GMR
The Original

TIME SYNCHRONIZED GESTALT PATTERN MATCHING REGRESSIVE CRYPTOSYSTEM BASED USER AUTHENTICATION FOR SECURE COMMUNICATION IN CLOUD

Shakira P V[1], Laxmi Raja[2]

[1]Research Scholar Department of CSE Faculty of Engineering Karpagam Academy of Higher Education Coimbatore – 641021. Shaky.cet@gmail.com
[2]Assistant Professor Department of Cyber Security Faculty of Engineering Karpagam Academy of Higher Education Coimbatore – 641021. laxmirajaphd@gmail.com

ABSTRACT
Cloud computing(CC) is a novel technology to distribute and access the services to the users through the internet. One essential and automatic point when cloud is utilize the presence of better authentication approach. User authentication is process of verifying the user's identity while establishing secure communications to cloud servers. In this paper, a novel technique called Time Synchronized Gestalt Pattern Matching Regressive Cryptosystem based User Authentication (TSGPMRC-UA) method is to improve cloud security level with better data confidentiality rate. TSGPMRC-UA Method comprise three processes, time synchronized confidential key generation, encryption, and decryption. In TSGPMRC-UA Method, cloud user registers his/her detail to CS for performing user authentication. After registration, CS generates public key as well as private key in key generation step for each registered cloud user with help of Boneh–Goh–Nissim Cryptosystem. Subsequent to receiving request, server confirm user's authenticity by sending dynamic session password and Deming regressive gestalt pattern matching. Then, data acquire decrypted through private key of cloud user. In his manner, cloud user data gets conserved from unauthorized access for enhancing data confidentiality as well as data integrity. Performance analysis is performed on authentication accuracy, authentication time, confidentiality rate, and data integrity with number of data.

KEYWORDS: Cloud, user authentication, Cloud server,Boneh–Goh–Nissim Cryptosystem, Deming regressive gestalt pattern matching, Cryptographic algorithms

1. INTRODUCTION

CC creates efficient computing as well as storage resources available to every servers and users via Internet. Cloud server consists of additional resources as well as more influential computation facility. Cloud server provides improved QoS for remote users to store, manage, and process data. Through data sharing between user and cloud server, security is important disquiet to defend cloud environment, data and so on against unauthorized access. User authentication is procedure of confirming user's identity. Numerous researchers performed their research on user authentication in cloud environment.

Privacy Attribute-based Credentials (Privacy-ABCs) based support pseudonym authentication technique was developed [1] for achieving fine-grained access control by detecting the authorized users' identity. But the time-based attribute handling was not performed for improving the authentication. For enhancing security , Secure Authentication and Data Sharing in Cloud (SADS-Cloud) was developed [2] with big data. However it failed to test with some other encryption algorithms to more expedite encryption as well as decryption operations.

For guarantying security against various attacks , novel authentication scheme was designed in [3]. But designed scheme was not more secure and efficient. An ECC-based approach was introduced in [4] for performing the authentication between users' devices and cloud servers. However, the user authentication time consumption was not minimized. A privacy-preserving cloud auditing method was introduced in [5] for numerous users with authorization to improve the security of shared data. However performance of data confidentiality was not enhanced.

Lightweight authentication protocol was designed [6] for IoT-enabled cloud computing environments to perform formal security analysis. However, the performance of security was not improved. A robust and privacy-preserving

authentication method was introduced in [7] for end-users to securely access the services distantly without losing performance. But the performance of the time consumption of user authentication was not reduced.

For user authentication against various attacks, elliptic curve cryptography (ECC) method was developed in [8] .however computation time was not decreased. ECC technique was developed [9] for a secure user authentication cloud. However technique was not effective to improve data confidentiality rate. ECC based enhanced secure mutual authentication method was introduced in [10] with lesser computational, and storage overhead.

1.1 Objective of this manuscript

Main objective of TSGPMRC-UA technique is include as below

- To improve security of data access control, a novel TSGPMRC-UA Method is introduced.
- To enhance authentication accuracy as well as reduce time, Deming regressive gestalt pattern matching is designed in TSGPMRC-UA method to recognize the authorized or unauthorized user. Authorized cloud user access data from server outcoming it enhance authentication accuracy.
- To enhance data confidentiality rate and integrity level, TSGPMRC-UA Method uses the Boneh–Goh–Nissim Cryptosystem which guarantees data security between cloud server as well as user through time synchronized session key generation, data encryption and decryption.
- Finally, the widespread experiments are performed to estimate performance of our TSGPMRC-UA Method and literature review. Experimental outcome demonstrates which TSGPMRC-UA Method is tested through various performance parameters.

Manuscript is structured as below . Section 2 provides literature survey in field of user authentication in cloud. In Section 3, a TSGPMRC-UA Methodis described with a different process. In Sections 4, experimental setup, dataset description as well as execution procedures are designed. Section 5 gives explanation of metrics and comparative study of different techniques are presented. Finally, manuscript is summarized in section 6.

2. LITERATURE SURVEY

For peer-to-peer Communication based on elliptic curve certificate-free cryptography ,A mutual authentication as well as key agreement technique was designed in [11]. But failed to explore as well as design protocol which permits numerous users to distribute data across dissimilar cloud servers, for enhancing effectiveness of data sharing between many users. An improved authentication technique was developed in [12] for accessing the data and distribution over cloud storage. But authentication accuracy was not improved.

Secure authentication protocol was designed in [13] for hierarchical attribute support configuration to considerably improve security. But the efficient authentication in cloud big data was a major challenging issue. For providing privacy requirements of cloud users , lightweight anonymous authentication technique was developed in [14]. But, performance of data integrity level was not enhanced.

Improved authentication as well as key agreement approach were designed [15] for IoT-based secure cloud data communication. However, the computational cost of the approach was slightly higher. A novel anonymous authentication approach was designed in [16] for sharing the information and efficiently authenticating service providers before accessing the data. But it was not efficient to perform batch authentication.

