The Scientific Temper (2024) Vol. 15 (1): 1826-1831
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2024.15.1.34
https://scientifictemper.com/

RESEARCH ARTICLE

Session password Blum–Goldwasser cryptography based user three layer authentication for secured financial transaction

N. Ruba*, A. S. A. Khadir

Abstract

Cloud computing is an eminent and evolving technology that offers various services such as data transaction, authentication, distribution and so on. In this article, session password Blum–Goldwasser Cryptography based user authentication (SPBGCUA) method is proposed to enhance the communication security of cloud services with minimum overhead. Moreover, SPBGCUA is a cryptographic technique that provides secured authentication mechanism for financial transaction with higher confidentiality rate. In order to fill the security lack of recent authentication techniques, this method develops dynamic security structure with key generation, encryption, authentication and decryption techniques. Finally, analysis is performed using SPBGCUA Method on factors such as authentication accuracy, data confidentiality rate and data integrity for number of financial data and cloud users.

Keywords: Cloud computing, Blum–Goldwasser Cryptography, Session Password, Secured.

Introduction

Cloud computing is used in scalable applications at anytime and anywhere. Security is an important one for data preservation in cloud environment. Many authentication techniques were introduced to validate the identity of users on cloud. Certificateless group-oriented signcryption technique with fractional chaotic maps (FCM) termed CGST-FCM technique was introduced by Chandrashekar, Agbotiname, Sajjad, Adel, Sarita and Iqtadar (2002) with provably secure manner. But, data confidentiality rate was not minimized by CGST-FCM technique. A three-factor certificateless-signcryption-based user access control (CSUAC-IoT) was designed by Shobhan, Basudeb, Anil, Ashok,Kim-Kwang and Youngho (2020) for efficient user authentication.

Department of Computer Science, Khadir Mohideen College, Adirampattinam, Thanjavur Affiliated to Bharathidasan University, Tamilnadu, India

***Corresponding Author:** N. Ruba, Department of Computer Science, Khadir Mohideen College, Adirampattinam, Thanjavur Affiliated to Bharathidasan University, Tamilnadu, India, E-Mail: rubaanand17@gmail.com

How to cite this article: Ruba, N., Khadir, A. S. A. (2024). Session password Blum–Goldwasser cryptography based user three layer authentication for secured financial transaction. The Scientific Temper, **15**(1):1826-1831.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.1.34

Source of support: Nil

Conflict of interest: None.

Lightweight IoT information sharing security framework was introduced by Haiping, Changxia, Yanling, Hongboand and Lei (2019) to improve information sharing. But, the designed framework not addressed privacy issues. Secure transmission was carried out by Ding and Hongbo (2019) with IoT devices. But, the designed algorithm not improved. A distributed key management system was introduced by Sarada, Chhagan, Lokesh, Sharma, Deepak, Jose and Utku (2019) for data transmission. But, the authentication accuracy was not improved by SADS-Cloud.

RBE scheme was designed by Muhamman, Mian and Xiangjian (2017) in cloud environment. The designed scheme support real-time processing with power-saving limitations. But, the data confidentiality was not improved and the computational complexity was not minimized. The lightweight authentication protocol was introduced by Arezou, Hamed, Mortezaand and Dariush (2019) for increasing the security.

The problems are lesser data confidentiality rate, lesser data integrity rate, lesser authentication accuracy, higher computational cost, higher complexity, higher time complexity and so on. In order to address the above mentioned issues, Session Password Blum–Goldwasser Cryptography based User Authentication (SPBGCUA) Method is introduced.

Research Contribution

The main contribution of the research is given as:

- The SPBGCUA Method is specifically crafted for facilitating efficient financial transactions in the

Received: 09/01/2024 **Accepted:** 12/02/2024 **Published** : 15/03/2024

context of IoT, with a primary focus on enhancing data confidentiality. The method involves a straightforward process:

- User Registration: Cloud users initiate the process by registering their details with the server for authentication purposes.
- Key Generation: The Cloud Server (CS) responds by generating a unique pair of cryptographic keys, namely a public key and a secret key, dedicated to the registered cloud user.
- Financial Transaction Initiation: In the event that a cloud user needs to execute a financial transaction, they log in using the generated key pair and submit a request message to the Cloud Server (CS).
- User Authentication: The Cloud Server (CS) conducts user authentication by transmitting a session password to verify the legitimacy of the cloud user.
- Secure Financial Transaction: With user authenticity confirmed, the SPBGCUA Method ensures that financial transactions are executed efficiently and securely, thereby contributing to an elevated level of data confidentiality.

