International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Time Variant Password Okamoto–Uchiyama Cryptography based Three Layer Authentication for Secured Financial Transaction

[1] N. Ruba, [2]Dr. A. Shaik Abdul Khadir

Submitted: 10/10/2023 **Revised:** 30/11/2023 **Accepted:** 08/12/2023

Abstract

Cloud computing enabled customers to save data on a cloud server for scalable services. The Internet of Things (IoT) provides a virtual representation for physical objects in order to share data and adapt to environmental changes with efficient resource utilization. IoT include distributed sensor nodes to gather cloud user information from different location through wireless medium. A financial transaction represents the exchange of goods, services, or assets for payment and serves as a form of communication between the buyer and seller. Different authentication methods are introduced by existing researchers for performing efficient secured financial transaction. However, there was no enhancement in authentication accuracy, and the authentication time remained unimproved. In order to address these issues, an IoT framework with three layer authentication called Time Variant Password Okamoto–Uchiyama Cryptography based Three Layer Authentication (TVPOUC-TLA) Method is introduced. The main aim of TVPOUC-TLA Method is to perform IoT based efficient financial transaction with higher confidentiality rate. TVPOUC-TLA Method covers four steps, which are crucial generation, encryption, authentication and decryption for taming the safety level performance in cloud environment. In the TVPOUC-TLA Method, a cloud user located in a different location (acting as the buyer) initiates the registration process with the cloud server (acting as the seller) to facilitate authentication. During the strategic key generation phase, the Cloud Server (CS) generates both the public and private keys for the registered cloud user. Whenever a cloud user needs to perform any financial transaction, cloud user gets logged in with help of key pair and transmits the demand note to the CS. Later getting request, CS confirms the cloud manipulator authenticity through sending the time variant password and fingerprint. When the cloud user pass in password and fingerprint acquires matched with CS sent password, cloud manipulator has said to be an authorized user and accomplish financial transaction. Otherwise, the transaction between cloud server and cloud user gets declined. This approach enables the efficient and secure execution of financial transactions through the TVPOUC-TLA Method. An experimental assessment is conducted, focusing on factors including authentication accuracy, data confidentiality rates, and data integrity, taking into account variations in the number of financial data entries and cloud users.

Keywords: *Internet of Things, Financial Transaction, Authentication, Okamoto–Uchiyama Cryptography, Fingerprint*

1. Introduction

Despite the rapid evolution of information, communication, and data security, ensuring reliable computing remains a primary concern in contemporary cloud computing applications. SADS-Cloud for Big Data Environment has been introduced [1]. To divide the input file into fixed-size of blocks, the MapReduce paradigm was employed. For secure file retrieval, the SALSA20 Encryption algorithm was used in each block. However, SADS-Cloud did not enhance authentication accuracy. In [2], an effective and publicly verifiable method was introduced for enhancing the security of data transfers in cloud computing, aimed at facilitating secure communication among various users. This approach employed a public key-based homomorphic authenticator with random masking for privacy preservation during data transmission. It is important to note, though, that despite these efforts, the designed approach did not lead to improvements in the data integrity rate.

In [3], a combination of blockchain technology and attribute-based signcryption has been devised to achieve efficient and secure data distribution while enhancing data confidentiality. However, the data integrity has not been improved by designed signcryption. BVOABSC has been designed for secured health record distribution [4]. However BVOABSC method minimized

[1]*Research Scholar, Dept of Computer Science, KhadirMohideen College, Adirampattinam, Thanjavur Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India,email id: rubaanand17@gmail.com*
[2]*Associate Professor and Head, Dept of Computer Science, KhadirMohideen College, Adirampattinam,Thanjavur Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India, email id: hiqmath4u@gmail.com*

the time and cost, the data confidentiality rate has not been improved.

In [5], a privacy preservation technique was developed for data sharing in the cloud, where the group manager was responsible for system initialization. This privacy-centric approach outperformed others, achieving the highest detection rate with minimal computation cost and memory usage. However, it's important to note that the designed technique did not reduce computational complexity.

Additionally, in [6], Securely Encrypted Data Access Policies (SEDAP) were introduced for the cloud platform. SEDAP comprehensively understands cloud services and access from various perspectives, including user actions and jobs initiated by users. SEDAP attained better solidity and guaranteed multilevel security in cloud. But, the data integrity was not improved by SEDAP.

A two-phase search framework termed SecVKQ was introduced in [7] with screening phase and search phase. SecVKQ used secure data separation and adaptive encryption strategy. But, the computational cost was not reduced by SecVKQ. In [8], the Duplicateless Encryption for Simple Storage (DupLESS) scheme was introduced for storing data in a remote storage environment. DupLESS scheme maintained the key and data on single storage server. DualDup framework was used to optimize the storage through minimizing the duplicate encrypted data from multiple users. However, the authentication time was not reduced by DupLESS scheme.

