ISSN 2278-3091

Volume 9, No.4, July – August 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse381942020.pdf

https://doi.org/10.30534/ijatcse/2020/381942020

Ephemeral Schnorr Signcryption for Secure Data Transaction in Cloud

Kavitha K[1], Saravanan V[2]

[1]Department of Computer Applications, Dr. N.G.P. Arts and Science College, Coimbatore, India

[2]Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, India

[1] kavitha.k@drngpasc.ac.in, [2]vsreesaran@gmail.com

ABSTRACT

Cloud computing is a new method used to offer the various services. Security is a major concern for protecting the data from the unauthorized user access while performing the data transaction from cloud user and server. However, the conventional methods still have the issues of data transaction security. In order to improve the security level during the data transaction, Ephemeral Schnorr Signcryption based Secured Data Transaction (ESS-SDC) method is introduced for improving the data confidentiality rate in cloud environment. The ESS-SDC method includes the three processes, namely ephemeral key generation, signcryption and signature verification. Initially, the cloud server generates the ephemeral key pair (i.e., private key and public key) for each registered cloud user to access the data. When a cloud user wants to access the data from server, the data owner performs identity based authentication. If a cloud user is an authorized user, data owner request the cloud server to transmit the data in the form of ciphertext and signature to the cloud user. Finally, the signature verification is performed at the receiver side (i.e. user) to decrypt the data. Then the authorized users obtain the original data and improve the secure data transaction process. Experimental evaluation of proposed ESS-SDC method and existing methods are carried out with respect to the number of cloud users and data. The results and discussion confirmed that the proposed ESS-SDC method improves the transaction security with higher data confidentiality rate, authentication accuracy and minimum processing time than the other state-of-the-art-methods.

Key words: Cloud, data transaction security, Ephemeral key generation, identity based authentication, encryption, signature generation, signature verification

1. INTRODUCTION

Security issue on secure data transaction is to allow users for accessing their data over the cloud. Cloud computing provides flexible access through the internet-based computing to the users. As the users communicate with the cloud server, security is an essential issue for protecting the data from unauthorized access. To prevent unauthorized access in the cloud, signcryption is performed for improving the transaction security.

A Multi-Authority ciphertext policy attribute based sigcryption (MACP-ABSC) scheme was introduced in [1] for secure data access control. The designed scheme minimizes the complexity but the authentication was not performed to attain higher security. A DNA inspired symmetric key encryption technique (BDNA) was developed in [2] to prevent the unauthorized users accessing the data. Through the technique minimizes the encryption time but data confidentiality was not improved. A secure and practical searchable symmetric encryption method was developed in [3] for accessing the cloud data. But the designed scheme has higher time for symmetric encryption.

A different Privacy preserving approaches were developed in [4] for protecting the data from unauthorized access. But the quantitative performance of Privacy preserving parameters remained unaddressed. An attribute-based encryption scheme was introduced in [5] for secure cloud data access control. The designed scheme failed to use the authorization method for improving the security. A Ciphertext-Policy Attribute-Based Encryption was developed in [6] to enables the data owners for providing the data to authorized users. But it failed to use the signature scheme for enhancing the security. A blowfish hybridized weighted attribute-based Encryption (BH-WABE) method was developed in [7] for secure data access. Though the designed method improves the data confidentiality, the authentication was not performed to detect the unauthorized users. An Identity based access control method was proposed in [8] to ensure secure access of the data by the authenticated users. But the performance of data confidentiality was not improved. An Elliptic Curve Cryptosystem based user authentication was developed in [9] to guarantee cloud computing security. But an efficient cryptosystem was not used for enhance the security in cloud.

A revocable-storage identity-based encryption (RS-IBE) method was developed in [10] for secure data sharing. The method minimizes the encryption and decryption cost but the accurate authentication was not performed. A role based access control method was introduced in [11] for secure search applications and also improving the data confidentiality. But it failed to use any cryptographic technique to improve the performance of security. A new privacy-preserving attribute based signcryption (PROUD) method was developed in [12] for improving the security of data access. But the performance of data confidentiality rate was not improved. An anonymous ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE) was introduced in [13]. The user authentication was not performed to avoid the unauthorized access.