In summary, the SPBGCUA Method not only streamlines the registration and authentication process for cloud users but also employs cryptographic keys and session passwords to ensure the security and confidentiality of financial transactions within an IoT-based environment.

Related Works

The secure framework was introduced by Mohammad and Norah (2020) where task initiates with patient authentication. An improved partial homomorphic encryption algorithm was introduced by Hui, Zhengyuan, Qi, Shengjunand and Changzhen (2021) for fuzzy processing to enhance the function-privacy. However, the authentication accuracy was not improved. A cryptographic method was introduced by Fursan, Sharaf and Sudhir (2021) to improve cloud computing security. SEDAP was designed by Gayathri, Rakesh and Fadi (2021) for cloud access.

In the papers, Qin, Zhengzheng, Yu, Hongbo, Jie, Tao, Guojun and Shaobo (2021), they have proposed a screening phase and search phase. DupLESS scheme was designed by Vikas, Sateesh and and Rajkumar, (2022) to store data in remote storage environment.

A novel Identity based signcryption mechanism was used to designed mechanism, computational time was reduced and the designed mechanism was secured against chosen cipher attacks. But, the complexity level was not minimized by designed mechanism. A new data sharing method was introduced by Manoj, Harshand and Geeta (2020) to improve the data safety using CLSC scheme. Diffie-Hellman inversion (DHI) was employed to increase the authenticity and confidentially with minimal overhead. A secure data protection method was introduced by Amr, Passent, Amr, Mohamed and Ismail (2021) to attain better solution.

An Enhanced AES-256 cipher round algorithm was developed by Santhanalakshmi, Lakshana and Shahitya (2023) for IoT applications. A Quantum key distribution-based techniques in IoT was presented by Neeraj and Singhrova (2023) to provide authentication accuracy. However, the authentication accuracy was not improved.

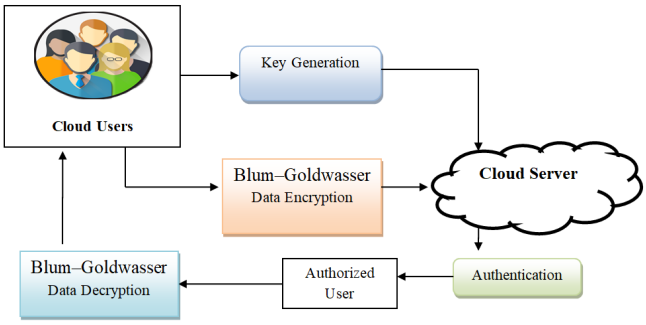

Figure 1: Structural diagram of Proposed TVPOUC-TLA method

Methodology

User authentication validates the user identity when user logs into computer system. It is essential to identify different attacks posed by attackers to ensure secure and trustworthy environment. However, financial data collected from IoT devices transmitted securely for reducing the cost. In order to address these problems, Session Password Blum–Goldwasser Cryptography based User Authentication (SPBGCUA) Method is introduced. SPBGCUA Method is to perform efficient secured data transmission in cloud environment. The architecture diagram of SPBGCUA Method is illustrated in Figure 1.

Figure 1 explains the proposed SPBGCUA method diagram for secured data transaction.

Key Generation

Key generation is the first process in SPBGCUA Method. In SPBGCUA Method, client registers information to the cloud server. The cloud server generates the key pair 'P_{key}' and secret key 'S_{key}'. The number of users in cloud is represented as '$CU_i = CU_1, CU_2, \ldots CU_N$'.

Blum–Goldwasser Data Encryption

Transaction security protects the client data against unlawful access. The cryptographic techniques are used to encrypt the data before performing transaction. However, the cloud data transaction security was not adequate as user secret key is stolen. In SPBGCUA Method through integrating the session password in existing Blum–Goldwasser cryptosystem shown in Figure 2.

The designed algorithm considered number of cloud user data as input. After that, Blum–Goldwasser Data Encryption algorithms generate the random bits for cloud user data.