In [9], a Hadoop-based secure big data storage scheme was created to distribute the NameNode service across multiple servers, employing HDFS federation and HDFS high availability mechanisms to coordinate each node for dual-channel storage. However, it's noteworthy that the designed scheme did not reduce time complexity.

Furthermore, in [10], the DistB-SDCloud architecture was introduced to enhance cloud security for smart IIoT applications. This structural design utilized a distributed blockchain method to improve security, privacy, and integrity. Nevertheless, the computational complexity was not reduced by the designed architecture.

More authentication time, more computational complexity, lower data integrity rate, lower confidentiality rate, higher encryption time, higher computational cost, and so on are the difficulties identified in the preceding research. In order to address these issues, Time Variant Password Okamoto–Uchiyama Cryptography based Three Layer Authentication (TVPOUC-TLA) Method is introduced.

1.1 Research Contribution:

- The main contributions of the research can be summarized as follows:
- TVPOUC-TLA Method is introduced to perform IoT based efficient financial transaction. TVPOUC-TLA Method performs strategic generation; encryption, decryption and authentication are used for enlightening security level.
- The cloud user in a different location registers the cloud user's details to the cloud server for authentication in the TVPOUC-TLA Method.
- CS produces a public and private key pair for each registered cloud manipulator. If cloud user has to perform any financial transaction, cloud user gets logged in and transmits the request message to the CS.
- CS verifies cloud user authenticity through sending a time variant password and fingerprint. Using the TVPOUC-TLA Method, an efficient secured financial transaction is carried out.

2. Related Works

In [11], a unique DNA-based data encryption technique for cloud computing environments was developed. Based on DNA computing, user attributes, and the user's Media Access Control (MAC) address, a 1024-bit secret key was produced. A two-layer encryption scheme was introduced in [12] with chaos based cryptography and DNA computing to perform solid encryption for cloud environment. The designed scheme used SHA-512 technique for control parameter selection.

[13] proposed a secure R-Tree index structure with a secure grouping protocol to allow for the grouping of relevant private variables with increased querying efficiency. Over the outsourced cloud, an efficient, secure, and verifiable KNN set similarity search system was built. However, there was no improvement in data integrity. In [14], a data transmission structure known as HBRSS was invented for highly secure data transmission and processing in the cloud. HBRSS partitioned the data into blocks and formed a block ring based on blockchain using the data splitting principle.

In [15], a blockchain-based ciphertext-policy attribute-based encryption method was developed for secure cloud data delivery. However, it's worth noting that this method did not lead to an increase in the data confidentiality rate. A trapdoor-based Non-Dominated Sorting Genetic Algorithm Access Control (NDSGA-II AC) was designed in [16] to minimize the energy consumption. A stream cipher algorithm (SCA) was employed to encrypt input data based on water tank parameters obtained from

sensors. Nevertheless, the NDSGA-II AC approach did not succeed in reducing the computational cost.

Blockchain-based reliability protection method has been designed to reduce the storage and time complexity [17]. Then, the designed approach not improved authentication accuracy. In [18], the Machine Learning-created Secure Cloud Job Services (MLSCS) were introduced to enhance multi-level security within a cloud job checking system. MLSCS achieved this by eliminating irrelevant cloud jobs, thereby minimizing scheduler complexity and processor utilization.

A secured and dependable structural design has been introduced in [19] for performing efficient electronic health data to improve the efficiency. However, the mechanical design has not been efficient to perform secured and dynamic method. In [20], the Secure Aware Scheduling Model (SASM) was introduced to enhance security and manage scheduling in cloud computing. The incorporation of the SXOR function contributed to increased security by facilitating encryption and decryption processes in cloud computing.

3. Time Variant Password Okamoto–Uchiyama Cryptography Based Three Layer Authentication

Cloud computing platform is developing one for increasing the security in the financial data transaction. The system model of TVPOUC-TLA Method is presented with cloud users and cloud server for financial data transaction.

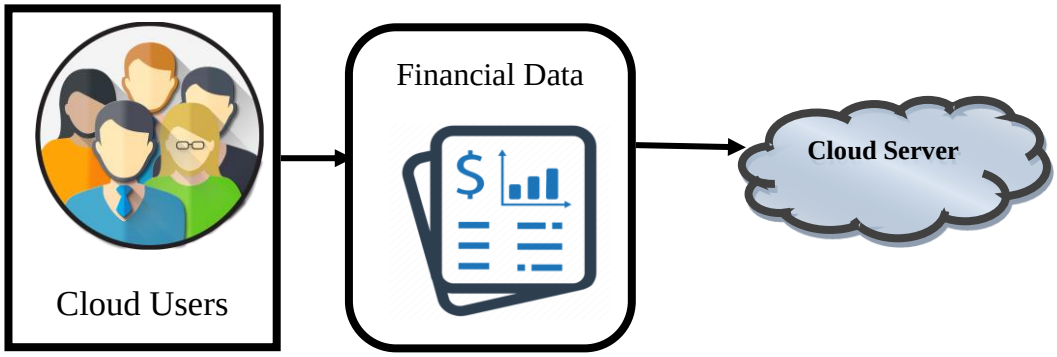

Fig 1 Financial Data Transmission Model

Figure 1 illustrates the system model for secure financial data transmission, encompassing both cloud users and cloud servers within the designed framework. The cloud users $CU_1, CU_2, CU_3 \ldots . CU_n$ with financial data $fd_1, fd_2, fd_3, \ldots . fd_m$ stored in cloud server 'CS' in secured manner. The TVPOUC-TLA Method includes registration, encryption, authentication and decryption. The three processes of TVPOUC-TLA Method are described in upcoming subsections.