A new model was developed in [17] to provide authentication and data integrity during the data distribution. But the method failed to work in a complex environment to test scalability of scheme. A three-level security with a secure email-based OTP system was designed in [18] to enhance authentication. But failed to improve performance of authentication accuracy level.

Two-factor secure authentication method was designed in [19] against the different types of attacks. Though the method consumed less time to provide better security but a better confidentiality rate was not achieved. A novel lightweight multi-factor authentication and authorization approach was designed in [20] for real-time data access. But it failed to design promising security solutions.

3. PROPOSED METHODOLOGY

Cloud computing is a novel technology since it provides thousands of services at a laminated cost and it uses at anytime from anywhere only a network connection is required. In CC architecture, collections of different computing units are internationally divided. Due to this, the number of cloud users has sufficiently increased. To avoid unlawful access of intruders, strong user authentication method is needed for CC environment for computationally efficient communication of sensitive information. In this manuscript, new TSGPMRC-UA Method is designed for security of data access in CC by cryptographic method.

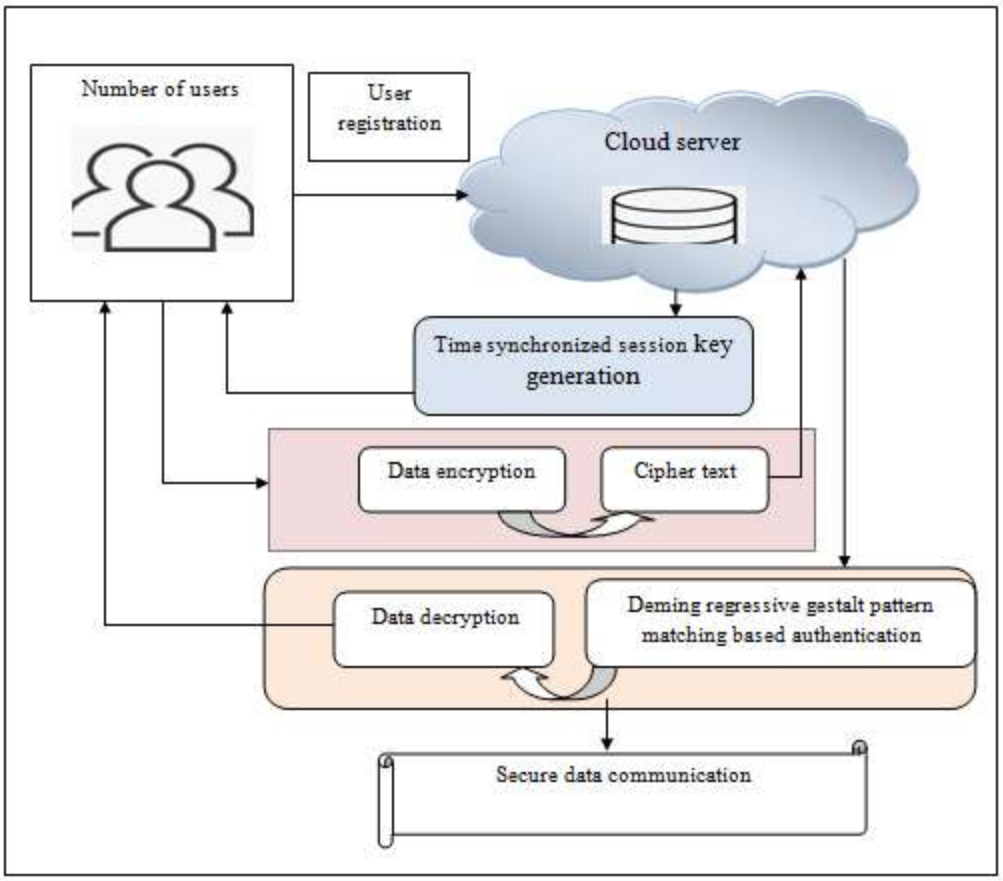

Figure 1 workflow diagram of the proposed TSGPMRC-UA Method

Figure 1 given above depicts procedure involved in TSGPMRC-UA technique to guarantee security in process of data storage as well as access control in the cloud environment. Cloud architecture design contains dissimilar entities contributing for protected data transmission. Architecture consists of cloud user's $U_1, U_2, U_3, \ldots . U_n$who generates the data $D_1, D_2, \ldots D_m$to store and access from cloud server (CS).

Proposed architecture diagram includes different processes namely user registration as well as key generation, encryption, authentication, decryption. Initial, users register their particulars to server for later login. After that, the cloud server performs Time synchronized session key generation using Boneh–Goh–Nissim Cryptosystem. Followed by, encryption process is performed to change the sensitive information or user data into an unreadable form. Deming regressive gestalt pattern matching-based authentication is performed to distinguish the authorized or unauthorized cloud users. Finally, the server provides data access for authorized users which enhances the secure data communication between the user and the cloud server.

3.1 Registration and key generation

In this phase, user registers with cloud server and shares secret keys for later login, encryption and decryption. First, user sends the registration request to CSwith their terminal (Desktop or Laptop) and his basic information such as name, mail ID and password in a secure channel. Once CS receives the request, shares the time synchronized session keys for each registered user.Time synchronization is the process of coordinating the time. It means that the key is generated for each session. After the session is expired, new key is generated to avoid the unauthorized access and also improves the confidentiality level.

The secret keys are generated by the cloud server using Boneh–Goh–Nissim Cryptosystem. It is public-key cryptography which uses the pairs of related keys. Each key pair comprises of a public key and an equivalent private key. Security of proposed public-key cryptography based on keeping private key secret as well as public key clearly distributed. Key size of authenticity is public key as well as private key in key generation using minimum 1kb as well as maximum 2.048 kb.

The proposed algorithm is a fundamental security cryptosystems, including an application which provides an assurance of the confidentiality and authenticity of data communications.

Let us consider the two large numbers N_1 and N_2. Therefore, the multiplication of these two large prime numbers is used for public key generation.

$$P = N_1 * N_2 \quad (1)$$

Then the parameter 'H' is computed as given below,

$$H = b.N_2 \quad (2)$$

Where, b denotes a generator of the Prime cyclic group 'K', K denotes a group of order 'P'.

