www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 9 Issue 08 August 2020, Page No. 25156-25164
ISSN: 2319-7242 DOI: 10.18535/ijecs/v9i08.4539

Ensuring Data Integrity and Confidentiality in Financial Transactions Using Aes-256-Gcm And Secure Transmission

[1]Yashwant Kumar Kolli, [2]Karthick.M
Cognizant Technology Solutions US Corp, College Station, Texas, USA
SNS College of Technology, Coimbatore, India.

Abstract
This study focuses on the aspects of securing financial transaction data through encryption and other forms of encryption. The most recommended ones are AES-256-GCM encryption and its application towards having data integrity and confidentiality at the time of transmission. The study describes the threat involved in the transfer and storage concerning financial data. Combining with secure transport protocols shows the clear way in which AES-256-GCM encryption would protect other types of sensitive data, such as through IPsec VPN tunnels. Both management services and the market are dependent on data technologies, since new forms of services and facilities are being developed with each single device. Some of the challenges associated with this area were given as performance overhead due to encryption, and the system's inability to scale to accommodate large amounts of financial data. However, with this method, it has taken care of the industry-standard compliance aspects, making it, thereby, a formidable ground in the security of financial transactions in the digital environment. The results obtained from As shown in the graph, the increase in plaintext size (P_size) correlates with the increase in AES-256-GCM encryption time (T_encryption), which goes from about 20 ms for 1 MB to over 120 ms for 20 MB, indicating that more and more computational work is required to encrypt such a large data file. In the meantime, the security (S_encryption) of the encrypted data-which is graphically represented by the blue line-increases immensely when the Data size becomes larger. On the contrary, the red line, which refers to that of unencrypted data, remains static to illustrate the low security level. Thus, encryption becomes necessary to secure sensitive data as it grows in size.

Keywords: AES-256-GCM Encryption, Data Integrity, IPsec VPN, Cloud Storage

1. Introduction

The transfer of transaction data in a financial institution now represents the highest echelons of encryption, underpinned by a solid framework of protocols for securing transactions over the digital landscape [1]. Such sensitive information as bank account numbers, values of transactions, and customer identities is what could ever stand to be intercepted and modified [2]. Another good contender for encryption is AES using the GCM mode of operation with a 256-bit key [3]. This encryption of transactions guarantees, among other things, confidentiality of the transactions and provides for other methods of authenticating the integrity of the data during transmission [4]. GCM is meant not just for tagging the MAC (message authentication code) to its processed message, but also to detect unauthorized alterations of the encrypted data; hence, it fits into protecting the processing of financial transactions in real-time [5]. Strength has been added to this two-concept architecture with the introduction of the tools for secure communications [6], such as the IPSec VPN, which cloaks the network; apart from the end-to-end encryption for transportational security, it ensures that data is secure as it traverses untrusted networks [7]. This provides another layer protecting against breach of financial data and snooping attacks, and also from man-in-the-middle attacks [8]. Such a multilayer architecture is critical for ensuring compliance of financial institutions with standards such as PCI DSS and GDPR. In particular [9], the AES-256-GCM algorithm and, in general, IPSec safeguard the confidentiality [10], integrity, and rightful access to sensitive data. This further adds to the scalability and,

importantly, high performance, which can meet the ever-increasing and demanding requirements of a secure online cloud financial transaction system. This, too, is an accepted and validated methodology for operational integrity and long-term prospects for data protection.

It is a methodology that creates financial transaction data lifecycle security techniques. It starts with the Data Collection, which will have transaction data from all sources for a primary dataset while protecting sensitive information from possible threats. The next step is AES-256-GCM encryption, which encrypts data and therefore treats data as confidential. This is to make the information unreadable for unauthorized individuals using the algorithm [11]. Also, the algorithm implements authenticated encryption, which guarantees the integrity of the data by proving that the original data has not been changed throughout the transmission process [12]. Immediately after that, the data undergoes secure transmission through ipsec VPN tunnel to ensure that none of the transferred data gets eavesdropped on or tampered with during transport through untrusted networks such as the internet [13]. Finally is the cloud storage, which gives one an elastic and secure storage. So, cloud will have advanced security measures like encryption and access control to ensure that only authorized individuals can gain access to the stored data. All these techniques: encryption, secure transmission, and cloud storage work together to protect financial transaction data and to minimize the risk of loss or illegal treatment of sensitive information during its lifecycle concerning the three aspects mentioned. For yet another limitation, the framework is seen to heavily lean on centralized cloud storage systems in case of any probable breach or outage on the side of cloud providers, so that the data becomes unavailable eventually. On the other hand, in AES-256-GCM encryption, the level of security provided is good, but it also adds overheads in performance [14], more so with the transfer of large volumes of financial data. Securing all networks against data in motion represents another problem in upholding the scenario, since there are loopholes that exist in VPN tunnels through which data may get exposed while being transmitted. Access control and authentication of a user in a distributed system create a complexity that is prone to security gaps [15]. Finally, a scalability problem arises in extending these controls such that they will apply to very large datasets that differ from one application to another, while rigorous security conditions are maintained. The contribution of the paper is below:

- Design of a secure financial transaction framework that adopts encryption methodologies up to AES-256-GCM standards in IPSec VPNs and cloud storage relative to data confidentiality, integrity, and availability.
- Implementation through a multi-layered security architecture combining all types of encryption with secure transmission and cloud storage, which makes sensitive financial information unattainable to unauthorized access and tampering.
- Addressed Issues on Scalability and Performance for securing enormous amounts of financial data, highly compliant according to industry standards as PCI DSS and GDPR.

2. Literature Survey

The birth of the impending surround cloud environment has raised many more questions about how financial services would be delivered. The only thing that niche would call for clouds was: flexible, scalable, cost-effective, and many, many more [16]. Allocation of such names usually conjures for greatest troubles to the entire data governance, i.e., having fragmented data, different security postures, a plethora of regulations imposed, and even that of data integrity breach or availability, among many others. To facilitate such an undesired open road ahead, the school or institution must provide a protective wall for sensitive information while fulfilling all requirements imposed under such internal governance of data [17]. Plus, tie clouds with data governance frameworks, ultra-modern new-age encryption, and tokenization, and then fit all those in real-time monitoring of anomalous behaviour with AI and next-level Machine Learning. It would be highly crucial that achieving it through proper development and education, mankind has to keep up with the new skills [18]. Due to automated processes, an overdose of human intervention would not lead to less human error consistency in policy enforcement, effective data management, more overhead resources, and full compliance with the regulatory standards. The methodologies of the authors regarding the management and protection of secret data are relayed in this paper, whereby securing data services is given prominence [19]. This information-sharing protocol secures data services as classified into different levels of safeguarding information. The new class of protocols, dubbed intelligent linguistic threshold schemes, which employ cryptographic threshold techniques with a linguistic method to split a secret among a pool of secret trustees,

is proposed by the authors [20]. The proposed solutions are applicable at different levels of data management, including the specific processes of cloud management, and all of them will be evaluated for feasibility. By a certain theoretical special graph formalism, a new aspect is introduced: that of forming a secret representation, which may then be split and transmitted over a disseminated network. Capabilities of business analytics are desired to provide better security management to cloud computing applications; thus, these capabilities are an important antecedent for any program to implement security enhancements for cloud computing applications. A work model about this construct would rest upon the value chain theory of information and the theory of IT affordance, through which IT affordances would inform the research model to understand the underlying mechanism through which business analytics affordances enhance data security management in cloud computing. The model describes analytics affordances in terms of cloud computing's good affordances concerning decision making, wherein rationality is extended toward cloud computing data security decision-making and management in maintaining respect for cloud computing data security. In this scenario, it considers the role played by culture driven through data integration and IT business processes. A partial least squares-based structural equation model was used on the data collected with 316 companies as an empirical test of the model [21]. Results without data-driven culture and IT business-process integration imply a process from business analytics affordances to decision-making-affordances concerning cloud-computing data security, followed by rationality of decision-making regarding cloud-computing data security, and finally management concerning cloud-computing data security. From the viewpoint of mediation, data-driven culture and IT business-process integration had a positive influence on the relationship between business analytics affordances and decision-making affordances of cloud-computing data security. Findings of the current study are of great reference value for enterprises in strengthening management of cloud-computing data security through the use of business analytics. Cloud computing service providers are rendering their services to enterprises and individuals in light of rapid growth in big data and big data analytical techniques. In many large enterprises, setting up a cloud computing platform environment enables the placing of several enterprise services onto the cloud platform to deliver resource-sharing services to various departments. With competitive improvements in the computing performance of computer clusters, big data and cloud computing technologies have been maturing [22]. We would like to combine cloud with services in financial management, thereby using innovative modern techniques to create a novel financial management model that would change the paradigm of financial management for enterprises constructed on the back of financial sharing service centers offering much better financial management service efficiency. Apart from exploring the research efforts being implemented in cloud computing technology, this paper elaborates on the application of cloud computing in financial sharing, as well as the transformation of financial management models in the reputable context of cloud computing [23]. Clarify the full set of principles and procedures for the building of financial sharing service centers on the foundation of cloud computing, explaining the basic structure of financial cloud management. Finally, in this paper, we will discuss the operation model of financial management based on cloud computing that would serve as a good reference for other researchers in the field of financial management.