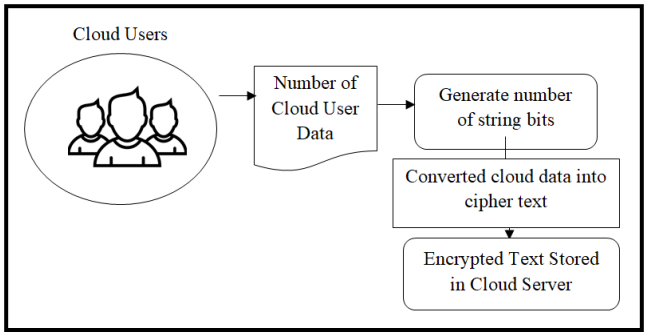

Figure 2: Process of Blum–Goldwasser data encryption

The cloud user data are XORed to convert into ciphertext. The ciphertext is transmitted to cloud server with minimal time consumption. SPBGCUA Method consumed lesser computational time for secured data transaction. The number of cloud user data as '$cd_i = cd_1, cd_2, \ldots cd_n$'. SPBGCUA Method encodes the cloud user data stored into number of strings of 'm' bits. It is formulated as,

$$cd_i = (cd_0, cd_1, \ldots, cd_{k-1}) \quad (1)$$

Consequently, SPBGCUA Method chooses the random number 'r' i.e. '$1 < r < N$' and computed as,

$$\gamma_0 = r^2 mod P_{key} \quad (2)$$

Next, the SPBGCUA Method uses the Blum Blum Shub (BBS) pseudo-random number generator to create random bits '$\overrightarrow{rb_i} = rb_0, rb_1, .. rb_{m-1}$'. For every random bit 'i' to 'm', then SPBGCUA Method allocates 'rb_i' equal to least significant bit of 'γ_i'. It is given as,

$$\gamma_i = (\gamma_{i-1})^2 mod P_{key} \quad (3)$$

$$\overrightarrow{rb_i} = LSB(\gamma_i) \quad (4)$$

From (3) and (4), '$LSB(\gamma_i)$' symbolizes the least significant bit of 'γ_i'. SPBGCUA Method creates the cipher text bits with 'rb_i' from the BBS. The cloud data are XORed with random bits to construct the cipher text. It is devised as,

$$c_i = \overrightarrow{cd} \oplus \overrightarrow{rb} \quad (5)$$

From (5),'c_i' symbolizes the cipher text. Algorithm 1 describes the Blum–Goldwasser Data Encryption Algorithm.

Algorithm 1 explains the algorithmic process of Blum–Goldwasser Data Encryption. SPBGCUA Method generates the ciphertext for each cloud user data and transmitted to cloud server database to improve security level.

Blum–Goldwasser Data Decryption

SPBGCUA Method authenticates the secret key and generates the session password to validate the cloud user identity. The generated password is valid for particular session. Accordingly, SPBGCUA Method provides additional security layer to guarantee the cloud user identity and to minimize the illegal access risk on cloud data transaction. SPBGCUA Method combined the secret key with present timestamp through cryptographic hash function and transmitted to the equivalent cloud user through mobile number. When cloud user entered and generated password

```
// Blum–Goldwasser Data Encryption Algorithm
Input: Cloud User 'CU_i = CU_1, CU_2, ... CU_N';Cloud Data '
cd_i = cd_1, cd_2, ... cd_n'
Output: Increased cloud data security
1: Begin
2:    For each 'CU_i'
3:       For each 'cd_i'
4:          Generate 'm' number of string bits
5:          Select 'r' and create 'rb' with cloud user 'P_key'
6: Obtainciphertext 'c_i'
7:       End for
8:    End For
9: End
```

Algorithm 1: Blum–Goldwasser data encryption

is matched, the cloud user is authentic and data gets decrypted. For every cloud user request, Blum–Goldwasser Data Decryption verifies the secret key. It is given as,

$$AR = \{If(S_{key} == S^*_{key}) session password is generated else session password is not generated \quad (6)$$