With the above said parameters, the public key of registered user is generated as follows,

$$Pk_p = [P, K, b, H] \quad (3)$$

Where, k_p denotes a public key of the user generated based on the multiplication of two large prime numbers 'P', 'K 'group of order 'P', b indicates a generator of the group 'K', H denotes a parameter obtained by using (2).

Followed by, private key of the user is computed as given below,

$$Sk_b = N_1 \quad (4)$$

Where, Sk_b indicates a private key of the user, N_1 denotes a prim number.

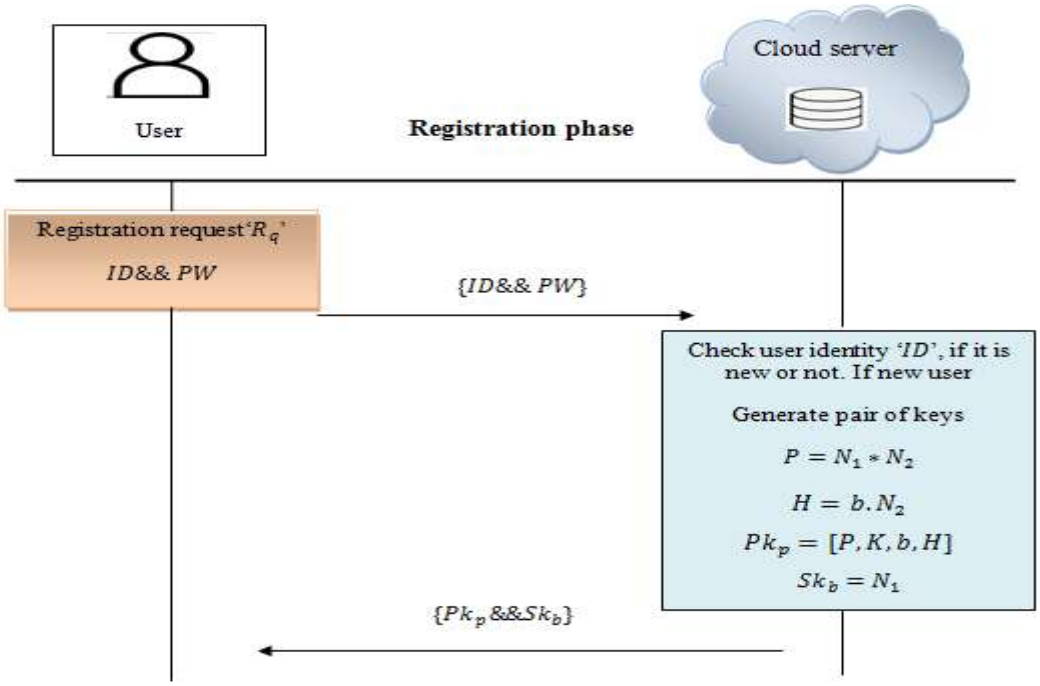

Figure 2 registration and key generation

Figure 2 demonstrates flow process of registration as well as key pair generation. This procedure is carried out between user and cloud server. Initial, user registers their particulars and ID&& PW to CS. Server verifies whether the user ID is already exists or not. If it is exist, server replies user ID already available try again with new ID. Otherwise, the cloud server generates private as well as public key for every registered user. Upon distributing pair of keys, CS provides access to the user.

3.2 Encryption

In public key cryptography, encryption is procedure of converting original representation of the information, called as plaintext; into an unreadable form i.e. cipher text through assist of receiver public key.

Let us consider user's $U_1, U_2, U_3, \ldots . U_n$who generates the data $D_1, D_2, \ldots D_m$ to store a the CS. Encryption is process of converting original data to cipher text is follows,

$$C_x = [D * b] + [R * P] \quad (5)$$

Where, C_x denotes cipher text, D represents data, b indicates public key, R denotes random number$R \in [0,1,2 \ldots P - 1]$. Cipher text of input data is sent to CS for evading unauthorized access.

3.3 Deming regressive gestalt pattern matching based user authentication

In cloud, whenever CU requires to access encrypted data, they transmit request message to CS. Subsequent to receiving request, server confirms CU authenticity through sending dynamic session password. Proposed technique performs the user authentication with the help of the Deming regressive gestalt pattern matching. Regression is ML technique used to find relationship among the variables. The Deming regression tries to find the line of best fit (i.e. authorized user or unauthorized user) through the session password matching.