3. Problem Statement

Therefore, the occurrence of almost predominantly digital financial transactions that have caused a colossal threat to highly sensitive financial data might not come as a shock. This predisposes current increasingly broader sets of data on financial transactions to risks caused by unauthorized access, cyber attack, and breaches that already cause thousands of dollars worth of loss and, more tragically, public trust in the digital financial system. Conventional security mechanisms cannot anymore safeguard sensitive financial data from its creation to storage-while current strategies and protocols have never been truly effective in addressing threats against data through all its stages [24]. Some of the common functionalities in the convenience of these financial systems have been either not end-to-end encrypted during transit or else utilized insecure storage solutions, which made financial data available to would-be attackers. Organizations face problems of maintaining the integrity of data being encrypted and also guarding the data against unauthorized amendments that could result from fraud or fault in accounting, or both. The next challenge would be scalability, since organizations would need to install a highly scalable architecture around their secure storage design to cater for the extremely high volumes of financial transactions expected to soar in complexity and size over time increasingly more flexible, robust storage system is needed to adequately process huge datasets without compromising on security [25]. Another major venture is the architecture of a

more comprehensive security framework for encrypting and securing financial data, while ensuring, at the same time, its confidentiality and integrity in the course of the entire lifecycle. This should incorporate secure data collection, encryption through robust algorithms, transmission over possibly untrustworthy channels, and storage solutions associated with the cloud, with effective scalability with growing demands and data safekeeping. Presumably, tighter closure of these gaps would do much more in reducing breach probabilities while conforming to the requirements of the regulatory framework and protecting confidentiality, integrity, and availability of financial data from increased threats in a digital economy. Total digital financial transactionality poses a much larger threat to very sensitive financial data, endangering more and more sets of financial transaction data. Such datasets are endangered by unauthorized access, cyber attacks, and breaches, which finally lead to massive loss and sometimes worse destabilization of trust in the digital financial system. Conventional security mechanisms are not working up to the mark nowadays in protecting sensitive financial data, as they realize very little about threats to data in an entire life cycle, from data collection to data storage-since they are not addressing threats. Common failures across the convenience of these financial systems are usually not end-to-end encrypted while in transit, and use unsafe storage solutions, making financial data available to would-be attackers.

4. Proposed Methodology

The diagrammatic flow indicates that it provides for proper procedures for access, and therefore will secure and safeguard accuracy concerning the financial transactions' data throughout its entire life cycle. The first process is termed Data Collection, where financial transaction data collated from several sources constitutes a primary dataset. Data relevant for analyses and decision-making shall be safeguarded against all potential threats of insecurity. After undergoing data collection, encryption is performed using AES-256-GCM, a very common and well-proven encryption scheme recognized for both strong encryption and performance qualities. Encryption protects the confidentiality of data by converting it to an unreadable condition and prevents unauthorized access. However, even though AES-256-GCM encrypts the data in a very confidential manner, the authenticated encryption will also ensure integrity, thus making the algorithm appropriate for sensitive data. During the Secure Transmission process, encrypted data is transmitted via an IPsec VPN Tunnel. The additional protections ensure that there are no eavesdroppers to listen to the channel or modify the information. It provides for additional security while their data is transported over a possibly untrustworthy network. Come along the tunnel, the encrypted data will be stored in Cloud Storage. This is where the cloud has its offering designed to ensure given authority have access to the data while keeping it secure. Massively storing financial data will benefit from cloud storage in terms of scalability and achieving the needed security. This methodology guarantees an extra layer of security applied to the financial transaction data set at the collection, encryption, and secure transmission, and ends at the storage level. This ensures that whatever means are used in the secure handling of sensitive financial data within the digital space are fortified by advanced encryption algorithms and secured transmission protocols. Cloud storage is that which provides maximum flexibility and scalability with this application theory to ensure authorized accessibility. This means that it is a very good point of this whole approach in massively reducing the risk of data leakage and cyber-attacks while promoting the confidentiality, integrity, and availability of financial data.