3.1 Time Variant Password Okamoto–Uchiyama Cryptography based Three Layer Authentication

A novel TVPOUC-TLA Method has introduced for increasing the data privacy in cloud environment. In TVPOUC-TLA Method, a Time Variant Password Okamoto–Uchiyama Cryptography is the public key cryptography. Time variant password is the encryption keys generated randomly for certain time period. TVPOUC-TLA Method avoids the unauthorized user from data access.

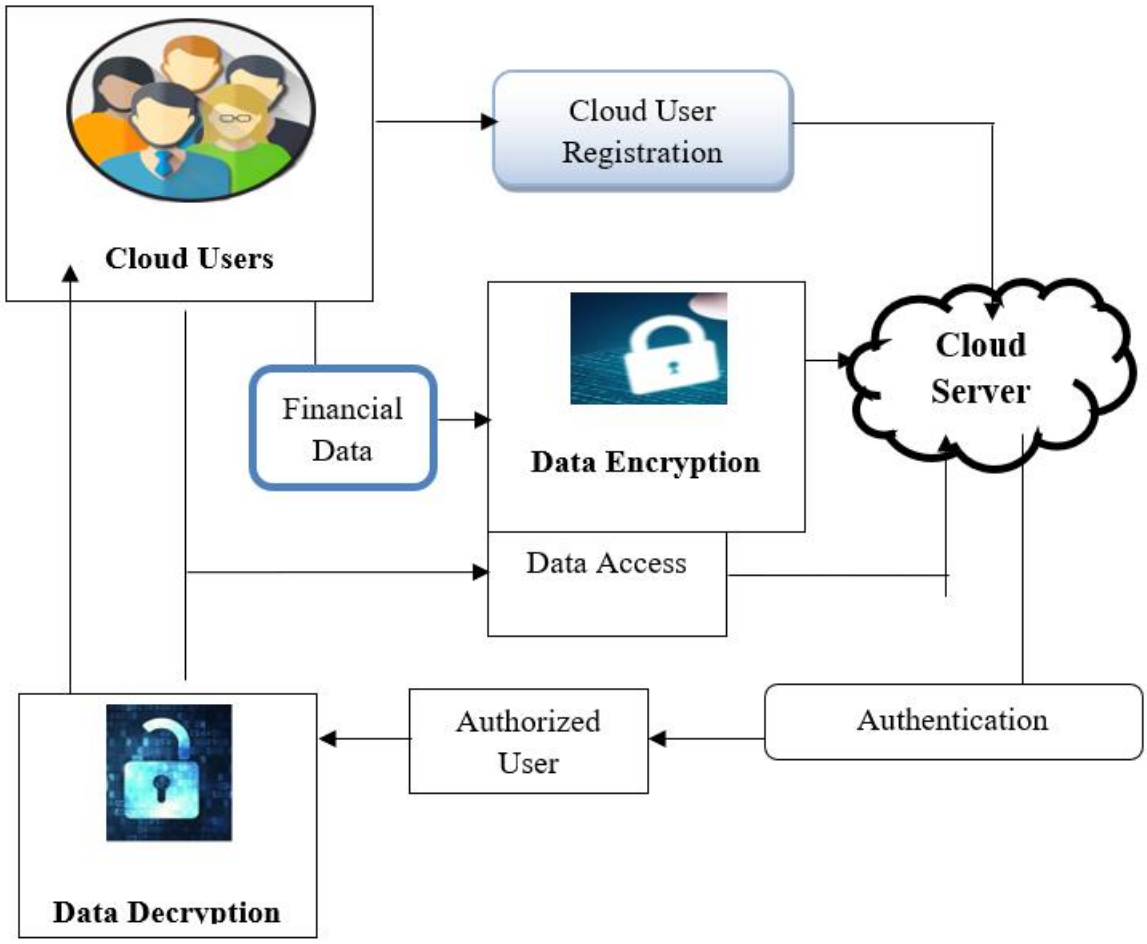

Fig 2 Architecture diagram of Proposed TVPOUC-TLA Method

Figure 2 explains the structural diagram of the proposed TVPOUC-TLA Method for secured data transaction in a cloud.