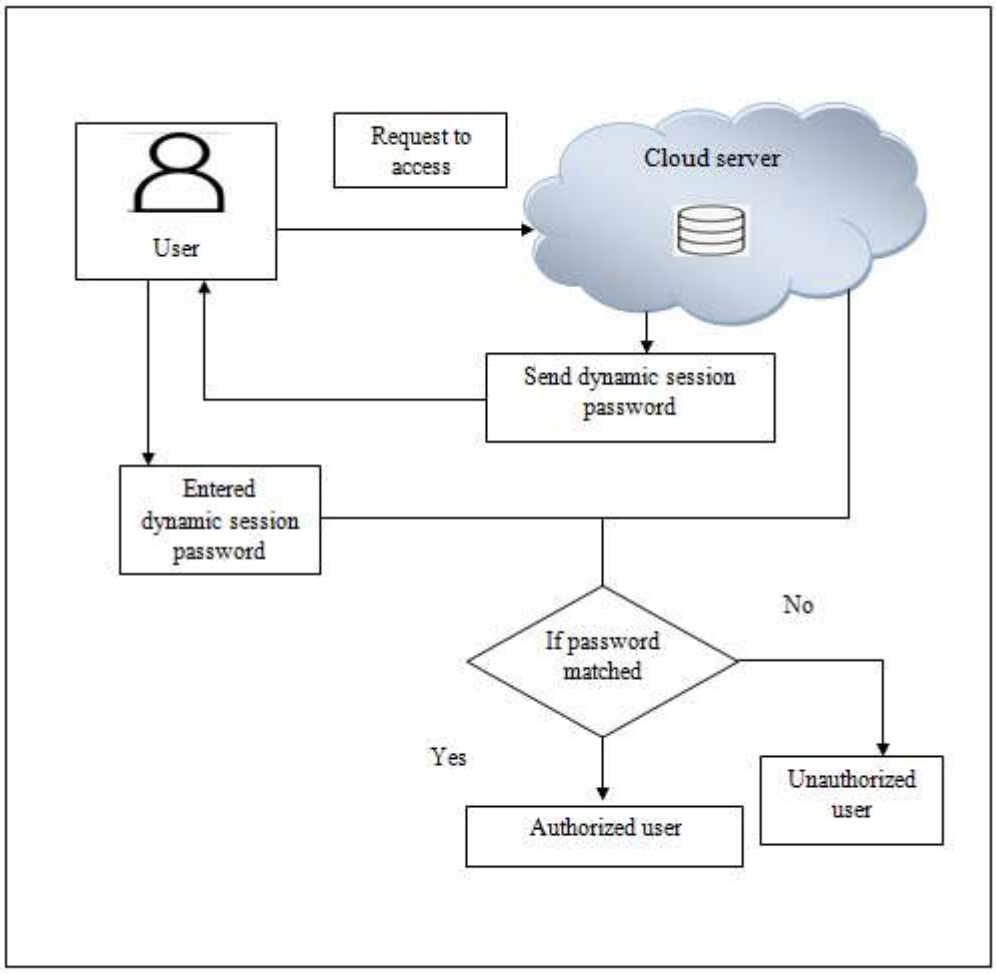

Figure 3 Deming regressive gestalt pattern matching based user authentication

Figure 3 given above illustrates the flow process of the user authentication in cloud environment using Deming regressive gestalt pattern matching. After getting request from user, server confirms authenticity with help of sending the dynamic session password and gestalt pattern matching. Therefore, the pattern matching process is given below,

$$PM = 2 * \frac{M_{Patterns}}{n} \quad (6)$$

Where, PM denotes a pattern matching,$M_{Patterns}$ denotes a number of matched patterns i.e. word, n indicates a number of words in entered password and password sent by server. Pattern matching function provides the output

values between zero and one. When CU entered password acquire matched through CS sent password, CU is said to authorized user as well as permitted to access data from CS. Otherwise, cloud user is said to unauthorized user and allowed to deny data from CS.

$$PM = \begin{cases} 1\ ; & \text{authorized user} \\ 0\ ; & \text{unauthorized user} \end{cases} \quad (7)$$

From the matching patterns, the accurate authentication process is performed. If both the dynamic session password is matched, user is said authorized. The authorized user decrypts the data.

3.4 Decryption

It is process of converting encrypted data i.e. cipher text into its original data. It helps to decode the encrypted data hence which authorized user merely decrypts data since decryption requires a secret key generated through CS. Authorized user decrypts data through their private secret key as follows,

$$D = \log_{N_1 b} [N_1 C_x] \quad (8)$$

Where, D indicates a user original data, C_x denotes a cipher text, N_1 denotes a prime private key, b denotes a generator. The algorithmic process of Time Synchronized Gestalt Pattern Matching RegressiveCryptosystem based User Authentication (TSGPMRC-UA) is described as follows,

// Algorithm 1 Time Synchronized Gestalt Pattern Matching Regressive Cryptosystem based User Authentication

Input: cloud user's $U_1, U_2, U_3, \ldots . U_n$ who generates the data $D_1, D_2, \ldots D_m$ to store and access the from the cloud server (CS).
Output: Improve the authentication accuracy

Begin
// registration and key generation
1: For each user U_i
2. Send Registration request 'R_q' to CS
3. Register with ID && PW
4. CS stores detail to database
5. **End for**
6. for each registered user RU_i
7. CS generates time synchronized key pair $\{Pk_p, Sk_p\}$ using (3) (4)
8. **end for**
9. User perform data encryption using (5)
10. Obtain cipher text 'C_x'
11. Send Ciphertext and stored in CS
12. **If** user access data **then**
13. CS verifies the authenticity using (6)
14. **If** ($PM = 1$) **then**
15: User is recognized as a authorized
16. CS permit to access the data
17. **else**
18. User is recognized as a unauthorized
19. CS deny to access the data
20. **End if**
21. End if
22. Authorized user receives the original data 'D' using (8)
End

The above algorithmic process demonstrates the process of user authentication for safe data communication in cloud environment. Number of users in a cloud environment is first o register their details with ID and password. Then CS generates key and sends it to the corresponding user. Through the generated keys, the cloud user carry outs data encryption to convert original data to cipher text and stored it in CS. Whenever user requires to access data from server, they primary verify authenticity through dynamic password matching. When the user dynamic password gets

matched, CS detects authorized user as well as authorize to access stored data. Otherwise, CS removes access to unauthorized users. After that authorized user carry outs decryption through their private key o obtain original data.

4. Implementation setup

In this section, experimental evaluation of the TSGPMRC-UA, existing Privacy-ABCs [1], SADS-Cloud [2] are executed using java language. To perform implementation, cloud users' and data are collected from Amazon access sample dataset from UCI repository https://archive.ics.uci.edu/ml/datasets/Amazon+Access+Samples. The datasetincludes a large amount of cloud users data with varied registered and authorization data. This is sparse dataset including users and their assigned access. File consist of 4 kinds of attributes. This kind of dataset describes a users can possibly have access and label '1'. Otherwise it will be 0.