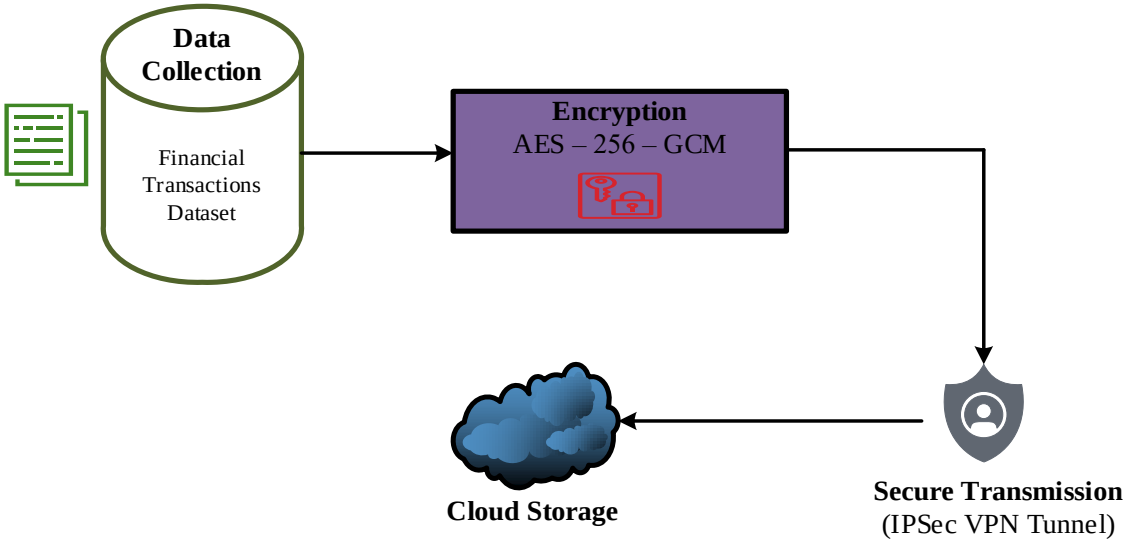

Figure 1: Overall architecture of the proposed method

4.1 Data Collection

During the Data Collection phase of the above model, the financial transaction data is gathered from various sources, which can be payment gateways, transaction records, bank statements, and financial systems. The information is of great importance in establishing a reliable and correct dataset for subsequent analysis, reporting, and decision-making procedures. It provides the ground for transaction behavior patterns, consumers' behavior, and money styles analysis, the necessity to appropriately govern financial processes. At this point, retaining integrity and protection of collected information is important, as any revealing or corruption of personal financial details may lead to extreme privacy desecration as well as legal infractions. This is the initial part of the follow-up processing, such as encryption, safe transit, and storage, wherein all collected data will be safeguarded prior to follow-up action for confidentiality and compliance. Careful handling of the data gathering process ensures that only relevant and clean financial transaction information is fed into the system for follow-up processing in the system.

4.2 Encryption

The encryption operation secures the financial transaction data through the AES-256-GCM algorithm. AES stands for Advanced Encryption Standard, a symmetric-key encryption algorithm so strong that it is accepted in practice for securing almost any sensitive data with confidence. AES-256-GCM stands for Advanced Encryption Standard with a 256-bit key in Galois/Counter Mode (GCM), which provides confidentiality and integrity for that data. Rather than allowing data in financial transactions to be read clearly by unauthorized users, it will ensure that the integrity is assured through authenticated encryption.

4.2.1 Steps in AES –256– GCM Encryption

Key Generation: A random encryption key of 256 bits is created and is referred to as K for encrypting or decrypting the data.

Initialization Vector (IV): The IV for the AES-256-GCM possesses the property that encrypting the same plaintext will yield different ciphertexts. Each IV is made unique, such that it cannot repeat during one session of encryption.