Secure and efficient elliptic curve cryptography based mutual authentication protocol was introduced in [14]. Though the method minimizes the computation cost but the higher security was not achieved. A novel dynamic password-based two-server authentication mechanism was developed in [15] based on public and private key cryptography. The mechanism achieves secure access to the cloud services but time analysis remained unsolved. A proxy re-encryption based multi-factor access control (PMAC) scheme was introduced in [16] for increasing the cloud security and access control. The scheme failed to use the signature generation mechanism for achieving higher confidentiality. The different cryptographically enforced secure cloud storage solutions were proposed in [17] to protect the data from the invalid users. A privacy preserving access control method was introduced in [18] for secure service provision. The performance of security metrics evaluation was not considered. A hybrid cryptography algorithm based end-to-end encryption (E2EE) method was developed in [19] to maintain integrity and confidentiality of data. A secure data access and sharing scheme were developed in [20] for secure cloud services to guarantee the data integrity and confidentiality. However, the above said methods measures only the data confidentiality. The other metrics like time analysis was not considered.

1.1 Major contribution of the paper

The several issues identified from the above- said literatures are overcome by introducing a novel ESS-SDC method. The major contribution of ESS-SDC method is summarized as follows,

- To improve security level of data transaction in cloud, ESS-SDC method is introduced based on the authentication and Schnorr signcryption.
- To improve the authentication accuracy, the ESS-SDC method uses the identity based authentication. The cloud user access the data from server, the data owner finds the authorized and unauthorized user based on the user identity. The authorized user only accesses the data for improving the security.
- To improve the data confidentiality rate, the ESS-SDC method performs the Schnorr signcryption and signature verification. The server sends the encrypted data and signature to the authorized cloud users. Then the signature verification is done to guarantee data security in cloud environment. The signature is valid and then the user decrypt the data otherwise, the decryption is not performed. Therefore, the authorized user obtains the data from the cloud server.

1.1 Outline of paper

The paper is structured into different sections. In section 2, a brief explanation of the proposed ESS-SDC method with neat diagram is presented. Experimental evaluation is conducted with various parameters in section 3. This is followed by, results and discussion of the proposed method and existing state-of-art methods are presented in Section 4. Finally, section 5 provides the conclusion.

2. EPHEMERAL SCHNORR SIGNCRYPTION BASED SECURED DATA TRANSACTION

The Ephemeral Schnorr Signcryption is the public-key cryptography that simultaneously executes the both processes namely encryption as well as digital signature. The Ephemeral Schnorr Signcryption is more computationally efficient and also provides greater security to the data in the cloud. The data confidentiality and integrity are two major parameters in the cloud data transaction from server to users. Confidentiality is achieved using encryption and digital signature verification algorithms, whereas integrity is obtained by the use of authentication techniques. Therefore, the proposed ESS-SDC method achieves higher confidentiality by using public key encryption based digital signature generation and verification algorithm.