5. Performance analysis

Comparative study of TSGPMRC-UA, conventional Privacy-ABCs [1], SADS-Cloud [2] are presented for cloud environments through dissimilar valuation parameters namely

- Authentication accuracy
- Authentication time
- Data confidentiality rate
- Data Integrity rate

Authentication accuracy: It is defined as ratio of number of cloud users that are properly authenticated as authorized or unauthorized for secure communication. It is calculated as follows.

$$\mathrm{AU_{Acc}} = \sum_{i=1}^{n} \frac{\mathrm{UCA}}{\mathrm{U_i}} * 100 \quad (9)$$

Where, $\mathrm{AU_{Acc}}$ represents an authentication accuracy, UCAdenotes a users correctly authenticated, $\mathrm{U_i}$denotes a total number of users. It is measured in percentage (%).

Authentication time: It is defined as amount of time consumed through algorithm to classify authorized or unauthorized users. Overall time consumption of authentication time is estimated as follows.

$$\mathrm{AU_{Time}} = \sum_{i=1}^{n} \mathrm{U_i} * \mathrm{Time\ [UA]} \quad (10)$$

Where, $\mathrm{AU_{Time}}$represents an authentication time,$\mathrm{U_i}$ denotes a total number of cloud users, Time [UA]designates a time consumed for user authentication. It is calculated in milliseconds (ms).

Data confidentiality rate: It is measure of number of data which are accessed through authorized access as well as denied access for unauthorized user. It is calculated as below

$$\mathrm{Rate_{DC}} = \left[\frac{\mathrm{Numberofdataprotected}}{\mathrm{m}}\right] * 100 \quad (11)$$

Where, $\mathrm{Rate_{DC}}$ represent data confidentiality rate, m indicates number of data that is measured in percentage (%).

Data integrity rate: It defined as number of data which are not altered through any unauthorized users. It is calculated as below,

$$\mathrm{Rate_{DI}} = \left[\frac{\mathrm{Numberofdata\ not\ altered}}{\mathrm{m}}\right] * 100 \quad (12)$$

Where, $\mathrm{Rate_{DI}}$ indicates data confidentiality rate, m represents number of data that is measured in percentage (%).

Table 1 comparison of authentication accuracy

Number of cloud users	Authentication accuracy (%)		
	TSGPMRC-UA	Privacy-ABCs	SADS-Cloud
1000	96.5	92.5	90.5
2000	97	91.75	89.4
3000	96.63	91.5	88.16
4000	95.62	92.8	89.62
5000	94.7	89.12	87.24
6000	95.91	88.31	86.08
7000	96.42	90.17	88.71
8000	95.68	88.87	86.95
9000	96.62	91.66	87.76
10000	95.23	90.12	86.55

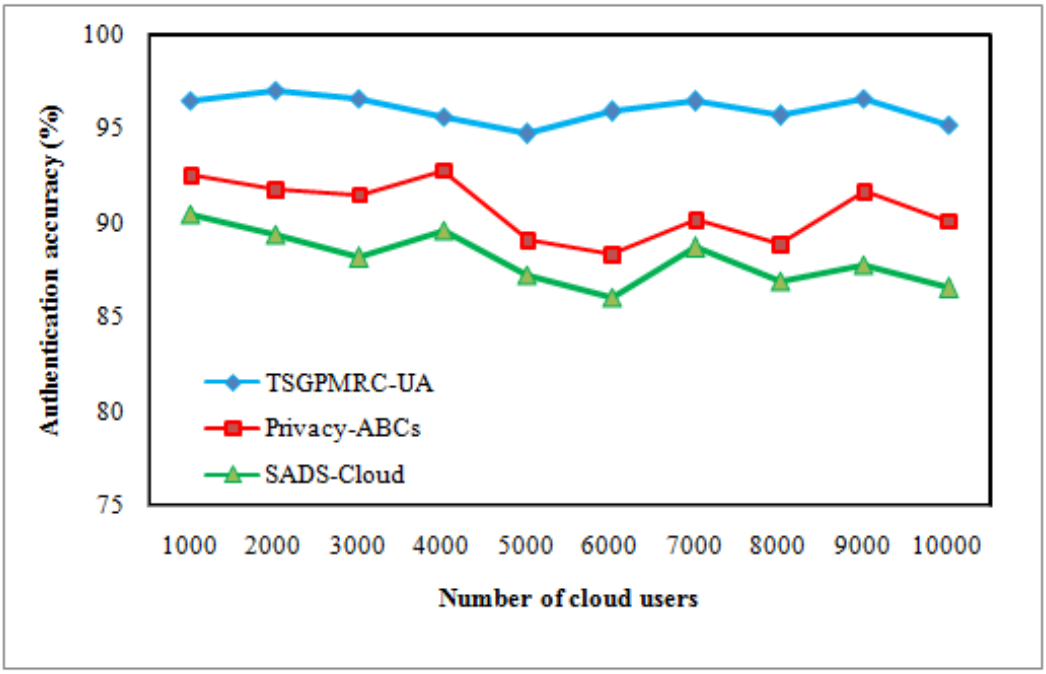

Figure 4 Comparative results of authentication accuracy

Table 1 and figure 4 indicates the comparative analysis of user authentication accuracy with number of cloud users. To conduct experimentation, accuracy is calculated using three methods namely TSGPMRC-UA, existing Privacy-ABCs [1], SADS-Cloud [2]. For every technique, ten various outcomes were examined. Experimental outcomes reported that proposed TSGPMRC-UA technique provides better performance when compared to two conventional methods. Let us assume 1000 users in the cloud environment for storing as well as access data from the cloud. Authentication accuracy of TSGPMRC-UA was observed 96.5% and the accuracy of existing [1] [2] were 92.5% and 90.5% respectively. The overall observed results of TSGPMRC-UA are compared to conventional methods. Finally, average of comparison outcomes proves which the overall authentication accuracy of TSGPMRC-UA is considerably improved by 6% and 9% than the [1],[2] respectively. This improvement is achieved by using Deming regressive

gestalt pattern matching. When the user wants to access data from CS, they initial confirm authenticity through dynamic session password matching. Pattern matching concept in regression analysis accurately performs user authentication as well as identifies the authorized user to permit data access. Otherwise, the server removes the access for unauthorized user.