Encryption: The plaintext message (denoted P) is the one undergoing the AES encryption via the 256-bit key and IV. The AES algorithm, therefore, applies multiple rounds of substitution, permutation, and transformation during which the plaintext becomes ciphertext, here represented as C. The AES encryption operation can be represented as:

$$C = AES - 256 - GCM(P, K, IV) \quad (1)$$

Here, the plain text is p, the 256-bit encryption key is K, the initialization vector is IV, and the ciphertext is C.

Tag Authentication: By providing encryption, AES-256-GCM additionally provides data integrity through the creation of an authentication tag T. The authentication tag will be recognized in the creation process when the data is fed to indicate that the existing input data, being encrypted, has not been compromised with input or output. This tag formation is important for ensuring that the data has not been corrupted during transmission or storage.
The tag generation can be represented as:

$$T = GCM - Authenticate(C, IV, K)$$

(2)
C is the binding of multiple pieces starting with the ciphertext, where the original order is C (thus the ciphertext), followed by the initialization vector (IV), then the encryption key (k), with the authentication key (T) finally closing the group.
Final Output: The outcome of the encryption process is the ciphertext C, which, alongside the authentication tag T, is transmitted to ensure both confidentiality and integrity of the data. Hence, even in cases of eavesdropping, the encryption will not work due to the wrong key, and any modification will be detected during decryption.
Therefore, the final output for the encrypted data can be represented as:

$$\{C, T\} = AES - 256 - GCM(P, K, IV)$$

(3)

4.3 Secure Transmission

Confused transfer involves the conveyance of encrypted financial transaction data through the creation of an IPsec VPN Tunnel through which the encrypted data is transmitted. After transmission through a secure method, the data has to be encrypted itself with AES-256-GCM. It is said that secure transmission prevents interception and modification in transit. An IPsec VPN tunnel would, therefore, provide the security mechanisms for data confidentiality and integrity in otherwise insecure networks like the Internet.

Key Features of Secure Transmission:
Confidentiality: IPsec encrypts communication between its sender and its receiver, thus keeping the communication private during transmission. Hence, no one else is going to be able to read it.
Integrity: Integrity of the transmitted data is an important one- it gets identified and discarded if any such changes have taken place in it.
Authentication: As authentication is done by IPsec, it is ensured that the source of a particular data using the authentication cannot gain unauthorized access to it via some other means.
VPN Tunnel: IPsec creates a secure "tunnel" for the otherwise unsecured surrounding networks for the transmission of encrypted data to an endpoint.
The mathematical representation of Secure Transmission is

$$\text{Secure Transmission} = \text{IPsec}(\text{C}, K_{trans,} IV_{trans})$$

(4)
Where C is the ciphertext generated by AES-256-GCM encryption, K_{trans} is the transmission key used by the IPsec protocol to encrypt and decrypt the data within the VPN tunnel, IV_{trans} is the initialization vector used to ensure the uniqueness of the encrypted data packets during transmission.

4.4 Cloud Storage

Another section would typically provide some information on financial transactions sent over secure communication channels. Physically scalable to any extent, the system, in practice, would accommodate limitless sensitive data. Thus, in addition to real-world security, securing the data in use assures legitimate persons an opportunity to access the data when held in the cloud. This goes far beyond standard access control mechanisms and encryption in use, even up to an administrative permission level. In turn, the cloud service would have thought of having those redundancies in place that would protect from local power failure and corruption of financial records. Data loss at the point of time, corruption, and failure of the system ultimately lead to unavailability or unavailability and integrity. Some very elementary management features would allow efficient indexing and retrieval of the financial-related information across some primary storage features offered by the cloud, essentially. This will augment the aspect of timely delivery of such data for any analysis or decision-making. Another take regarding the cloud storage indicates that enterprises may scale up or down on their storage needs as the requirement for data changes at all times in

the present and near future. The most severe reservations would apply if the cloud storage were to assume a position somewhere between other cloud services, enabling these institutions to perform advanced analytics about transaction trends through those advanced analytical tools. Yet again, cloud storage would remain a huge guarantee toward realizing security, availability, and scalability compatibility under the entire system security framework for their encrypted financial transactions.

