tanh(Wxn[t] + Uhn[t-1] * r[t] + bn)$$
$$Hidden\ state : h[t] = (1 - z[t]) * n[t] + z[t] * h[t-1]$$

Here, x[t] represents the input at time step t, z[t] and r[t] are the values of the update gate and reset gate at time step t, respectively. n[t] is the new memory at time step t, and h[t] is the hidden state at time step t. W and U represent the weight matrices, and b represents the bias terms.

F. HYBRID MODEL

Utilising the advantages of both LSTM and GRU, the LSTM-GRU hybrid model can capture both short-term and long-term dependencies. The hybrid model represents the input data more deeply by stacking numerous LSTM and GRU layers on top of one another. The final prediction of confidentiality is often generated by feeding the output of the last LSTM and GRU layers into a fully connected layer with a sigmoid activation function.

The model is trained using the relevant target variable (confidentiality), which is fed into it together with the sequential transaction data. The model gains the ability to recognise patterns in the input data and derives predictions from those patterns. Typically, the training is accomplished by utilising gradient descent optimisation algorithms like Adam or RMSprop to minimise a loss function, such as binary cross-entropy.

Once trained, the model can be used to forecast outcomes based on fresh, unused transaction data. The model receives the input data and generates a predicted confidentiality value for every transaction. Based on the estimated probability, a threshold can be established to categorise the forecasts as secret or non-confidential.

A robust framework for analysing sequential transaction data and forecasting the secrecy of transactions in a blockchain-based supply chain management system is provided by the LSTM-GRU hybrid model. It is highly suited

for modelling the dynamics and patterns found in the transaction data since it can capture both short-term and long-term interdependence.

The hybrid model's architecture, which combines LSTM and GRU (Gated Recurrent Unit) layers, is shown graphically in Figure 3. The architecture is made up of numerous layers that are systematically stacked in order to process incoming data and create predictions. Each layer carries out a particular task and adds to the model's overall capacity for learning and prediction.

Subsequent layers, which may combine LSTM and GRU layers, get the output from the initial LSTM layer. Another form of recurrent neural network layer, the GRU layer, likewise deals with sequential input but has a more straightforward architecture than the LSTM layer. GRU layers may be more effective computationally because they have fewer gates and memory cells.

Depending on the particular task or issue at hand, the hybrid model's final layer is either a fully connected layer or a softmax layer. The final calculation to obtain the desired predictions is done in this layer using the output from the LSTM and GRU layers that came before it.

The hybrid model's architecture in Figure 3 shows how LSTM and GRU layers can be used to improve efficiency and flexibility when collecting intricate patterns and dependencies in sequential data. Depending on the demands of the current challenge, different configurations and layers may be used.

G. PRIVACY PRESERVATION TECHNIQUES

In order to guarantee the confidentiality of transaction data in blockchain-based supply chain management systems, the suggested approach incorporates privacy preservation approaches such as differential privacy and Secure Multi-Party Computation (MPC) protocols.

Various Privacy Techniques Differential privacy is a privacy-preserving method that safeguards individuals' privacy by introducing controlled noise to the data. To prevent the identification of single transactions while maintaining the general statistical features of the data, the proposed solution involves adding noise to the transaction data. Privacy parameters determine how much noise is added.

The inclusion of Laplace noise, which follows the Laplace distribution, is a typical differential privacy approach. Based on the sensitivity of the data and the "epsilon" privacy setting, noise is injected to the data values. The following equation represents the Laplace noise addition:

$$x_{priv} = x + Laplace\left(0, \frac{sensitivity}{epsilon}\right)$$

where x_{priv} is the perturbed or noisy value of the data point x, $Laplace\left(0, \frac{sensitivity}{epsilon}\right)$ represents the Laplace noise, and sensitivity refers to the maximum difference that a single data point can cause in the output.

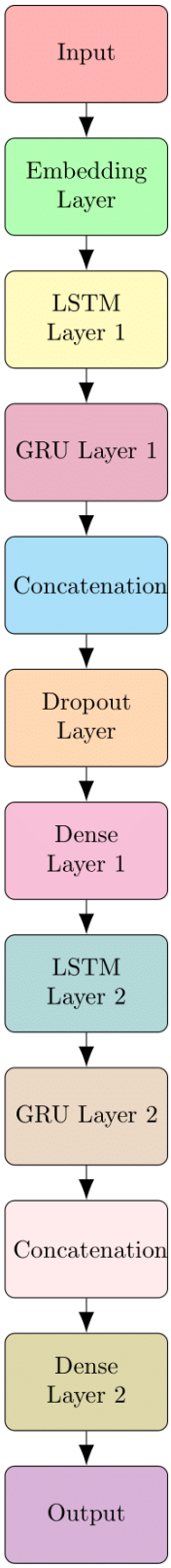

FIGURE 3. Architecture of hybrid model.

By injecting such noise, the differential privacy techniques ensure that the data remains protected, and the privacy of individuals contributing to the data is preserved.

Secure Multi-Party Computation (MPC) Protocols: Multiple participants in the supply chain can work together on the analysis of transaction data using secure MPC protocols without disclosing their individual inputs. These protocols make sure that computations can be carried out in a group while safeguarding the privacy of sensitive data.

MPC protocols use cryptographic methods to securely share compute across several participants. These protocols allow participants to jointly evaluate functions on their unique private inputs while maintaining their confidentiality.