From (6), 'AR' obtains the secret key authentication result.'S_{key}' symbolizes the client entered secret key at login time period and 'S^*_{key}' denotes the secret key of cloud user stored in database. When 'S_{key}' and 'S^*_{key}' is equal, BGDD generates session password. The SPBGCUA Method uses session password and given as,

$$SP = OTP(S_{key}, time)) \quad (7)$$

From (7), 'OTP' is generated for every time step through HMAC-based One-time Password algorithm. When cloud user is authentic, SPBGCUA Method performed the Blum–Goldwasser data decryption process. The cloud user obtain the original data with secret key 'S_{key}'. By this manner, the data decryption is carried out and formulated as,

$$cd_i = c_i \oplus rb_i \quad (8)$$

From (8), original cloud user data 'cd' is re-generated. As a result, SPBGCUA Method enhanced the data security level with minimal computational cost.

Experimental Setup

The proposed SPBGCUA Method, along with the existing CGST-FCM technique (Chandrashekar, Agbotiname, Sajjad, Adel, Sarita and Iqtadar, 2002) and Certificateless-Signcryption-Based User Access Control for the IoT environment (CSUAC-IoT) (Shobhan, Basudeb, Anil, Ashok,Kim-Kwang and Youngho, 2020), has been implemented in the Java programming language. For experimentation and validation, a finance dataset sourced from Kaggle (https://www.kaggle.com/) has been utilized. This finance dataset comprises 10,000 rows and 5 columns. The default column indicates whether an individual is a defaulter or not, with 'yes' and 'no' values in the respective column.

Result And Analysis

The proposed SPBGCUA Method and existing CGST-FCM technique (Chandrashekar, Agbotiname, Sajjad, Adel, Sarita

and Iqtadar, 2002) and CSUAC-IoT (Shobhan, Basudeb, Anil, Ashok,Kim-Kwang and Youngho, 2020) are discussed.

Data Confidentiality Rate

Data confidentiality rate is defined as the ratio of number of financial data protected from an access. The data confidentiality rate is calculated as,

$$DCR = \left[\frac{Numberoffinancialdataprotectedfromunauthorizedaccess}{Numberoffinancialdat77a}\right] * 100 \quad (9)$$

From (9), 'DCR' represent the data confidentiality rate and computed in terms of percentage (%).

Table 1 presents a comparative analysis of data confidentiality rates achieved by the proposed SPBGCUA Method, the existing CGST-FCM technique and the CSUAC-IoT. The determination of data confidentiality rates in these techniques is based on the volume of financial data. The results reveal that the SPBGCUA Method consistently outperforms the existing methods in terms of data confidentiality. For instance, when the number of financial data points is set at 600, the SPBGCUA Method achieves an impressive data confidentiality rate of 94%. In contrast, the existing CGST-FCM technique and CSUAC-IoT attain data confidentiality rates of 88% and 77%, respectively. These findings highlight the superior performance of the proposed SPBGCUA Method across various data quantities. This trend is observed consistently across different data volumes, further reinforcing the effectiveness of the SPBGCUA Method in ensuring higher levels of data confidentiality in comparison to the existing CGST-FCM technique and CSUAC-IoT.

Figure 3 depicts the performance of data confidentiality rates achieved by three distinct security mechanisms: the proposed SPBGCUA Method, the existing CGST-FCM technique, and the CSUAC-IoT. The representation employs blue, red, and green cylinders to signify the data confidentiality rates of the SPBGCUA Method, CGST-FCM technique and CSUAC-IoT respectively. The experimental results clearly demonstrate that the proposed SPBGCUA Method consistently outperforms the other existing

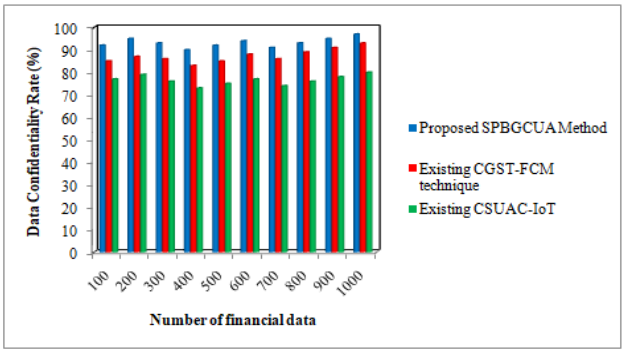

Figure 3: Measurement of Data Confidentiality Rate

techniques in terms of data confidentiality rates. This improvement can be attributed to the incorporation of the Session Password Blum–Goldwasser cryptographic process in the SPBGCUA Method. Notably, the Cloud Server (CS) verifies the authenticity of cloud users through session passwords, contributing to the heightened data confidentiality rates observed in the SPBGCUA Method. Specifically, the data confidentiality rate achieved by the SPBGCUA Method is 7% and 22% higher than that of the existing CGST-FCM technique and CSUAC-IoT respectively. These findings underscore the effectiveness of the SPBGCUA Method in enhancing data confidentiality, establishing it as a robust choice for secure financial transactions in comparison to the existing security mechanisms.