5. Dataset Description

The Financial Transactions Dataset encapsulates tracks of transactions transacted between users in terms of transaction-ID, customer-ID, amount, type of transaction, date-time, payment method, and much more. It consists of not only the legitimate transactions but also the frauds; hence, it becomes ideal for anomaly and pattern detection concerning fraud in the financial domain. Actual database utilizing training and testing models on transactions classification and using predictive and fraud detection analytics in financial systems. The dataset contains all whole details that are needed for making secure management systems for financial data and even further improving algorithms for fraud detection.
Dataset Link: https://www.kaggle.com/datasets/cankatsrc/financial-transactions-dataset

6. Result And Discussion

The work is situated on a system configuration consisting of the 12th Gen Intel(R) Core (TM) i5-12400 Processor, 8 GB RAM, and a 64-bit OS based on the x64 processor architecture. The additional system requirements for the work should consist of a minimum of 4 GB RAM (with 8 GB recommended), an OS of at least Windows 7, a fairly modern CPU (Intel i3 or better), and reasonable storage space (100 GB recommended). The implementation work used PyCharm version 3.11.

6.1 Encryption Time for AES-256-GCM

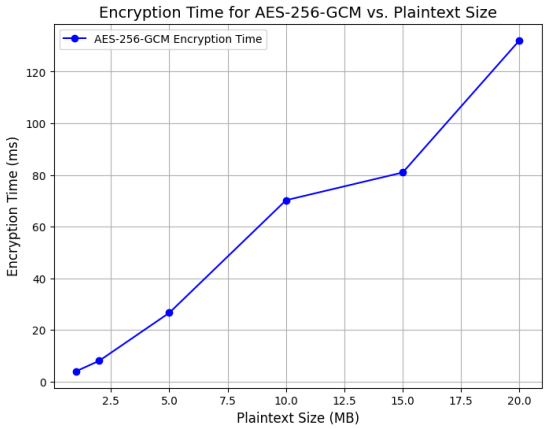

Figure 2: Encryption Time for AES-256-GCM

Figure 2 shows the relationship between the time spanned by AES-256-GCM encryption and the size of the plaintext. It is seen that by increasing the plaintext size, the time spent for the corresponding encryption also increases fairly substantially, almost in a direct-linear proportionality. Encryption time is recorded on the scale of milliseconds (ms) and varies from about 20 ms for small data amounts to more than 120 ms for larger amounts. This indicates that for larger quantities of data, encryption requires much more computational effort when using the AES-256-GCM algorithm.

6.2 Security Comparison with and Without AES-256-GCM

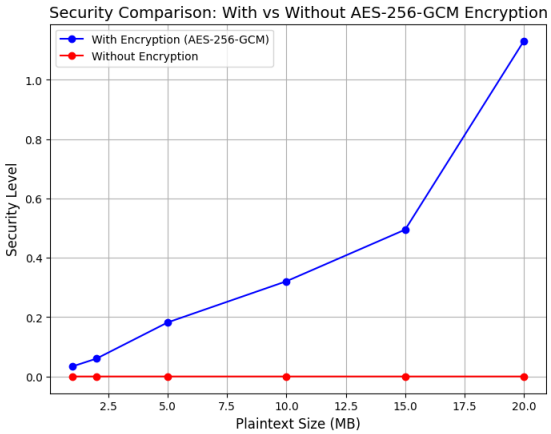

Figure 3: Security Comparison with and Without AES-256-GCM

Figure 3 shows a comparison between strong security and no security with AES-256-GCM encryption over various plaintext sizes. The blue line evidences an increasing security level with increasing plaintext input to encryption, which is corroborated by the rapid rise in security observed with increases in the data size. However, the red line representing the security levels of unencryption is kept at a low constant value and does not change irrespective of the size of the data. Contrasting such lines depicts how encrypted data is essentially safe, especially as the data size increases.

7. Conclusion

It is the study of end-to-end security of transactional data using AES-256-GCM encryption, a Virtual private network via IPsec, and cloud storage. In the case of large enough data sizes, encryption will sufficiently secure transactional data. AES-256-GCM theoretically quite probably secures the data very well, but has minimal performance overhead, especially on very large data. It also states the need for a scalable security model that will capture the complexities of the modern-day financial systems, which will, by design, withstand data breach attacks under certain constraints and will ensure security, integrity, and availability of financial transaction data. The parameter scalability, having withstood a thorough investigation, is left for a prospective group of researchers to verify better through more secure encryption algorithms, enhancing performance without the corresponding risk of security.