Table 2 comparison of authentication time

Number of cloud users	Authentication time (ms)		
	TSGPMRC-UA	Privacy-ABCs	SADS-Cloud
1000	32	36	40
2000	40	44	48
3000	45	51	54
4000	52	56	60
5000	55	60	65
6000	57	63	67.2
7000	61.6	66.5	73.5
8000	68	**72**	**76**
9000	73.8	**79.2**	**84**
10000	76	**82**	**89**

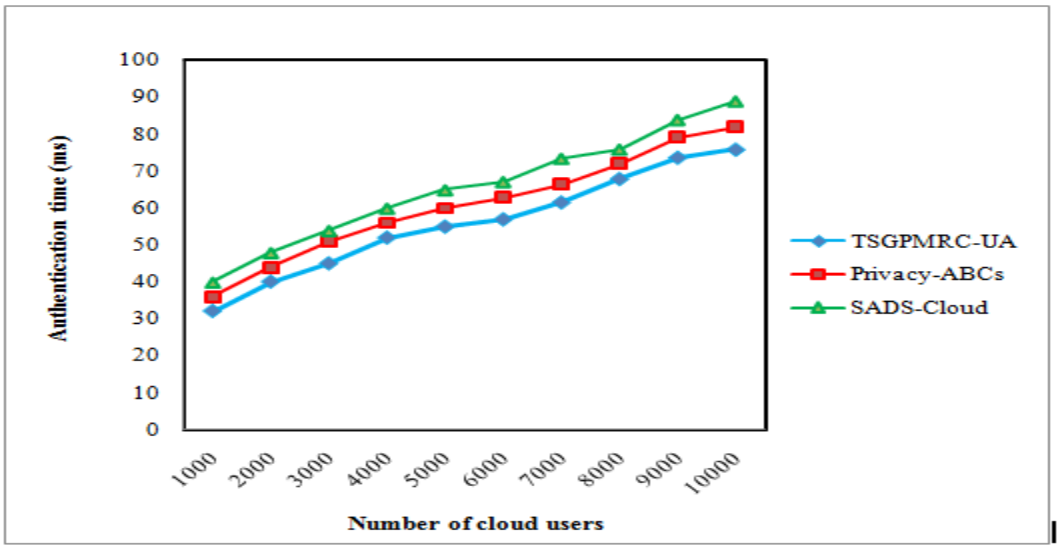

Figure 5 Comparative results of authentication time

Performance of user authentication time with number of cloud users is given in table 2 and figure 5.The observed performance result of authentication timedesignates that the authentication time increased linearly while increasing the number of cloud users. Among the three methods, TSGPMRC-UA method reduces the overall time consumption of cloud user authentication when compared to other two methods Privacy-ABCs [1], SADS-Cloud [2]. Let us consider number of cloud users is 1000, time utilization of cloud user authentication using TSGPMRC-UA methodwas

found to be32ms and hence the authentication time of the other two conventional methods [1], and [2] were 36ms and 40ms. For every technique, different performance outcomes were examined through a number of cloud users. Therefore, the overall comparison results of TSGPMRC-UA methodare compared to outcomes of conventional methods. As a result, time involved in performing user authentication between the users are said to be comparatively reduced using TSGPMRC-UA method. With this performance analysis, authentication time using TSGPMRC-UA method is considerably decreased by 8% compared to [1] and 15% compared to [2]. This is because of the application of Deming regressive gestalt pattern matching based user authentication. By applying regression function, authorized as well as unauthorized users are recognized during the dynamic session password matching process. This process consumed lesser time for authenticating the user for access control policy in cloud environment.

Table 3 comparison of data confidentiality rate

Number of users data	Data confidentiality rate (%)		
	TSGPMRC-UA	Privacy-ABCs	SADS-Cloud
10000	95.66	92.14	90.22
20000	94.83	89.27	87.11
30000	96.65	88.18	85.51
40000	95.305	91.02	86.41
50000	97.11	92.42	89.13
60000	95.74	90.18	87.76
70000	94.26	90.74	88.77
80000	95.69	89.31	87.62
90000	97.28	91.72	89.51
100000	96.36	90.23	88.65

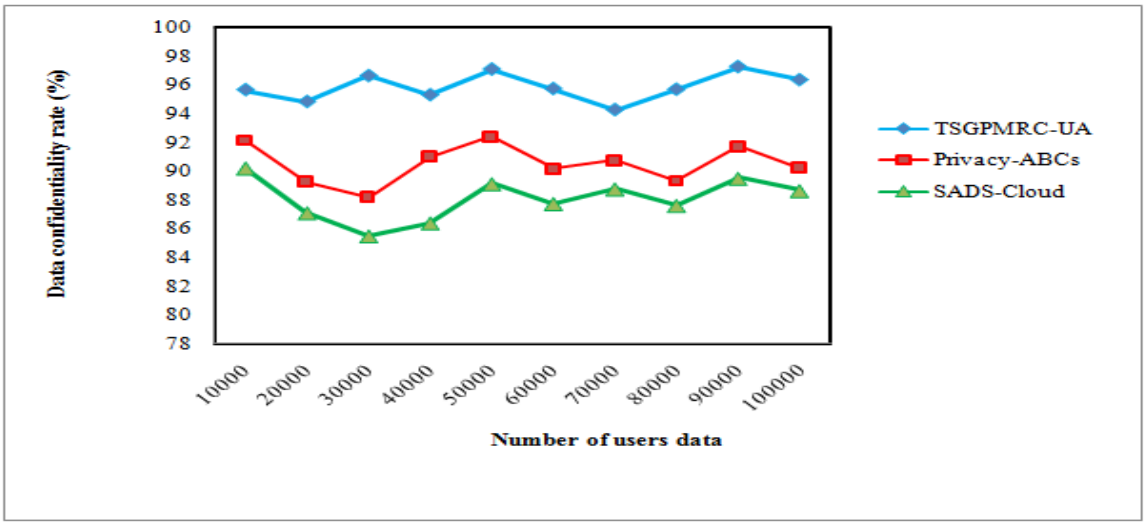

Figure 6 Comparative results of Data confidentiality rate

Table 3 , figure 6 illustrates overall performance comparative analysis of $Rate_{DC}$in cloud environment with number of user data . Data confidentiality measurement is used to protect cloud user information from unauthorized users. In other words, the rate at which the data access and communication between users ad cloud server is secured from unauthorized access. Examined graphical outcomes indicate that the $Rate_{DC}$ using TSGPMRC-UA method provides improved confidentiality level. This is proved during sample mathematical calculation, through considering '10000' user data for estimating confidentiality rate. Confidentiality rate was found '95.66% using the TSGPMRC-UA method, similarly '92.14 %' using an [1] and '90.22%' using [2] respectively. The confidentiality rate for each