3.1.1 Registration

Initially, the proposed TVPOUC-TLA methods register details to cloud server before storing the data. Let's assume that a financial data transaction has been conducted to securely store a significant amount of cloud user data in the cloud server. Every cloud user in cloud server, registration has been performed by cloud server. Throughout the registration phase, the cloud manipulator data names like original, middle, last, birth date, genders, contact, age, monthly income, weight, etc. After the registration process, the cloud server generates a key pair for each registered user. The key pair has been generated using Okamoto–Uchiyama Cryptographic technique. It is given as,

$$Pb_k = (Matrix, weight) \quad (1)$$

$$Matrix = B_s P_c P \quad (2)$$

$$Pv_k = (B_s, P_c, P) \quad (3)$$

From (1), (2) and (3), 'Pv_k' symbolizes the private key. 'Pb_k' represent the public key. In this context, 'B_s' represents the binary non-singular matrix, while'P_c' stands for the parity check matrix. 'P' represents the permutation matrix. By this manner, the key pair has been produced designed for all listed users in cloud.

3.1.2 Okamoto–Uchiyama Cryptographic Encryption

In TVPOUC-TLA Method, data encryption is a technique of encrypting financial data earlier sending from one place to another place. In addition, the data exists whipped during allocation to the cloud server. Consequently, the TVPOUC-TLA Method used for Okamoto–Uchiyama Cryptographic Encryption for guaranteeing improved security in cloud server. Okamoto–Uchiyama Cryptographic Encryptionis an asymmetric key cryptographic algorithm with public key and private key. Encryption is performed using the receiver's public key to protect financial data from unauthorized access.

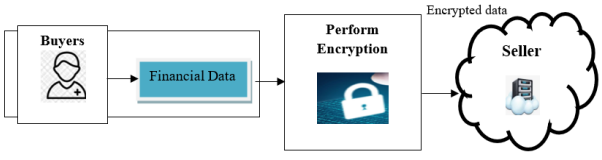

Fig 3 Block Diagram of Okamoto–Uchiyama Cryptographic Encryption

Figure 3 illustrates a block diagram of Okamoto–Uchiyama Cryptographic Encryption process to enrich the financial data transmission security. Let us consider the financial data '$fd_1, fd_2, fd_3, \ldots . fd_m$'. The input financial data has been encrypted into string of bits. The financial data is encoded with receiver public key. It is formulated as,

$$CT = Rbs_j{}^T \quad (4)$$

From (4), 'CT' symbolizes the ciphertext, 'bs_j' symbolizes the bits of strings, 'T' represents the transpose. 'R' portrays the public key.

3.1.3 Bivariate Coefficient Authentication

When a cloud consumer needs to access data from the server, the cloud user is required to validate its authenticity. Later getting request, cloud server confirms the user authenticity through transmitting a time variant password.

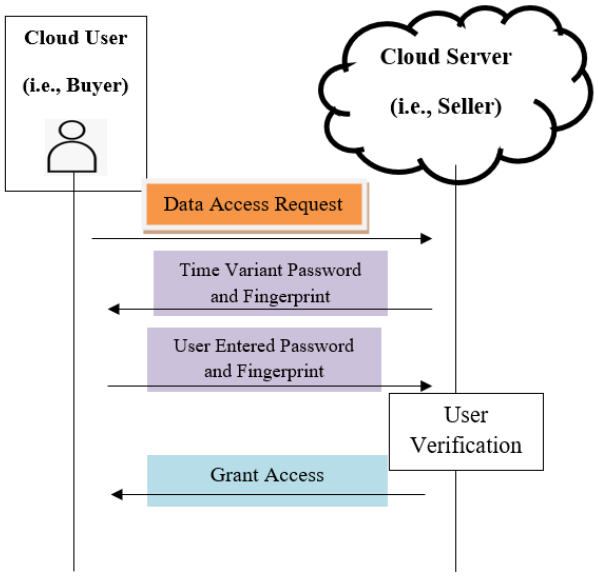

Fig 4 Authentication Process

Figure 4 illustrates the user authentication process in cloud. The user sends a request message to the server. When receiving request, server transmits a time variant password (X). When the user entered password (X_i) acquires matched with the cloud server sent password, the user has been considered as user with proper authorization and permitted to access the data from cloud server. A time variant password and fingerprint has been matched through bivariate coefficient. Bivariate coefficient is a similarity index used for validating a time variant password and fingerprint. The bivariate correlation is computed as,

$$BC = \frac{\sum X * X_i}{\sqrt{\sum X^2 \sum X_i{}^2}} \quad (5)$$

From (5), 'BC' indicates the bivariate similarity coefficient, $\sum X * X_i$ represents the amount of product of balancing score of two session passwords, $\sum X^2$ implies the squared score of X and $\sum X_i{}^2$ denotes the squared score of X_i. Bivariate correlation coefficient (BC) attains a value ranging from '-1' to '+1'. When the similarity coefficient equals '+1', it indicates that both the password and fingerprint have been matched correctly, and the user is regarded as an authorized user eligible to conduct financial transactions. If not, the user is classified as unauthorized and the financial transaction is denied.