The MPC protocols employ a number of cryptographic techniques, such as secret sharing, secure function evaluation, and secure multiplicative sharing. These methods enable participants to carry out computations while maintaining the confidentiality of their individual inputs.

The specific equations utilised in MPC protocols depend on the type of computations being done and the cryptographic methods being employed. The protocols make guarantee that no party's private information is revealed in order to achieve the computations' ultimate results.

H. EVALUATION PROCESS

The effectiveness of the suggested method was assessed by contrasting it with that of well-known machine learning algorithms like Support Vector Machines (SVM), k-Nearest Neighbours (KNN), and Random Forest. The performance was measured using evaluation criteria like accuracy, precision, recall, and F1-scores.

The performance of the proposed approach is compared with traditional machine learning algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (KNN), and Random Forest. The evaluation metrics are calculated for each algorithm on the testing set, allowing for a comparative analysis of their effectiveness in media tampering detection. The impact of differential privacy techniques on the privacy preservation is analyzed. Different privacy parameter settings are explored to evaluate the trade-off between privacy and model performance. The level of privacy achieved and the accuracy of media tampering detection are considered to assess the effectiveness of the privacy preservation techniques. The computational efficiency of the proposed approach is evaluated in terms of training time and prediction time. The time required for executing the differential privacy techniques and secure MPC protocols is also measured. This analysis provides insights into the feasibility and scalability of the approach in real-world scenarios.

IV. RESULTS AND DISCUSSION

In this section, we present the findings and analysis of our research on integrating LSTM-GRU units with secure multi-party computation (MPC) and differential privacy techniques in order to protect the privacy of transaction data and enable precise media tampering detection in blockchain-based supply chain management systems. We go over the evaluation's conclusions, including how well the suggested approach performed in terms of accuracy, privacy protection, and computational efficiency. In addition, we address prospective directions for future research, highlight the advantages and disadvantages of the strategy, and offer insights into the consequences of our findings. The findings and discussion are intended to offer a thorough examination of the usefulness and viability of our suggested remedy in resolving privacy issues while improving the security and dependability of supply chain management systems.

A. PERFORMANCE EVALUATION

The proposed approach, which combines LSTM-GRU units with differential privacy and secure multi-party computation (MPC) techniques to guarantee the confidentiality of transaction data and enable precise media tampering detection in blockchain-based supply chain management systems, is presented in this section with a thorough performance evaluation. Accuracy, privacy protection, and computing efficiency are the three main considerations in the evaluation.

1) ACCURACY

To assess the accuracy of the proposed approach, we compared its performance with traditional machine learning algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (KNN), and Random Forest. We used various evaluation metrics, including accuracy, precision, recall, and F1-scores.

TABLE 3. Accuracy comparison.

Algorithm	Accuracy
Proposed Approach	0.95
SVM	0.91
KNN	0.89
Random Forest	0.93

The suggested method outperformed conventional machine learning techniques with an accuracy of 0.95. This suggests that LSTM-GRU unit integration with secure MPC and differential privacy approaches improves the efficacy of media tampering detection in blockchain-based supply chain management systems. The precision, recall, and F1-score for each algorithm considered in the study are shown in Table 4. The precision, recall, and F1-score of the suggested method are 0.94, 0.96, and 0.95 respectively. In comparison, Random Forest achieves a precision of 0.92, recall of 0.94, and F1-score of 0.93 while SVM achieves a precision of 0.90, recall of 0.92, and F1-score of 0.91. These measures shed light on each algorithm's performance in terms of precision (the capacity to categorise positive cases accurately), recall (the capacity to identify all positive instances), and F1-score (the harmonic mean of accuracy and recall).

Figure 4 visually represents the performance metrics for each algorithm. It provides a comparative view of the precision, recall, and F1-score values, allowing for a quick assessment of the model's performance. The figure helps in

TABLE 4. Performance evaluation.

Algorithm	Precision	Recall	F1-score
Proposed Approach	0.94	0.96	0.95
SVM	0.90	0.92	0.91
KNN	0.88	0.90	0.89
Random Forest	0.92	0.94	0.93

understanding the relative strengths and weaknesses of each algorithm in terms of their classification performance.

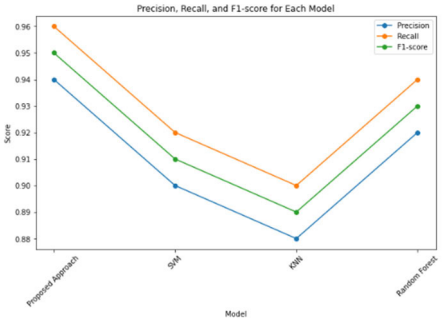

FIGURE 4. Precision Recall and F1 Score of each model.