of algorithms is obtained from average of 10 iterations. Results represent that data confidentiality rate is significantly minimized by 6% , 9% than the conventional methods. This is owing to Boneh–Goh–Nissim Cryptosystem applied in the TSGPMRC-UA method. For each registered user, server generates the time synchronized confidential key pairs for each session to remove unauthorized data access. In addition, Boneh–Goh–Nissim Cryptosystem also performs data encryption through receiver public key. Then authentication process of TSGPMRC-UA method helps to permit the access for authorized user and remove access for unauthorized user resulting it enhance the data confidentiality rate.

Table 4 comparison of data integrity rate

Number of users data	Data integrity rate (%)		
	TSGPMRC-UA	Privacy-ABCs	SADS-Cloud
10000	94.55	90.2	89.56
20000	93.27	87.94	85.5
30000	95.22	85.51	83.66
40000	93.88	88.81	85.25
50000	96.31	86.51	84.24
60000	94.75	87.75	85.75
70000	93.92	86.30	83.50
80000	94.81	85.31	81.56
90000	96.13	88.40	84.33
100000	95.65	86.56	84.12

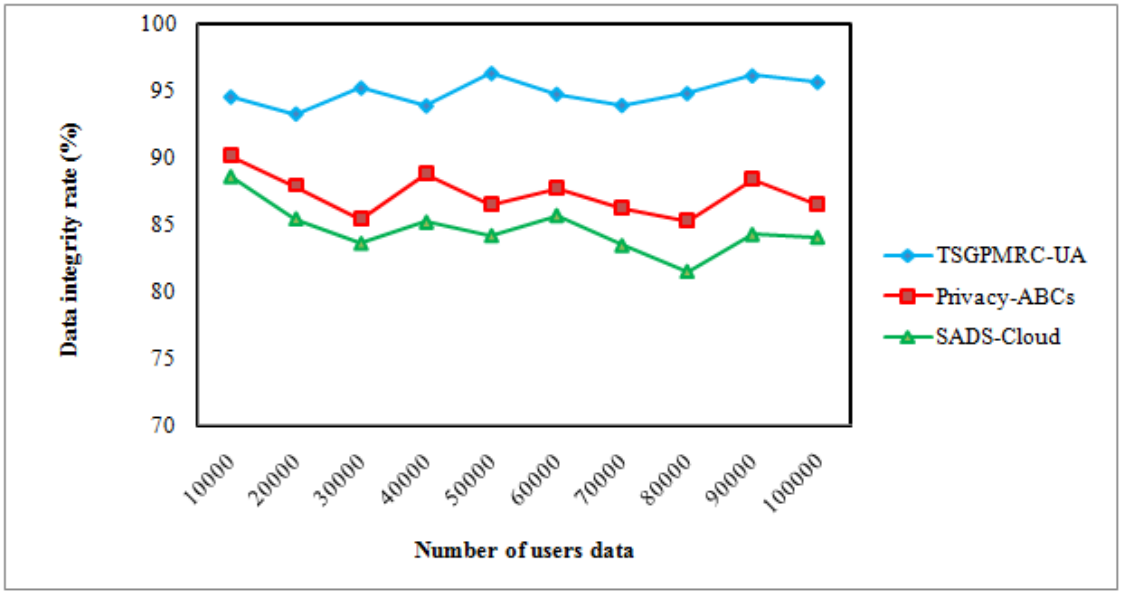

Figure 7 Comparative results of data integrity rate

Table 4 , figure 7 shows graphical analysis of $Rate_{DI}$ for cloud user data ranging between 10000 and 100000. To

conduct an analysis of our results in terms of data integrity rate and then compared it with existing [1] and [2] respectively. Figure 7 shows Rate_{DI} for TSGPMRC-UA technique is considerably improved when compared to[1] and [2] respectively. Let us consider number of cloud users data is 10000. The Rate_{DI} of TSGPMRC-UA method was observed 94.55% , Rate_{DI} of existing [1] [2] were observed to be 90.2% and 89.56% respectively. Average of ten iterations and outcomes are denoted by Rate_{DI} noticeably enhanced by 9% and 12% when compared to existing methods. Hence, our proposed TSGPMRC-UA method gave satisfactory results in terms of data integrity rate. The reason for this improvement was owing to the application of Boneh–Goh–Nissim encryption and decryption for ensuring security in the data access. With these two functions, TSGPMRC-UA method uses data authentication to remove the data access for unauthorized user. This process aids to evade data alteration and modification of data.

6. CONCLUSION

CC is newly emerged paradigm where multiple users are connected through the Internet to share and store data. Because a large number of users' private data is stored on the cloud server, providing authentication for secure communication between user and server is still an important issue. In this article, the TSGPMRC-UA technique is developed to resolve security issue in cloud environment. In the cloud, server generates pair of time-synchronized keys through help of Boneh–Goh–Nissim Cryptosystem. Then user encrypts their data and stored it on a CS for additional processing. When user wants to access stored data from CS, the authenticity is initial verified and grants data. The authorized user accesses the data and other users remove the data access for achier better secure communication in the cloud. Experimental implementation is carried out for examining performance of TSGPMRC-UA method and conventional encryption techniques by various parameters. Execution outcomes confirm that TSGPMRC-UA method performed well and is more efficient having a higher confidentiality rate, authentication accuracy, integrity rate, and lesser authentication time than the conventional authentication methods.