3.1.4 Okamoto–Uchiyama Cryptographic Decryption

Later performing the user authentication, Okamoto–Uchiyama cryptographic decryptionis carried out through the accredited handler obtain the original patient data. The decryption has been carried out with private key.

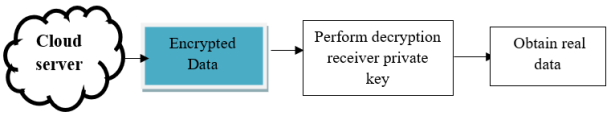

Fig 5 Okamoto-Uchiyama Cryptographic Decryption Block Diagram

Figure 5 illustrates Okamoto–Uchiyama Cryptographic Decryption process attains the original data. The private key was used to decrypt the data. The original bit message $\{0,1\}$ is acquired as,

$$b^{-1}CT = P_c P bs_j{}^T \quad (6)$$

'b' represents the binary non-singular matrix in (6). The symbol 'P_c' stands for parity check matrix. 'P' stands for the permutation matrix. The letter 'CT' represents the ciphertext. 'bs_j' represents a bit of data. The letter 'T' stands for transpose. Secure financial data transfer has been carried out in this manner, with greater data secrecy. The algorithmic method of the TVPOUC-TLA Method is still illustrated here.

// Algorithm 1 Time Variant Password Okamoto–Uchiyama Cryptography based Three Layer Authentication
Input: cloud users $CU_1, CU_2, CU_3 \ldots . CU_n$and financial data $fd_1, fd_2, fd_3, \ldots . fd_m$, cloud server 'CS' **Output:** Secured Financial Data Transmission
Begin **1: For each financial data** fd_i **2:** Cloud server informs cloud user to enter their details

3: Cloud user enters and transmits to the cloud server

4: CS generates key pairs 'Pb_k' and 'Pv_k'

5: end for

\\Data Encryption

6: For each financial data fd_i

7: Partition the financial data into string

8: Encrypt the string with public key

9: Converted into ciphertext'CT'

10: End for

\\ User Authentication

11: Cloud manipulator gets logged into system by time variant password

12: Cloud server verifies time variant password and fingerprint using correlation measure

13: $if\ (BC = 1)$then

14: Cloud manipulator is an authorized user

15: else

16: An unauthorized user is a cloud manipulator.

17: end if

//Decryption

18: For each ciphertext'CT'

19: Decrypt the data using the private key

20: Acquire the plain text

21: end if

Algorithm 1 explains step-by-step process of time variant password okamoto–uchiyama cryptography based three layer authentications in cloud platform. The cloud user registers their information with the cloud server. The cloud user sends their information to the cloud server. For registered cloud users, the cloud server produces key pairs. When a cloud user accesses stored data, the cloud server uses bivariate correlation to validate the user's identity. The correlation value returns '+1' and then cloud manipulator is an authorized user. Or else, the cloud manipulator is an unauthorized user. Consequently, the authorized users are allowed to obtain the original data with higher confidentiality of data rate.

4. Experimental Settings

Experimental evaluation of proposed TVPOUC-TLA Method and existing methods Protected Authentication and Data Sharing in Cloud [1] and efficient and publicly verifiable approach [2] has been carried out in Java language. To conduct the experimentation, the finance dataset is taken from the Kagglehttps://www.bing.com/search?q=financial+dataset&qs=n&form=QBRE&sp=-1&ghc=1&pq=financial+dataset&sc=10-17&sk=&cvid=B1834DA3FB494AE583B4D8B24297E2BA&ghsh=0&ghacc=0&ghpl= intended designed for secure data transmission on server. Finance type dataset contains the 10k rows and 5 columns. The default column represent that someone is defaulter or not in the data with yes and no data in particular column. The data be present used to accomplish the protected communication in cloud environment.

5. Result And Analysis

The performance of suggested TVPOUC-TLA Method and existing SADS-Cloud [1] and efficient and publicly verifiable approach [2] are discussed with performance metrics such as data confidentiality rate, data integrity rate and authentication accuracy.

5.1 Data Confidentiality Rate

The fraction of financial data threatened by illegal access is characterized as the data confidentiality rate. The data Confidentiality rate was calculated as follows:

$$DCR = \left[\frac{Number\ of\ financial\ data\ protected\ from\ unauthorized\ access}{Number\ of\ financial\ data}\right] * 100 \quad (7)$$

From (7), 'DCR' represent the data confidentiality rate. As a result, it is expressed as a percentage (%).