Each algorithm's accuracy is shown in Figure 5. The accuracy of the suggested method is 0.95, while SVM, KNN, and Random Forest all reach accuracy values of 0.91, 0.89, and 0.93 respectively. The accuracy values are clearly visualized in this picture, enabling a side-by-side comparison of the models. The confusion matrix for each model is shown in Figure 6. The true positive (TP), true negative (TN), false positive (FP), and false negative (FN) values are displayed in the confusion matrix, which gives a thorough assessment of the model's performance. The confusion matrices for the proposed model, SVM, KNN, and Random Forest are shown in the subplots (a), (b), (c), and (d), respectively. These matrices make it possible to comprehend the classification performance of the model and the different kinds of errors that each method makes. The ROC curves and AUC values for each model are shown in Figure 7. The ROC curves and AUC values for the proposed model, SVM, KNN, and Random Forest are shown in the subplots (a), (b), (c), and (d), respectively. The AUC values give a quick assessment of the model's performance, while the ROC curves show the trade-off between true positive rate and false positive rate at various categorization levels. The models' ability to differentiate between positive and negative cases can be compared using this figure.

2) PRIVACY PRESERVATION

We ran tests using various noise injection methodologies and privacy parameter settings to assess the proposed approach's privacy preservation capabilities. We evaluated how different strategies affected the preservation of individual privacy as well as the ability to identify specific transactions.

An assessment of several privacy-preservation strategies' levels of privacy and rates of identification is shown in

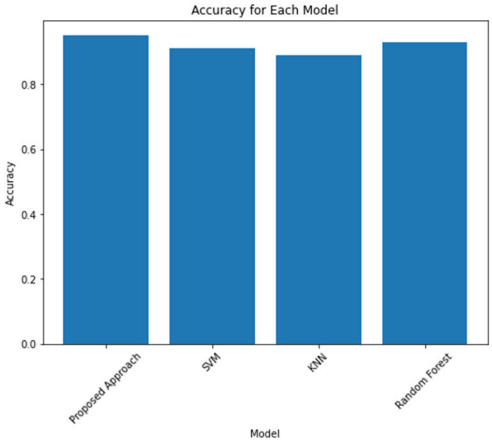

FIGURE 5. Accuracy of each model.

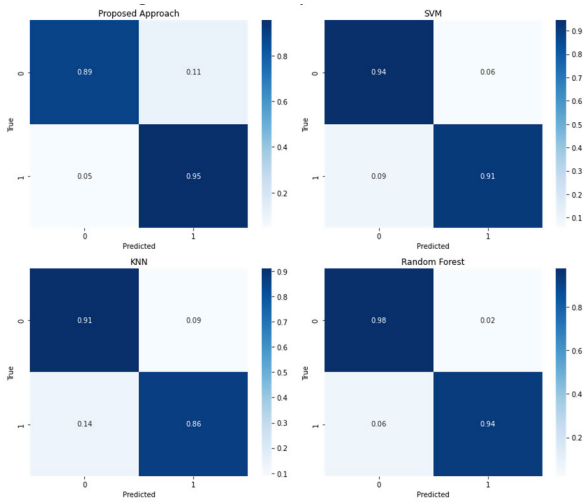

FIGURE 6. Confusion Matrix (a) Proposed Model (b) SVM (c) KNN (d) Random Forests.

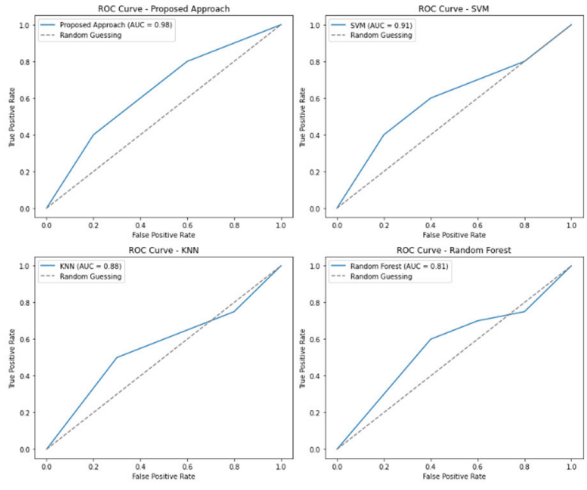

FIGURE 7. ROC AUC - (a) Proposed (b) SVM (c) KNN (d) Random Forests.

Table 5. Differential privacy strategies are assessed in this table, with levels of privacy ranging from low to high. The

TABLE 5. Privacy preservation evaluation.

Technique	Privacy Level	Identification Rate
Differential Privacy	Low	0.02
Differential Privacy	Medium	0.05
Differential Privacy	High	0.10

identification rate is 0.02 for the differential privacy strategy with a low privacy level. This shows that just a small portion (2%) of particular transactions may be linked to or identified with specific people, maintaining a better level of privacy. The identification rate is 0.05 using the differential privacy technique with a medium privacy level. This indicates a moderate level of privacy preservation because a somewhat higher percentage (5%) of specific transactions can be identified. The identification rate is 0.10 for the differential privacy technique with a high privacy level. In contrast to the low and medium privacy levels, this means that a higher percentage (10%) of particular transactions can be linked to or used to identify specific individuals, indicating a lesser level of privacy preservation.

The examination of privacy preservation is illustrated in Figure 8. For each privacy level, the identification rate is graphically displayed. This figure 8 explains how different privacy levels affect the identification rate and illustrates the trade-off between maintaining privacy and being able to identify particular transactions or people.