Data Integrity Rate

Data integrity rate is number of financial data not changed through illegal users. The data integrity rate is given as,

$$DIR = \left[\frac{Numberoffinancialdatanotmodifiedbyunauthorizedusers}{Numberoffinancialdata}\right] * 100 \quad (10)$$

From (10), 'DIR' symbolizes the data integrity rate and calculated in terms of percentage (%).

Table 2 provides a comprehensive comparison of data integrity rates among the proposed SPBGCUA Method, the existing CGST-FCM technique and the CSUAC-IoT. The

Table 1: Tabulation of data confidentiality rate

Number of financial data	Data Confidentiality Rate (%)		
	Proposed SPBGCUA Method	Existing CGST-FCM technique	Existing CSUAC-IoT
100	92	85	77
200	95	87	79
300	93	86	76
400	90	83	73
500	92	85	75
600	94	88	77
700	91	86	74
800	93	89	76
900	95	91	78
1000	97	93	80

Table 2: Tabulation of data integrity rate

Number of financial data	Data Integrity Rate (%)		
	Proposed SPBGCUA Method	Existing CGST-FCM technique	Existing CSUAC-IoT
100	97	81	78
200	94	79	75
300	93	77	72
400	95	79	74
500	96	81	76
600	98	83	78
700	95	80	75
800	93	78	73
900	90	77	71
1000	92	80	74

assessment of data integrity rates is conducted across a range of financial data volumes, spanning from 100 to 1000 entries. The results consistently demonstrate the superior data integrity rates achieved by the proposed SPBGCUA Method. For instance, when the number of financial data points is set at 700, the SPBGCUA Method exhibits an impressive data integrity rate of 95%. In contrast, the existing CGST-FCM technique and CSUAC-IoT achieve data integrity rates of 80% and 75%, respectively, at the same data volume. These findings highlight the enhanced data integrity provided by the SPBGCUA Method compared to the existing techniques across various data quantities. The trend of superior data integrity rates is consistently observed across the entire range of financial data volumes, establishing the efficacy of the SPBGCUA Method in ensuring higher levels of data integrity compared to the existing CGST-FCM technique and CSUAC-IoT.

Figure 4 visually represents the data integrity rates achieved by three distinct security mechanisms: the proposed SPBGCUA Method, the existing CGST-FCM technique and the CSUAC-IoT. The depiction utilizes blue, red, and green cylinders to signify the data integrity rates of the SPBGCUA Method, CGST-FCM technique and CSUAC-IoT respectively. The experimental results clearly demonstrate that the proposed SPBGCUA Method consistently outperforms the other existing techniques in terms of data integrity rates. This improvement is attributed to the incorporation of the Session Password Blum–Goldwasser cryptographic process in the SPBGCUA Method.

Notably, the verification of cloud user authenticity using session passwords contributes to the observed heightened data integrity rates in the SPBGCUA Method. Specifically, the data integrity rate achieved by the SPBGCUA Method is 19% and 26% higher than that of the existing CGST-FCM technique and CSUAC-IoT respectively. These findings underscore the effectiveness of the SPBGCUA Method in enhancing data integrity, positioning it as a robust choice

Table 3: Tabulation of authentication accuracy

Number of cloud users	Authentication Accuracy (%)		
	Proposed SPBGCUA Method	Existing CGST-FCM technique	Existing CSUAC-IoT
50	95	82	75
100	93	80	73
150	91	78	71
200	89	76	69
250	87	73	67
300	85	71	65
350	83	70	64
400	81	68	66
450	84	70	68
500	86	72	70