Table 1: Data Confidentiality Rate Tabulation

Number of financial data	Data Confidentiality Rate (%)		
	Proposed TVPOUC-TLA Method	**Existing SADS-Cloud**	**ExistingEfficient and Publicly Verifiable approach**
100	90	82	75
200	88	80	72
300	91	83	76
400	93	85	78
500	96	87	82
600	94	84	80
700	92	82	77
800	90	80	75
900	93	84	78
1000	95	87	80

Table 1 illuminates the data confidentiality rate comparison of proposed TVPOUC-TLA Method, existing SADS-Cloud [1] and existing efficient and publicly

verifiable approach [2]. The level of data confidentiality in proposed and existing systems has been determined. created the number of financial data varying from 100 to 1000. As illustrated an experimental results, the proposed TVPOUC-TLA Method attained better data confidentiality rate performance. When 800 financial data points are used, the data confidentiality rate of the TVPOUC-TLA Method is 90%, while the data integrity rate of the existing SADS-Cloud [1], efficient, and publicly verifiable technique [2] is 80% and 75%, respectively. Similarly, data confidentiality rate are observed for every method.

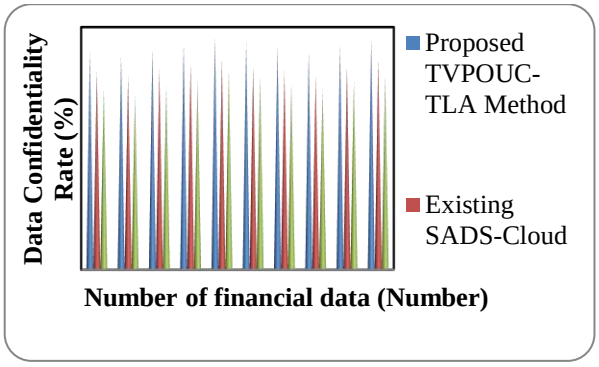

Fig 6 Data Confidentiality Rate Measurement

Figure 6 illustrates the comparative analysis assigned data confidentiality rate by means of three dissimilar security mechanisms that is proposed TVPOUC-TLA Method, existing SADS-Cloud [1] and existing efficient and publicly verifiable approach [2]. The blue color cone represents the data confidentiality rate of proposed TVPOUC-TLA Method whereas brown color and green color cone represents the data confidentiality rate of SADS-Cloud [1] and existing efficient and publicly verifiable approach [2]. Consequently, the experimental result shows that the proposed TVPOUC-TLA Method is better data confidentiality rate results than all other existing techniques. This is due to the application of Okamoto–Uchiyama Cryptography with registration, encryption, authentication and decryption. By using the cryptography, original patient data acquires encrypted and converted into ciphertext. The ciphertext is sent to the cloud server. As a result, the TVPOUC-TLA Method's data integrity rate has improved. The data integrity rate of the TVPOUC-TLA Method has been increased by 11% and 19% when compared to existing methods, according to an average of ten comparison results [1] [2].

5.2 Data Integrity Rate

The data integrity rate is defined as the proportion of financial data that is not altered by unauthorized users. The data integrity rate is calculated as follows:

$$DIR = \left[\frac{Number\ of\ financial\ data\ not\ modified\ by\ unauthorized\ users}{Number\ of\ financial\ data}\right] * 100 \quad (8)$$

From (8), 'DIR' symbolizes the data integrity rate. It is expressed as a percentage (%).

Table 2: Data Integrity Rate Tabulation

Number of financial data	Data Integrity Rate (%)		
	Proposed TVPOUC-TLA Method	Existing SADS-Cloud	ExistingEfficient and Publicly Verifiable approach
100	96	85	80
200	93	82	77
300	90	80	75
400	92	83	78
500	95	86	80
600	91	84	77
700	88	80	75
800	86	78	72
900	83	75	70
1000	87	79	73

Table 2 illustrates the data integrity rate comparison of proposed TVPOUC-TLA Method, existing SADS-Cloud [1] and existing efficient and publicly verifiable approach [2]. The data integrity rate of proposed and existing approaches was calculated using a range of financial data from 100 to 1000. As shown in experiential results, the proposed TVPOUC-TLA Method attained higher data integrity rate. When 500 financial data points are used, the data integrity rate of the TVPOUC-TLA Method is 95%, while the data integrity rates of the existing SADS-Cloud [1] efficient and publicly verifiable technique [2] are 86% and 80%, respectively. Similarly, data integrity rate are attained for every method.

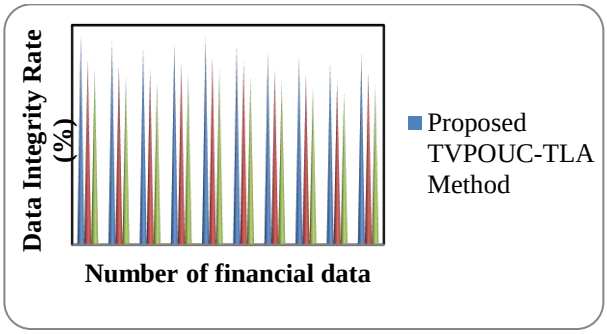

Fig 7 Data Integrity Rate Measurement

Figure 7 depicts a comparative comparison of data integrity rates using three distinct security mechanisms, including the new TVPOUC-TLA Method and the existing SADS-Cloud [1] and existing efficient and

publicly verifiable approach [2]. The blue color cone represents the data integrity rate of proposed TVPOUC-TLA Method whereas brown color and green color cone represents the data integrity rate of SADS-Cloud [1] and existing efficient and publicly verifiable approach [2]. Consequently, the experimental result shows that the proposed TVPOUC-TLA Method attained better data integrity rate results than all other existing techniques. This is due to the application of Okamoto–Uchiyama Cryptography process where soriginal patient data develops encrypted and changed into ciphertext. The ciphertext is transmitted to the cloud server for safe communication. As a result, the data integrity rate of the TVPOUC-TLA Method improves. The data integrity rate of the TVPOUC-TLA Method has been increased by 11% and 19% when compared to existing methods, according to an average of ten evaluation findings [1] [2].