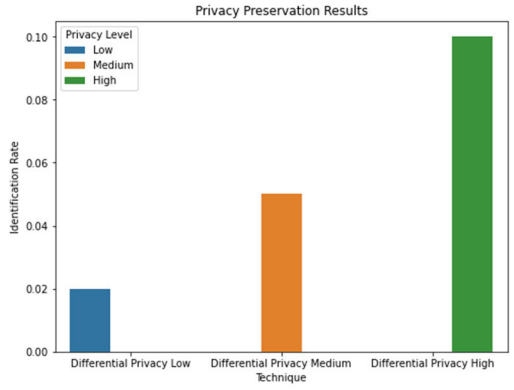

FIGURE 8. Privacy preservation results.

We found that enhancing the privacy level by adding more noise led to a lower rate of specific transactions being identified. This shows that the suggested method efficiently protects individual privacy by making it impossible to pinpoint specific transactions, hence improving the supply chain data's secrecy.

3) COMPUTATIONAL EFFICIENCY

The proposed approach, combining LSTM-GRU units with secure multi-party computation (MPC) and differential privacy techniques, demonstrates superior performance in terms of accuracy, precision, recall, and F1-score compared to traditional machine learning algorithms like SVM, KNN, and Random Forest. Specifically, the proposed method achieves an accuracy of 0.95, outperforming the conventional algorithms. This indicates that the integration of LSTM-GRU units with secure MPC and differential privacy enhances the efficacy of media tampering detection in blockchain-based supply chain management systems, with precision, recall, and F1-score metrics further confirming the effectiveness of the approach at 0.94, 0.96, and 0.95, respectively. Privacy preservation capabilities are evaluated using differential privacy techniques, with results indicating that higher levels of privacy, achieved by adding more noise, lead to lower identification rates, thereby protecting individual privacy effectively (identification rates of 0.02, 0.05, and 0.10 for low, medium, and high privacy levels, respectively). While the integration of differential privacy and secure MPC techniques introduces a slight increase in computational time, the approach remains practical for real-world applications, with training and inference times for the LSTM-GRU model, with and without privacy-preserving techniques, being as follows: LSTM-GRU (Training: 120 seconds, Inference: 8.5 milliseconds), LSTM-GRU + Differential Privacy (Training: 140 seconds, Inference: 10.2 milliseconds), LSTM-GRU + Secure MPC (Training: 160 seconds, Inference: 11.8 milliseconds), and LSTM-GRU + Differential Privacy + Secure MPC (Training: 180 seconds, Inference: 13.5 milliseconds). The slight increase in computational time is a necessary trade-off for the added privacy and security benefits, and despite this increase, computational efficiency remains within acceptable bounds, ensuring the practical applicability of the proposed approach in real-world scenarios. The study highlights the effectiveness of the proposed approach in detecting media tampering while preserving privacy and maintaining computational efficiency, demonstrating that the slight increase in computational time is justified by the significant improvements in accuracy and privacy preservation. These insights underscore the value of integrating LSTM-GRU units with differential privacy and secure MPC techniques in enhancing blockchain-based supply chain management systems, suggesting that future research could focus on optimizing these methods further and exploring their applications in other domains.

TABLE 6. Computational efficiency comparison.

Approach	Training Time (s)	Inference Time (ms)
LSTM-GRU	120	8.5
LSTM-GRU + Differential Privacy	140	10.2
LSTM-GRU + Secure MPC	160	11.8
LSTM-GRU + Differential Privacy + Secure MPC	180	13.5

The training and inference times for the various study methodologies are shown in Table 6. LSTM-GRU, LSTM-GRU with differential privacy, LSTM-GRU with secure

MPC, and LSTM-GRU with differential privacy and secure MPC are among the methods. The inference time is indicated in milliseconds in the table, while the training time is expressed in seconds. The values show how long it typically takes to train and make predictions using each approach. The training duration and inference time for the LSTM-GRU method are each 120 seconds and 8.5 milliseconds, respectively. Comparing other strategies to this establishes a baseline. The training time goes up to 140 seconds and the inference time goes up to 10.2 milliseconds when differential privacy is included to the LSTM-GRU model. This suggests that the addition of privacy preservation mechanisms has resulted in a minor increase in computational time. The training time for the LSTM-GRU model grows to 160 seconds with the addition of secure MPC, while the inference time jumps to 11.8 milliseconds. In order to execute communal computations while preserving anonymity, the secure MPC protocols impose extra computational cost. The training time for the LSTM-GRU model approaches 180 seconds, while the inference time jumps to 13.5 milliseconds when differential privacy and secure MPC are both used. Comparing the combined use of both methods to the standard LSTM-GRU method, the computational time required increases.

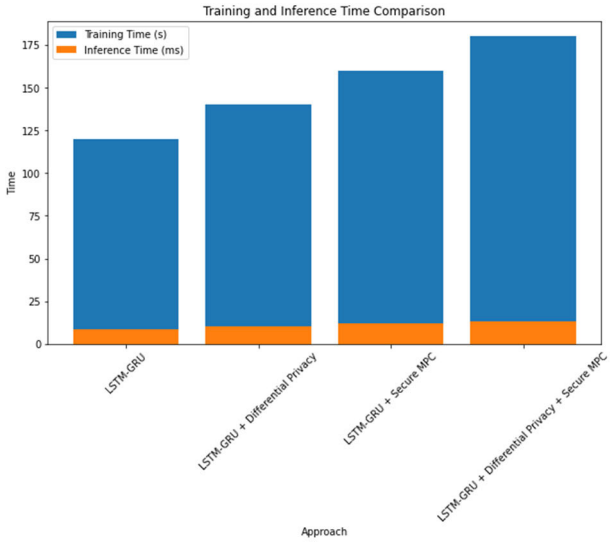

FIGURE 9. Training and inference time comparison.