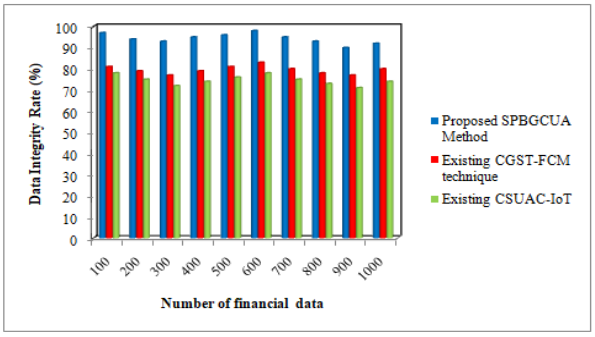

Figure 4: Measurement of data integrity rate

for secure financial transactions when compared to existing security mechanisms.

Authentication Accuracy

Authentication accuracy (AA) is number of cloud users that are correctly classified as authorized or unauthorized users. The authentication accuracy is given as,

$$AA = \left(\frac{Number\ of\ cloud\ users\ that\ are\ correctly\ authenticated.}{Number\ of\ cloud\ users}\right) * 100 \quad (11)$$

From (11), the authentication accuracy is calculated in terms of percentages (%).

Table 3 explains the authentication accuracy comparison of proposed SPBGCUA Method, existing CGST-FCM technique and existing CSUAC-IoT. The authentication accuracy of proposed and existing methods is determined based on the number of loud users ranging from 50 to 500. As shown in results, the proposed SPBGCUA Method attained higher authentication accuracy. When number of cloud users is 100, the authentication accuracy of SPBGCUA Method is 93% and the authentication accuracyof existing CGST-FCM technique and CSUAC-IoT is 80% and 73% respectively. Similarly, the authentication accuracy is attained for all three methods. Figure 5 illustrates the experimental analysis of authentication accuracy across three distinct security mechanisms: the proposed SPBGCUA Method, the existing CGST-FCM technique and the CSUAC-IoT. The representation employs blue, red, and green cylinders to signify the authentication accuracy of the SPBGCUA Method, CGST-FCM technique and CSUAC-IoT respectively.

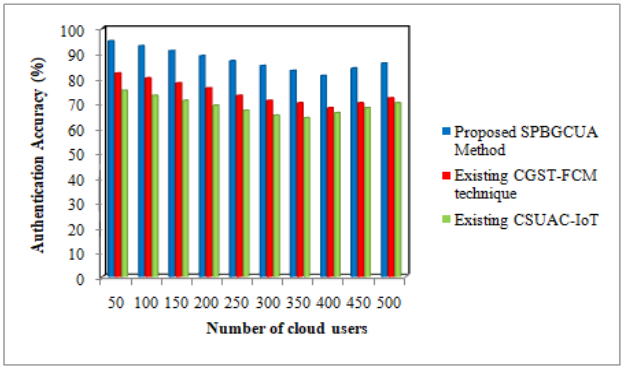

Figure 5: Measurement of authentication accuracy

The experimental results unequivocally demonstrate that the proposed SPBGCUA Method consistently outperforms the other existing techniques in terms of authentication accuracy. This improvement is attributed to the utilization of the Session Password Blum–Goldwasser cryptographic process.

In the SPBGCUA Method, cloud user authentication occurs through the login process using a cloud user ID and password. Successful authentication is achieved when the entered user ID and password match the stored credentials. Consequently, the authentication accuracy of the SPBGCUA Method is increased. On average, the results indicate that the authentication accuracy of the SPBGCUA Method is improved by 18% and 27% when compared to the existing CGST-FCM technique and CSUAC-IoT respectively. These findings underscore the efficacy of the SPBGCUA Method in enhancing authentication accuracy, positioning it as a robust choice for secure financial transactions when compared to existing security mechanisms.

Conclusion

A novel SPBGCUA Method is introduced for secured financial transaction with higher confidentiality rate. The cloud user registers their detail to cloud serverfor authentication. Cloud server (CS) generates the key in key generation process for registered cloud user. After user logged in with key pair, request message is sent to the CS for financial transaction. The CS verifies the cloud user authenticity through transmitting the session password. When cloud user entered password gets matched with the CS sent password, cloud user is an authorized user for performing financial transaction. By this way, efficient financial transaction is carried out with higher data confidentiality rate and data integrity rate. SPBGCUA Method increased authentication performance when compared to the existing works.