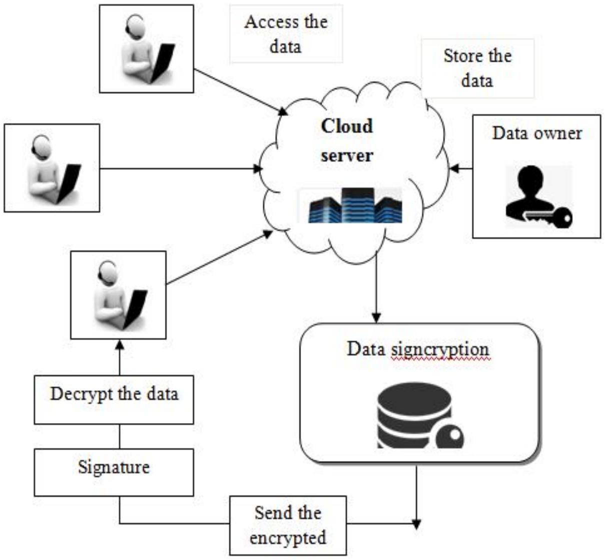

Figure 1: Flow process of signcryption based data transaction security in cloud

Figure 1 illustrates the flow process of proposed ESS-SDC method to obtain higher data transaction security in cloud. The cloud based architecture comprises the three entities such as a number of cloud users $Cu_1, Cu_2, Cu_3, \ldots . . Cu_n$, cloud server ($CS$) and data owner ($DO$) for providing the secure data access. The cloud owner sends their data to the cloud server. Whenever the cloud user wants to access the data, the cloud owner initially verifies the user identity. If the user is authenticated and the then cloud server sends the signature as well as the encrypted data to the user. Then the cloud user performs the signature verification and decryption to obtain the original data. The different processes of the proposed ESS-SDC method are described in the following sections.

2.1 Key generation

The first process of proposed ESS-SDC method is the key generation for every registered user in the cloud environments. Initially, the cloud user registers their personal information to access and store data such as first name, middle name, last name, date of birth, gender, mobile number and mail-id so on. After registering their details to the cloud server, the Ephemeral key pair's i.e. private or public keys are generated and send to the cloud user.

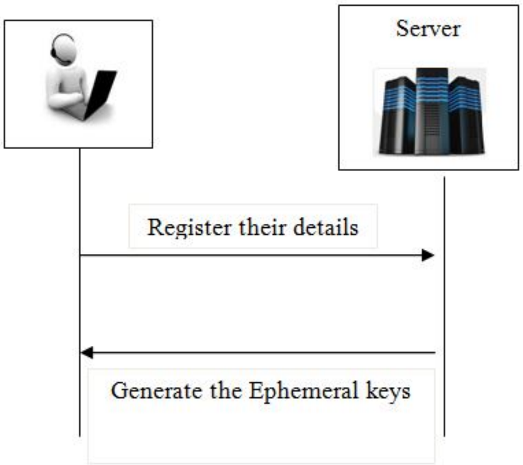

Figure 2: Flow process of the ephemeral key pair generation

Figure 2 shows the process of ephemeral key pair generation. In cryptography, ephemeral key is created for each execution of key establishment process. The ephemeral keys are used within a particular session where the cloud server generates only one ephemeral key pair (i.e. private and public) per user. The ephemeral private key is kept secret whereas the ephemeral public key is distributed for data encryption. Therefore, a proposed ESS-SDC method generates ephemeral public key for each session. Once the session is completed, then the server disables an ephemeral key and it creates a new public key for next session. This helps to avoid the unauthorized access as a results the confidentiality level gets improved.

The ephemeral private signing key EP_{rk} is chosen as uniformly at random and the public key is generated with the private key. Therefore, the ephemeral public verification key is generated as follows,

$$EP_{bk} = D^{EP_{rk}} \quad (1)$$

From (1),EP_{bk} denotes an ephemeral public key used for signature verification, D denotes an integer of prime order, EP_{rk} represents the private key. Then the cloud server sends the ephemeral key pair (EP_{rk}, EP_{bk}) to the each registered user in cloud environment. The ephemeral private key is kept secret used for signature generation whereas ephemeral public key is widely distributed for performing the encryption. As a result, the proposed ESS-SDC method efficiently performs ephemeral key pair generation with minimum time.

2.2 Identity authentication and Schnorr Signcryption

After the ephemeral key generation process, the data owner stores their data to the cloud server.

When, the cloud user sign in and wants to access the data, initially the data owner verifies their authenticity for secure service provisioning by avoiding the unauthorized user access. Therefore, the authentication is done by the data owner. The flow process of Identity Authentication and Schnorr Signcryption is shown in figure 3.