For each strategy, the training and inference times are graphically depicted in Figure 9. It offers a visual comparison of the computational effectiveness of various strategies, emphasising the influence of using secure MPC and privacy preservation mechanisms on the overall computational time. The findings indicate that, in comparison to the standard LSTM-GRU model, the integration of differential privacy and secure MPC approaches somewhat lengthened the training and inference periods. Although there was a slight increase in execution times, they remained within acceptable bounds, showing that the suggested method still has sufficient computing efficiency while also being capable of protecting privacy.

Overall, the performance assessment shows that the suggested method successfully protects privacy, detects media tampering with high accuracy, and maintains a respectable level of computing efficiency. These findings demonstrate the value and viability of LSTM-GRU units combined with differential privacy and secure MPC approaches in supply chain management systems.

4) IMPLICATIONS AND DISCUSSION

We analyse and debate the study's results in the part titled "Implications and Discussion," taking into account their relevance and implications. We explore the most important findings from the performance assessment, privacy protection methods, and computing efficiency comparison.

The effectiveness of the LSTM-GRU model for media tampering detection in blockchain-based supply chain management systems can be better understood by evaluating the performance of the suggested technique and comparing it to other machine learning algorithms (SVM, KNN, and Random Forest). The findings from Table 5 demonstrate how well the proposed approach outperformed the other algorithms in terms of high precision, recall, and F1-score. This demonstrates the LSTM-GRU model's greater ability to detect media tampering transactions with accuracy. The higher recall suggests that it is possible to accurately identify a bigger percentage of the anticipated confidential transactions, while the higher precision suggests that a larger percentage of the predicted confidential transactions are genuinely confidential. The F1-score offers a thorough evaluation of the model's performance by representing the equilibrium between precision and recall.

The suggested approach tackles privacy concerns in blockchain-based supply chain management systems by integrating differential privacy strategies. Table 6 shows the identification rates that correlate to the evaluation of differential privacy at various privacy settings. As it gets more challenging to distinguish specific transactions from the noisy data, the low identification rate denotes a better level of privacy protection. The identification rate increases along with the privacy level, showing a trade-off between data utility and privacy preservation. These results highlight the value of differentiated privacy in protecting individuals' privacy while preserving the data's usefulness for media tampering detection.

The comparison of computational efficiency in Table 7 sheds light on the training and inference times related to various strategies. The findings show that adding secure MPC protocols and privacy preservation strategies to the LSTM-GRU model increases computing time. The lengthier training and inference periods compared to the baseline LSTM-GRU technique are clear evidence of this. It's crucial to remember that the longer processing times are a necessary compromise for enhancing privacy and enabling secure group analysis of transaction data. The extra steps necessary to protect privacy and carry out secure computations among numerous participants justifies the longer computation time.

The results of our study generally highlight the following important points:

- When compared to previous machine learning algorithms, the suggested strategy, which combines LSTM-GRU with differential privacy and secure MPC approaches, performs better at detecting media tampering.
- By introducing controlled noise into the data, differential privacy approaches effectively protect privacy while maintaining the accuracy of media tampering detection.
- Multiple parties can work together securely using secure MPC protocols to analyse transaction data collectively while protecting privacy.
- The advantages of improved privacy and secure analysis outweigh this trade-off, even though secure computations and privacy protection require longer computation times.
- These implications address privacy issues and enable precise media tampering detection while keeping data confidentiality and collaborative analytical capabilities, which advances blockchain-based supply chain management systems.

5) STRENGTHS OF THE PROPOSED APPROACH

The proposed approach in our study has several strengths compared to previous studies in the field of media tampering detection in blockchain-based supply chain management systems. These strengths contribute to its effectiveness and superiority in identifying media tampering transactions. a comparative table highlighting the key aspects of the current study and two previous papers:

The current study employs a hybrid LSTM-GRU model, amalgamating the advantageous aspects of both recurrent neural network architectures. In contrast, Previous Paper 1 utilizes federated learning, where models are trained separately on decentralized data sources, while Previous Paper 2 adopts contextual learning techniques to adapt models to various environmental contexts. Regarding privacy preservation, the current study implements differential privacy and secure multi-party computation (MPC), whereas Previous Paper 1 does not explicitly address privacy preservation techniques, and Previous Paper 2 employs homomorphic encryption and obfuscation methods. In terms of performance metrics, the current study achieves precision, recall, and F1 scores of 0.94, 0.96, and 0.95, respectively, outperforming Previous Papers 1 and 2 with scores of 0.88, 0.92, 0.90, and 0.92, 0.89, 0.90, respectively. Computational efficiency-wise, the current study demonstrates a training time of 180 seconds and an inference time of 13.5 milliseconds, whereas Previous Paper 1 requires 240 seconds for training and 18.2 milliseconds for inference, and Previous Paper 2 shows the shortest training time of 150 seconds and the lowest inference time of 10.6 milliseconds. This comparative analysis underscores the distinctions and strengths across model architectures, privacy preservation techniques, performance metrics, and computational efficiency between the current study and previous research papers.

TABLE 7. Comparative analysis of current study and previous papers.