Acknowledgement

We would like to thank Khadir Mohideen College, Adirampattinam, which is affiliated to Bharathidasan University, Tamilnadu, for the helpful support of conducting research in an effective manner.

References

Amr, M.S, Passent, M.E., Amr, F.S., Mohamed, A.A,, Ismail, M.H(2021). A New Secure Model for Data Protection over Cloud Computing.*Computational Intelligence and Neuroscience. Hindawi Publishing Corporation*.1-14.

Arezou, O.S., Hamed, A., Morteza, N. and Dariush, A.M. (2019). Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Generation Computer Systems. Elsevier.***100:**882-892.

Chandrashekar, M., Agbotiname, L.I., Sajjad, S.J., Adel, R.A., Sarita, G.M. and Iqtadar, H. (2002). CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps. *IEEE Access*. 39853 – 39863.

Ding, X., Hongbo, Z. (2019). Secure Transmission for SWIPT IoT Systems With Full-Duplex IoT Devices. *IEEE Internet of Things Journal*. **6(6):**10915 – 10933.

Fursan, T., Sharaf, A. and Sudhir, J. (2021). A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. *International Journal of Intelligent Networks. Elsevier.* **2:**18-33.

Gayathri, N., Rakesh, K.S. and Fadi, A.T. (2021). Secure and Consistent Job Administration Using Encrypted Data Access Policies in Cloud Systems. *Computers & Electrical Engineering. Elsevier.***96:**1-15.

Haiping, S., Changxia, S., Yanling, L., Hongbo, Q. and Lei, S. (2019). IoT information sharing security mechanism based on blockchain technology. *Future Generation Computer Systems. Elsevier.***101:**1028–1040.

https://www.bing.com/search?q=financial+dataset&qs=n&form=QBRE&sp=-1&ghc=1&pq=financial+dataset&sc=1017&sk=&cvid=B1834DA3FB494AE583B4D8B24297E2BA&ghsh=0&ghacc=0&ghpl=

Hui, X.,, Zhengyuan, Z., Qi, Z., Shengjun, W. and Changzhen, H.(2021). HBRSS: Providing high-secure data communication and manipulation in insecure cloud environments. *Computer Communications. Elsevier.***174:**1-12.

Manoj, K., Harsh, K.V. and Geeta, S. (2020). A secure data transmission protocol for cloud-assisted edge-Internet of Things environment. *Transactions on Emerging Telecommunications Technologies. Wiley Online Library.***31(6):**1-15.

Mohammad, A.K., Mohammad, T.Q., Norah, S.A. and Mohammad, Y.K. (2020). A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data. *IEEE Access*.52018 – 52027.

Muhamman, U., Mian, A.J. and Xiangjian, H. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. *Information Sciences. Elsevier.***387:** 90-102.

Neeraj and Singhrova, A. (2023). Quantum key distribution-based techniques in IoT. *The Scientific Temper.* **14 (3)**: 1008-1013.

Qin, L., Zhengzheng, H., Yu, P., Hongbo, J., Jie, W., Tao, P., Guojun, W. and Shaobo, Z. (2021). SecVKQ: Secure and verifiable kNN queries in sensor–cloud systems. Journal of Systems Architecture. Elsevier. **120:**1-14.

Santhanalakshmi, M., Lakshana, K. and Shahitya, G.M. (2023). Enhanced AES-256 cipher round algorithm for IoT applications. *The Scientific Temper.* **14 (1)**: 184-190.

Sarada, P,G., Chhagan, L., Lokesh, S., Sharma, D.P, Deepak, G., Jose A.M.S. and Utku, K. (2019). Reliable and secure data transfer in IoT networks. *Wireless Networks. Springer.* 1-14.

Shobhan, M., Basudeb, B., Anil, K.S., Ashok, K.D., Kim-Kwang, R.C. and Youngho, P. (2020). Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment. *IEEE Internet of Things*. **7(4)**.

Vikas, C., Sateesh, K.P. and Rajkumar, B. (2022). dualDup: A secure and reliable cloud storage framework to deduplicate the encrypted data and key. *Journal of Information Security and Applications. Elsevier.***69**: 1-15.