5.3 Authentication Accuracy

Authentication accuracy (AA) is defined as the fraction of cloud users who are accurately identified as authorized or unauthorized users in the cloud. Authentication accuracy is formulated as,

$$AA = \left(\frac{Number\ of\ cloud\ users\ that\ are\ correctly\ authenticated}{Number\ of\ cloud\ users}\right) * 100 \quad (9)$$

From (9), the authentication accuracy is calculated. As a result, authentication accuracy is expressed as a percentage (%).

Table 3: Authentication Accuracy Tabulation

Number of cloud users	Authentication Accuracy (%)		
	Proposed TVPOUC-TLA Method	Existing SADS-Cloud	ExistingEfficient and Publicly Verifiable approach
50	92	80	78
100	94	83	80
150	92	81	77
200	95	84	79
250	93	82	76
300	90	80	74
350	88	77	71
400	85	75	69
450	89	78	72
500	92	81	75

Table 3 compares the authentication accuracy of the proposed TVPOUC-TLA Method to that of the existing SADS-Cloud [1] and the existing efficient and publicly verifiable technique [2]. The authentication accuracy of the proposed and existing methods are computed depending the number of financial data ranging from 100 to 1000. The proposed TVPOUC-TLA Method achieved a higher data integrity rate, as demonstrated by experimental findings. When number of financial data is 200, the authentication accuracy of TVPOUC-TLA Method is 95% and the authentication accuracy of existing SADS-Cloud [1] and efficient and publicly verifiable approach [2] is 84% and 79% respectively. Similarly, authentication accuracy is attained for every method.

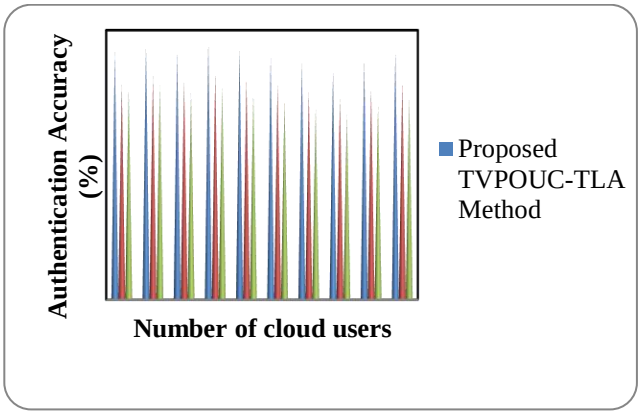

Fig 8 Measurement of Authentication Accuracy

Figure 8 explains the experimental analysis on authentication accuracy using three different security mechanisms namely proposed TVPOUC-TLA Method, existing SADS-Cloud [1] and existing efficient and publicly verifiable approach [2]. The blue color cone reflects the proposed TVPOUC-TLA Method's authentication accuracy, whereas the brown and green color cones indicate the authentication accuracy of SADS-Cloud [1] and the existing efficient and publicly verifiable technique [2]. Consequently, the experimental result shows that the proposed TVPOUC-TLA Method improved authentication accuracy results than other existing techniques. This is because of using Okamoto–Uchiyama Cryptography process. The original financial data gets encrypted to form cipher text. Then, ciphertext is sent to the cloud server for performing secured transmissionFinally, the suggested TVPOUC-TLA Method employs bivariate correlation to determine whether a cloud user is authenticated or not. As a result, the TVPOUC-TLA Method's authentication accuracy improves. The average of the data shows that the TVPOUC-TLA Method improves authentication accuracy by 14% and 21% when compared to the existing SADS-Cloud [1] and efficient and publicly verifiable approach [2].

6. Conclusion

A unique TVPOUC-TLA Method is intended to increase the security of financial data transfer in a cloud setting. The registration process was carried out through the TVPOUC-TLA Method. Then, cloud server produces the key pair for enumerated user. When cloud user needs to perform any financial transaction, cloud user gets logged in and send request message to the CS. Then, CS proves the cloud manipulator authenticity through sending the time variant password and fingerprint. If the cloud manipulator entered password and fingerprint acquires matched with CS sent password, user is an authorized user and perform financial transaction. Otherwise, the transaction will be rejected. Using the TVPOUC-TLA Method, an efficient secured financial transaction is carried out with greater data confidentiality and integrity. Finally, when compared to current works, the suggested TVPOUC-TLA Method is evaluated using clouds to assess the combination of verification accuracy, data confidentiality rate, and data integrity rate.