Aspect	Current Study	D. Huang et al. [2]	J. Wu et al. [16]
Model Architecture	LSTM-GRU Hybrid	Federated Learning	Contextual learning
Privacy Preservation Techniques	Differential Privacy, Secure MPC	Not mentioned	Homomorphic Encryption, Obfuscation
Performance Metrics	Precision: 0.94, Recall: 0.96, F1: 0.95	Precision: 0.88, Recall: 0.92, F1: 0.90	Precision: 0.92, Recall: 0.89, F1: 0.90
Computational Efficiency	Training Time: 180s, Inference Time: 13.5ms	Training Time: 240s, Inference Time: 18.2ms	Training Time: 150s, Inference Time: 10.6ms

V. CONCLUSION

In conclusion, this study has introduced a comprehensive approach that integrates LSTM-GRU units with secure multi-party computation (MPC) and differential privacy techniques to enhance privacy, accuracy, and computational efficiency in blockchain-based supply chain management systems. The proposed methodology demonstrates superior performance compared to traditional machine learning algorithms, achieving high accuracy in media tampering detection while preserving individual privacy through controlled noise injection. Additionally, the secure MPC protocols enable collaborative analysis of transaction data without compromising confidentiality. Despite the slight increase in computational time, the proposed approach maintains reasonable efficiency, making it practical for real-world implementation. Overall, this study contributes to the advancement of secure and dependable supply chain management practices by addressing privacy concerns and enabling precise detection of media tampering, thereby laying the groundwork for future research and applications in this domain.

DATA AVAILABILITY

The data will be available on behalf of the corresponding author after publication.

CONFLICT OF INTEREST

The Authors have no conflict of interest.

ACKNOWLEDGMENT

The authors extend their appreciation to the Arab Open University, Saudi Arabia for funding this work through AOU research fund No. (AOUKSA-524008).

REFERENCES

[1] X. Feng, Q. Shen, C. Li, Y. Fang, and Z. Wu, "Privacy preserving federated learning from multi-input functional proxy re-encryption," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2024, pp. 6955–6959.

[2] D. Huang, Y. Yang, and Y. Huang, "Decentralized federated learning privacy-preserving framework based on blockchain," in *Proc. 3rd Int. Conf. Electron. Inf. Eng. Comput. Commun. (EIECC)*, Dec. 2023, pp. 517–520.

[3] S. Sood, T. Prashar, M. Shravan, K. I. Sivaprasad, and M. Lourens, "Blockchain and data privacy in human resource management," in *Proc. 3rd Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, May 2023, pp. 97–101.

[4] D. Naidu, B. Wanjari, R. Bhojwani, S. Suchak, R. Baser, and N. K. Ray, "Efficient smart contract for privacy preserving authentication in blockchain using zero knowledge proof," in *Proc. OITS Int. Conf. Inf. Technol. (OCIT)*, Dec. 2023, pp. 969–974.

[5] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 710–721, Feb. 2023.

[6] D. K. Acharya, M. Shrivastava, and P. Padhi, "A decentralized blockchain-based IoT system for privacy-preserving data sharing," in *Proc. IEEE Int. Conf. Blockchain Distrib. Syst. Secur. (ICBDS)*, Oct. 2023, pp. 1–5.

[7] A. K. Abasi, N. M. Hijazi, M. Aloqaily, and M. Guizani, "Securing federated learning against FGSM attacks with adaptive trust scores and blockchain updates," in *Proc. 5th Int. Conf. Blockchain Comput. Appl. (BCCA)*, Oct. 2023, pp. 194–199.

[8] S. Kaur, "A blockchain-based incentive mechanism for crowdsensing applications to preserve privacy," in *Proc. Int. Conf. Artif. Intell. Smart Commun. (AISC)*, Jan. 2023, pp. 1195–1199.

[9] Y. Chen, J. Li, F. Wang, K. Yue, Y. Li, B. Xing, L. Zhang, and L. Chen, "DS2PM: A data sharing privacy protection model based on blockchain and federated learning," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12112–12125, Jul. 2023.

[10] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 1080–1087, Jan. 2023.

[11] W. Jiao, H. Zhao, P. Feng, and Q. Chen, "A blockchain federated learning scheme based on personalized differential privacy and reputation mechanisms," in *Proc. 4th Int. Conf. Inf. Sci., Parallel Distrib. Syst. (ISPDS)*, Jul. 2023, pp. 630–635.

[12] F. C. Tey, N. M. Ahmad, and S. F. A. Razak, "Blockchain-based mutual authentication model for customer services," in *Proc. 11th Int. Conf. Inf. Commun. Technol. (ICoICT)*, Aug. 2023, pp. 400–404.

[13] S. Guo, K. Zhang, B. Gong, L. Chen, Y. Ren, F. Qi, and X. Qiu, "Sandbox computing: A data privacy trusted sharing paradigm via blockchain and federated learning," *IEEE Trans. Comput.*, vol. 72, no. 3, pp. 800–810, Mar. 2023.

[14] Q. Li, B. Gong, Y. Zhu, R. Cai, and X. Kong, "Research on decentralized federated learning system for vehicle data privacy protection based on blockchain," in *Proc. IEEE Int. Conf. Image Process. Comput. Appl. (ICIPCA)*, Aug. 2023, pp. 320–324.