REFERENCES

[1]Victor Sucasas, Georgios Mantas, Maria Papaioannou, Jonathan Rodriguez, "Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services", IEEE Transactions on Cloud Computing, Volume 11, Issue 1, 2023, Pages 168 – 184. **DOI:** 10.1109/TCC.2021.3084538

[2]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, Volume 34, Issue 6, 2022, Pages 3121-3135. https://doi.org/10.1016/j.jksuci.2020.05.005

[3] Nishant Doshi and Payal Chaudhari , "Cryptanalysis of Authentication Protocol for Cloud Assisted IoT Environment", Procedia Computer Science, Elsevier, Volume 220 , 2023, Pages 886–891. https://doi.org/10.1016/j.procs.2023.03.120

[4] Ummer Iqbal , Aditya Tandon , Sonali Gupta , Arvind R. Yadav , Rahul Neware , and Fraol Waldamichael Gelana, "A Novel Secure Authentication Protocol for IoT and Cloud Servers", Wireless Communications and Mobile Computing, Hindawi, Volume 2022, March 2022, Pages 1-17. https://doi.org/10.1155/2022/7707543

[5] Xiaodong Yang, Meiding Wang, Ting Li, Rui Liu, Caifen Wang, "Privacy-Preserving Cloud Auditing for Multiple Users Scheme With Authorization and Traceability", IEEE Access Volume 8,2020, Pages 130866 – 130877. **DOI:** 10.1109/ACCESS.2020.3009539

[6] Tsu-Yang Wu, Qian Meng, Saru Kumari and Peng Zhang, "Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments", Sensors , Volume 22, Issue 10, Pages 1-19. **https://doi.org/10.3390/s22103858**

[7] Naveed Khan , Jianbiao Zhang , and Saeed Ullah Jan, "A Robust and Privacy-Preserving Anonymous User Authentication Scheme for Public Cloud Server", Security and Communication Networks, Hindawi, Volume 2022, March 2022, Pages 1-14. https://doi.org/10.1155/2022/1943426

[8] Mahdi Nikooghadam, Haleh Amintoosi, "Secure communication in CloudIoT through design of a lightweight authentication and session key agreement scheme", International journal of communication system, Wiley, Volume 36, Issue 1, 2020, Pages 1-17. https://doi.org/10.1002/dac.4332

[9] Diksha Rangwani & Hari Om, "A Secure User Authentication Protocol Based on ECC for Cloud Computing Environment", Arabian Journal for Science and Engineering, Springer, Volume 46, 2021, Pages 3865–3888. https://doi.org/10.1007/s13369-020-05276-x

[10] Prabhat Kumar Panda and Sudipta Chattopadhyay, "An enhanced mutual authentication and security protocol for IoT and cloud server", Information Security Journal: A Global Perspective, Taylor & Francis, Volume 31, Issue 2, 2022, Pages 144-156. https://doi.org/10.1080/19393555.2020.1871534

[11] Hong Zhong, Chuanwang Zhang, Jie Cui, Yan Xu, Lu Liu, "Authentication and Key Agreement Based on Anonymous Identity for Peer-to-Peer Cloud", IEEE Transactions on Cloud Computing, Volume 10, Issue 3, 2022, Pages 1592 – 1603. **DOI:** 10.1109/TCC.2020.3004334

[12] Zahid Ghaffar, Shafiq Ahmed , Khalid Mahmood , Sk Hafizul Islam , Mohammad Mehedi Hassan, and Giancarlo Fortino, “An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-Social-Systems”, IEEE Access , Volume 8, Pages 47144 – 47160. **DOI:** 10.1109/ACCESS.2020.2977264
[13] Jian Shen, Dengzhi Liu, Qi Liu, Xingming Sun, Yan Zhang, “Secure Authentication in Cloud Big Data with Hierarchical Attribute Authorization Structure”, IEEE Transactions on Big Data , Volume 7, Issue 4, 2021, Pages 668 – 677. **DOI:** 10.1109/TBDATA.2017.2705048
[14] Hamza Hammami, Sadok Ben Yahia & Mohammad S. Obaidat, “A lightweight anonymous authentication scheme for secure cloud computing services”, The Journal of Supercomputing, Springer, Volume 77, 2021, Pages 1693–1713. https://doi.org/10.1007/s11227-020-03313-y
[15] Yicheng Yu, Liang Hu and Jianfeng Chu, “A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment”, Symmetry, Volume 12, Issue 1 , Pages 1-16. https://doi.org/10.3390/sym12010150
[16] Anakath Arasan, Rajakumar Sadaiyandi, Fadi Al-Turjman, Arun Sekar Rajasekaran & Kalai Selvi Karuppuswamy, “Computationally efficient and secure anonymous authentication scheme for cloud users”, Personal and Ubiquitous Computing, Springer, 2021, Pages 1-11. https://doi.org/10.1007/s00779-021-01566-9
[17] Leila Megouache, Abdelhafid Zitouni & Mahieddine Djoudi, “Ensuring user authentication and data integrity in multi-cloud environment”, Human-centric Computing and Information Sciences, Springer, volume 10, 2020, Pages 1-20. https://doi.org/10.1186/s13673-020-00224-y
[18] Rahul Sahu, Sanjana Rathour, “An Improved Authentication and Data Security Approach Over Cloud Environment”, International Journal of Scientific & Technology Research, Volume 9, Issue 01, 2020, Pages 3596-3600.
[19] Sandeep kaur ,Gaganpreet kaur and Mohammad Shabaz, “A Secure Two-Factor Authentication Framework in Cloud Computing”, Security and Communication Networks, Hindawi, Volume 2022, March 2022, Pages 1-9. https://doi.org/10.1155/2022/7540891
[20] Ahmed Yaser Fahad Alsahlani and Alexandru Popa, “LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment”, Journal of Network and Computer Applications, Elsevier, Volume 192, 2021, Pages 1-20. https://doi.org/10.1016/j.jnca.2021.103177