References

[1] Uma Narayanan, Varghese Paul, Shelbi Joseph, "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment", Journal of King Saud University – Computer and Information Sciences, Elsevier, 2020, Pages 1-20

[2] ShejiNishoni and A. Aldo Tenis, "Secure Communication with Data Analysis and Auditing Using Bilinear Key Aggregate Cryptosystem in Cloud Computing", Materials Today: Proceedings, Elsevier, Volume 24, Part 4, 2020, Pages 2358-2365

[3] NabeilEltayieb, Rashad Elhabob, Alzubair Hassan and Fagen Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud", Journal of Systems Architecture, Elsevier, Volume 102, January 2020, Pages 1-28

[4] Xiaodong Yang, Ting Li, Wanting Xi, Aijia Chen, Caifen Wang, "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud", IEEE Access, Volume 8, 2020, Pages 170713 – 170731

[5] DorababuSudarsa, Nagaraja Rao A and Sivakumar A.P., "An effective and secured authentication and sharing of data with dynamic groups in cloud", Data & Knowledge Engineering, Elsevier, Volume 145, May 2023, Pages 1-15

[6] GayathriNagasubramanian, Rakesh kumarSakthivel and Fadi Al-Turjman, "Secure and Consistent Job Administration Using Encrypted Data Access Policies in Cloud Systems", Computers & Electrical Engineering, Elsevier, Volume 96, Part A, December 2021, Pages 1-15

[7] Qin Liu, ZhengzhengHao, Yu Peng, Hongbo Jiang, Jie Wu, Tao Peng, Guojun Wang and Shaobo Zhang, "SecVKQ: Secure and verifiable kNN queries in sensor–cloud systems", Journal of Systems Architecture, Elsevier, Volume 120, November 2021, Pages 1-14

[8] VikasChouhan, Sateesh K. Peddoju and RajkumarBuyya, "dualDup: A secure and reliable cloud storage framework to deduplicate the encrypted data and key", Journal of Information Security and Applications, Elsevier, Volume 69, September 2022, Pages 1-15

[9] Shaopeng Guan, Conghui Zhang, Yilin Wang and Wenqing Liu, "Hadoop-based secure storage solution for big data in cloud computing environment", Digital Communications and Networks, Elsevier, January 2023, Pages 1-15

[10] Anichur Rahman, Md Jahidul Islam, Shahab S. Band, Ghulam Muhammad, Kamrul Hasan and Prayag Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT", Digital Communications and Networks, Elsevier, November 2022, Pages 1-18

[11] SuyelNamasudra, Debashree Devi, SeifedineKadry, RevathiSundarasekar, A. Shanthini, "Towards DNA based data security in the cloud computing environment", Computer Communications, Volume 151, 1 February 2020, Pages 539-547

[12] Divyansh Agrawal and SachinMinocha, "Securing confidential data in the cloud environment by using DNA computing", Advances in Computers, Elsevier, December 2022, Pages 1-15

[13] Xufeng Jiang, Lu Li and Ge Gao, "Efficient secure and verifiable KNN set similarity search over outsourced clouds", High-Confidence Computing, Elsevier, December 2022, Pages 1-15

[14] Hui Xie, Zhengyuan Zhang, Qi Zhang, Shengjun Wei and Changzhen Hu, "HBRSS: Providing high-secure data communication and manipulation in insecure cloud environments", Computer Communications, Elsevier, Volume 174, 1 June 2021, Pages 1-12

[15] YutingZuo, Zhaozhe Kang, Jian Xu and Zhide Chen, "BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing", International Journal of Distributed Sensor Networks, 2021, Pages 1-16

[16] K. S. Saraswathy and S. S. Sujatha, "Secure data storage and access for fish monitoring in cloud environment", Measurement: Sensors, Elsevier, February 2023, Pages 1-17

[17] PengCheng Wei, Dahu Wang, Yu Zhao, Sumarga Kumar SahTyagi, Neeraj Kumar, "Blockchain data-based cloud data integrity protection mechanism", Future Generation Computer Systems, Elsevier, Volume 102, 2020, Pages 902-911

[18] S. Rajasoundaran, A.V. Prabu, SidheswarRoutray, S.V.N. Santhosh Kumar, Prince PriyaMalla, SumanMaloji, Amrit Mukherjee and Uttam Ghosh, "Machine learning based deep job exploration and secure transactions in virtual private cloud systems",Computers & Security, Elsevier, Volume 109, October 2021, Pages 1-15

[19] NureniAyofeAzeez and Charles Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis", Egyptian Informatics Journal, Elsevier, Volume 20, Issue 2, July 2019, Pages 97-108

[20] AntoViji A, J. Jasper and T. Latha, “Efficient Secure Aware Scheduling Model for Enhancing Security and Workflow Model in Cloud Computing”,Optik, Elsevier, December 2022, Pages 1-12