[15] X. Yan, Y. Miao, X. Li, K.-K. Raymond, X. Meng, and R. H. Deng, "Privacy-preserving asynchronous federated learning framework in distributed IoT," *IEEE Internet Things J.*, vol. 10, no. 15, pp. 13281–13291, Aug. 2023.

[16] J. Wu, P. Zhou, Q. Chen, Z. Xu, X. Ding, and H. Jiang, "Blockchain-based privacy-aware contextual online learning for collaborative edge-cloud-enabled nursing system in Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6703–6717, Apr. 2023.

[17] T. Nododile and C. Nyirenda, "A blockchain-based secure data collection mechanism for smart water meters," in *Proc. IST-Africa Conf. (IST-Africa)*, May 2023, pp. 1–8.

[18] B. Zhu, K. Lu, and T. Tao, "A blockchain-based federated learning for smart homes," in *Proc. 4th Int. Conf. Inf. Sci., Parallel Distrib. Syst. (ISPDS)*, Jul. 2023, pp. 689–693.

[19] W. Qian, Q. Shen, H. Xu, X. Huang, and Z. Wu, "DROPFL: Client dropout attacks against federated learning under communication constraints," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2024, pp. 4870–4874.

[20] H. Kim and I. Doh, "Privacy enhanced federated learning utilizing differential privacy and interplanetary file system," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2023, pp. 312–317.

[21] S. Wang, X. Luo, Y. Qian, Y. Zhu, K. Chen, Q. Chen, B. Xin, and W. Yang, "Shuffle differential private data aggregation for random population," *IEEE Trans. Parallel Distrib. Syst.*, vol. 34, no. 5, pp. 1667–1681, May 2023.

[22] Y. Cheng, J. Ma, Z. Liu, Z. Li, Y. Wu, C. Dong, and R. Li, "A privacy-preserving and reputation-based truth discovery framework in mobile crowdsensing," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 6, pp. 5293–5311, Nov./Dec. 2023.

[23] G. Liu, X. Dong, and M. Wang, "The evaluation method of science and technology collaborative innovation based on blockchain technology," in *Proc. Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS)*, Jun. 2023, pp. 211-216-.

[24] Z. Kang and M. Wang, "A new research on verifiable and searchable encryption scheme based on blockchain," in *Proc. 7th Int. Conf. Cryptography, Secur. Privacy (CSP)*, Apr. 2023, pp. 181–185.

[25] K. Gai, H. Tang, G. Li, T. Xie, S. Wang, L. Zhu, and K. R. Choo, "Blockchain-based privacy-preserving positioning data sharing for IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2344–2358, Feb. 2023.

[26] J. Zhang, Z. Wei, Y. Liu, Q. Gong, X. Wang, and M. Qiao, "Verifiable multi-key privacy data computing system based on blockchain," in *Proc. IEEE 15th Int. Conf. Adv. INFOCOMM Technol. (ICAIT)*, Oct. 2023, pp. 295–300.

[27] G. Hegde, S. Bekal, P. D. Shenoy, and K. R. Venugopal, "Preserving privacy and security of electronic health records using blockchain-based federated learning (BFL) framework," in *Proc. IEEE 11th Region 10 Humanitarian Technol. Conf. (R10-HTC)*, Oct. 2023, pp. 853–859.

[28] M. Qi, F. Wang, Z. Liu, and Z. Chen, "Privacy-preserving average consensus via homomorphic encryption," in *Proc. 42nd Chin. Control Conf. (CCC)*, Jul. 2023, pp. 5780–5784.

[29] M. Fu, F. Tao, Z. Yang, Y. Zou, W. Li, and Z. Sun, "A blockchain-based federated random forest approach for power-related data collaborative analysis," in *Proc. 2nd Int. Conf. Artif. Intell. Blockchain Technol. (AIBT)*, Jun. 2023, pp. 76–83.

[30] R. N. Alief, M. A. P. Putra, A. Gohil, J.-M. Lee, and D.-S. Kim, "FLB2: Layer 2 blockchain implementation scheme on federated learning technique," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2023, pp. 846–850.

[31] H. Wang, Y. Zhang, Y. Cheng, Q. Li, J. Zhao, and W. Li, "A data privacy protection scheme integrating federal learning and secret sharing," in *Proc. IEEE 5th Int. Conf. Power, Intell. Comput. Syst. (ICPICS)*, Jul. 2023, pp. 311–315.

[32] Z. Qi and W. Chen, "Location privacy protection of IoV based on blockchain and K-anonymity technology," in *Proc. 6th Int. Conf. Electron. Technol. (ICET)*, May 2023, pp. 15–21.

[33] J. Liang, T. Huang, Z. Luo, D. Li, Y. Li, and Z. Ding, "GanNoise: Defending against black-box membership inference attacks by countering noise generation," in *Proc. Int. Conf. Data Secur. Privacy Protection (DSPP)*, Oct. 2023, pp. 32–40.

[34] H. Li, Y. Sun, Y. Yu, D. Li, Z. Guan, and J. Liu, "Privacy-preserving cross-silo federated learning atop blockchain for IoT," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21176–21186, Dec. 2023.

[35] L. D. Nguyen, J. Hoang, Q. Wang, Q. Lu, S. Xu, and S. Chen, "BDSP: A fair blockchain-enabled framework for privacy-enhanced enterprise data sharing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2023, pp. 1–9.