References

1. Wang, Y., Tao, X., Ni, J., & Yu, Y. (2018). Data integrity checking with reliable data transfer for secure cloud storage. International Journal of Web and Grid Services, 14(1), 106-121.
2. Zhang, Y., Xu, C., Liang, X., Li, H., Mu, Y., & Zhang, X. (2016). Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation. IEEE Transactions on Information Forensics and Security, 12(3), 676-688.
3. Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2018). Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. IEEE Transactions on Information Forensics and Security, 14(2), 331-346.
4. Liang, W., Tang, M., Long, J., Peng, X., Xu, J., & Li, K. C. (2019). A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things. IEEE Transactions on Industrial Informatics, 15(6), 3582-3592.
5. Wang, T., Bhuiyan, M. Z. A., Wang, G., Qi, L., Wu, J., & Hayajneh, T. (2019). Preserving balance between privacy and data integrity in edge-assisted Internet of Things. IEEE Internet of Things Journal, 7(4), 2679-2689.
6. Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), 767-778.
7. Tan, S., Song, W. Z., Stewart, M., Yang, J., & Tong, L. (2016). Online data integrity attacks against real-time electrical market in smart grid. IEEE transactions on smart grid, 9(1), 313-322.
8. Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE transactions on reliability, 69(3), 1077-1086.

9. Yuan, J., & Yu, S. (2015). Public integrity auditing for dynamic data sharing with multiuser modification. IEEE Transactions on Information Forensics and Security, 10(8), 1717-1726.
10. Xu, Y., Ren, J., Zhang, Y., Zhang, C., Shen, B., & Zhang, Y. (2019). Blockchain empowered arbitrable data auditing scheme for network storage as a service. IEEE Transactions on Services Computing, 13(2), 289-300.
11. Li, Y., Yu, Y., Min, G., Susilo, W., Ni, J., & Choo, K. K. R. (2017). Fuzzy identity-based data integrity auditing for reliable cloud storage systems. IEEE Transactions on Dependable and Secure Computing, 16(1), 72-83.
12. Zhang, A., Wang, L., Ye, X., & Lin, X. (2016). Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. IEEE Transactions on Information Forensics and Security, 12(3), 662-675.
13. Yang, Q., An, D., Min, R., Yu, W., Yang, X., & Zhao, W. (2017). On optimal PMU placement-based defense against data integrity attacks in smart grid. IEEE Transactions on Information Forensics and Security, 12(7), 1735-1750.
14. Wang, B., Kong, W., & Li, W. (2019). A Dual-Chaining Watermark Scheme for Data Integrity Protection in Internet of Things. Computers, Materials & Continua, 58(3).
15. Zhang, A., Chen, J., Hu, R. Q., & Qian, Y. (2015). SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks. IEEE Transactions on Vehicular Technology, 65(4), 2659-2672.
16. Li, J., Yan, H., & Zhang, Y. (2018). Certificateless public integrity checking of group shared data on cloud storage. IEEE Transactions on Services Computing, 14(1), 71-81.
17. Hang, L., & Kim, D. H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. sensors, 19(10), 2228.
18. Jiang, T., Chen, X., & Ma, J. (2015). Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Transactions on Computers, 65(8), 2363-2373.
19. Wang, H., He, D., & Tang, S. (2016). Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud. IEEE Transactions on Information Forensics and Security, 11(6), 1165-1176.
20. He, D., Kumar, N., Zeadally, S., Vinel, A., & Yang, L. T. (2017). Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries. IEEE Transactions on Smart Grid, 8(5), 2411-2419.
21. Ahmed, S., Lee, Y., Hyun, S. H., & Koo, I. (2019). Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. IEEE Transactions on Information Forensics and Security, 14(10), 2765-2777.
22. Partala, J. (2018). Provably secure covert communication on blockchain. Cryptography, 2(3), 18.
23. Xu, X., Zhang, X., Gao, H., Xue, Y., Qi, L., & Dou, W. (2019). BeCome: Blockchain-enabled computation offloading for IoT in mobile edge computing. IEEE Transactions on Industrial Informatics, 16(6), 4187-4195.
24. Zhang, Y., Xu, C., Lin, X., & Shen, X. (2019). Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Transactions on Cloud Computing, 9(3), 923-937.
25. Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2018). Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet of Things Journal*, *6*(1), 410-420.