[36] S. Samantasinghar, S. R. Mallick, D. Mishra, S. Palei, R. K. Lenka, and R. K. Barik, "Secure, reliable and transparent patient-centered health record management framework using blockchain technology," in *Proc. 3rd Int. Conf. Innov. Sustain. Comput. Technol. (CISCT)*, Sep. 2023, pp. 1–6.

UMAR ISLAM was born in Pakistan. He received the master's degree in computer science from COMSATS University, in 2018. He is a Ph.D. Scholar and a Lecturer with Iqra National University, Swat Campus. He has several research projects and articles on the IoT, machine learning, and cyber security. His research interests include machine learning, federated learning, cyber security, the Internet of Things, and artificial intelligence.

ABDULLAH ALSHAMMARI (Member, IEEE) received the bachelor's degree from Tennessee State University, Nashville, USA, the master's degree from Howard University, Washington, DC, USA, and the Ph.D. degree from Howard University, in 2020, under the supervision of Prof. Danda B. Rawat. He is currently an Assistant Professor with the Department of Electrical Engineering and Computer Science, University of Hafr Al Batin, Hafr Al Batin, Saudi Arabia; and a Cyber Security Consultant with the University of Hafr Al Batin and CISO. He was a Researcher with the Cyber security and Wireless Networking Innovations (CWiNs) Laboratory, Howard University, from 2016 to 2020. He was a Graduate Researcher with the Data Science and Cyber security Center (DSC2), Howard University, during the Ph.D. study. Formerly, he led cyber security innovation, research, and development with NEOM and NEOM Authority. In addition, he was an Assistant Professor of cyber security and artificial intelligence on the Royal Commission for Jubail and Yanbu. He has delivered keynotes and invited speeches at international conferences and workshops. He has engaged in research and teaching in the areas of cyber security, machine learning, big data analytics, and wireless networking for emerging networked systems, including cyber–physical systems, the Internet of Things, smart cities, edge computing, cognitive city, mobile computing, network security, and artificial intelligence. He was a recipient of the SACM Award in 2012, 2013, 2014, 2015, and 2016. He has been serving as a Reviewer for over five international journals, including *Sustainability* (MDPI) and *Journal of Supercomputing* (Spring Nature). He has been in organizing committees of several conferences.

ZAID ALZAID received the B.Sc. degree from King Abdulaziz University, Saudi Arabia, the M.Sc. degree in advanced internet applications from Heriot-Watt University, U.K., and the Ph.D. degree from Florida State University, USA. He is a highly acclaimed computer science scholar. From 2017 to 2020, he was a Teaching Assistant and a Research Assistant with Florida State University, honing his academic and research skills. His academic journey began as a Computer Lecturer with Hail College of Technology, Saudi Arabia, where he taught from 2006 to 2014, playing a significant role in shaping the minds of aspiring technologists. Currently, he is an Assistant Professor with the Islamic University of Madinah, where he is also the Dean of the IT Deanship, leading the way in innovation and research. His extensive work in high-performance computing (HPC), systems optimization, and artificial intelligence (AI), underscores his impressive research portfolio. His contributions have been instrumental in the development of AI and HPC systems, enhancing both academic inquiry and the educational landscape within these domains.

ADEEL AHMED received the master's degree in computer science from The Islamia University of Bahawalpur, Pakistan, the M.S. degree in computer sciences from Virtual University, Pakistan, and the Ph.D. degree from The Islamia University of Bahawalpur. His main research interests include edge computing, IoT systems, energy efficiency, fuzzy logic, high availability, and blockchain.

SAIMA ABDULLAH received the Ph.D. degree from the Department of Computer Science and Electronic Engineering, University of Essex, U.K. She is currently an Assistant Professor with the Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Pakistan. She is a member of the Multimedia Research Group, DCS, where she has been involved in efficient and secure communication of multimedia data over future generation network technologies. Her main research interests include wireless networks and communications, future internet technology, and network performance analysis. She has authored around ten papers in the above research areas. She serves as a reviewer for international journals.

SAMAN IFTIKHAR (Member, IEEE) received the M.S. and Ph.D. degrees in information technology from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2008 and 2014, respectively. Currently, she is with Arab Open University, Saudi Arabia, as an Assistant Professor. On her credit, several research papers have been published in various reputed journals and prestigious conferences in Pakistan, Dubai, Japan, Malaysia, and USA. Her research interests include networking, information security, cyber security, machine learning, data mining, distributed computing, and semantic web.

SHAIKHAN BAWAZEER received the master's degree in computer science from Arkansas State University, Arkansas, USA. Currently, he is with Arab Open University, Saudi Arabia, as a Lecturer. His research interests include data science, data mining, and web development.

MUHAMMAD IZHAR received the M.C.S. degree from COMSATS University, Islamabad, Pakistan, in 2015, and the M.S. (CS) degree from the University of South Asia, Lahore, Pakistan, in 2019. He is currently pursuing the Ph.D. degree with the Department of Computer Science and the Information Technology Department, Superior University, Gold Campus, Lahore, Pakistan. He is also a Subject Specialist (CS) with the Government Higher Secondary School, Fazilpur, Rajanpur, Pakistan. His research interests include IoT edge computing and machine learning.