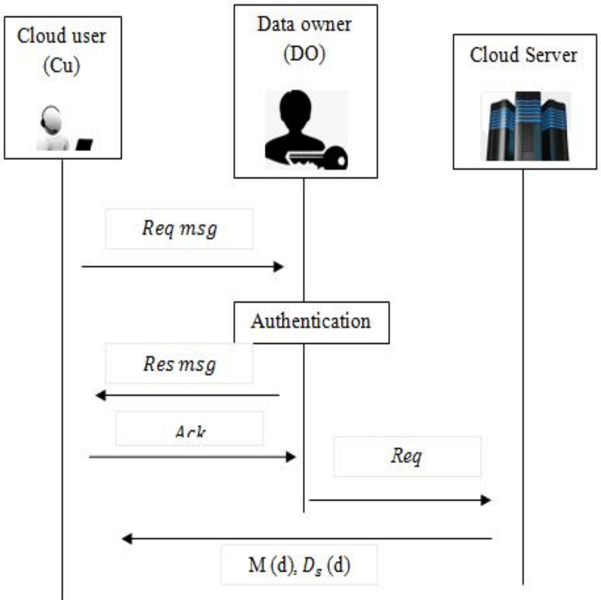

Figure 3: Flow process of identity authentication and signature generation

Figure 3 shows the flow process of the identity authentication and signature generation. When a cloud user wants to access the data from server, the cloud user (Cu) sends the request message ($Req\ msg$) to the data owner. Then, data owner (DO) performs identity based authentication for cloud user from CS. The data owner verifies whether the cloud user's currently entered identity during the signing phase is matched with the identity which is already stored at the time of registration. If these two ID's are matched, then the user is said to authorize otherwise the user is said to an unauthorized user. If the user is said to be an authorized user, the data owner sends the response message ($Res\ msg$) to cloud user. Upon the successful reception of response messages, the cloud user sends acknowledge message (Ack) to the data owner. Followed by, the data owner sends request (Req) to cloud server to transmit the encrypted data and signature to the authorized users.

The server performs the signcryption to improve the data confidentiality. A signcryption is a public-key method that simultaneously performs both digital signature and data encryption. Encryption and digital signature are two fundamental cryptographic tools that used to guarantee the confidentiality of the data in cloud.

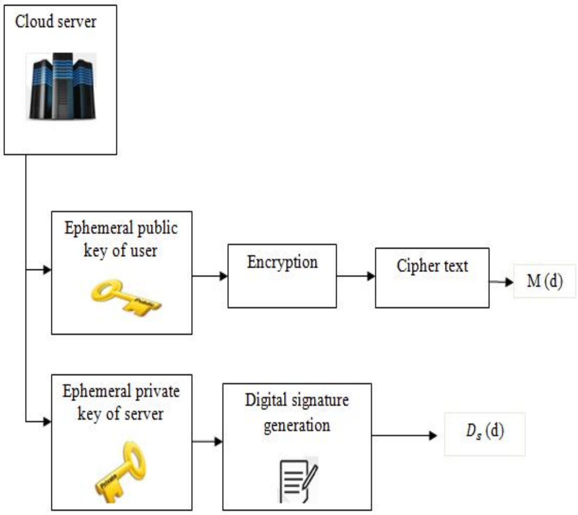
Cloud server
Ephemeral public key of user
Encryption
Cipher text
M (d)
Ephemeral private key of server
Digital signature generation
D_s (d)

Figure 4: Block diagram of Schnorr Signcryption

Figure 4 depicts the block diagram of schnorr signcryption used to obtain the cipher text of original data $M(d)$ and Digital signature$D_s\ (d)$. Encryption is the process of converting the original data into unreadable form (i.e. cipher text). Therefore the encryption is used for the data accessed by the authorized users and those who are not authorized cannot access the data.

Encryption is a probabilistic method that takes a original data 'd' and the Ephemeral public key of the receiver as input and outputs of cipher text is obtained as follows,

$$M\ (d) \leftarrow EN(EP_{bk}, d) \quad (2)$$

Where, $M\ (d)$ denotes a cipher text of original data 'd', EN indicates an encryption, EP_{bk} is an Ephemeral public key of user. After the encryption, cipher text is obtained as output and the signature generation is performed accordingly. A digital signature is used for determining the authenticity of original data. A valid signature is used to believe that the data is created by an authorized sender (i.e. cloud server), and that data is not modified by any intruders. Therefore, the proposed ESS-SDC method performs the digital signature generation with the secret private key of server during the data accessing in cloud. This digital signature is obtained in the form of hash value. A hash value is any function that is used to map the data of random size into a data of fixed length. The signature generation process is expressed as given below,

In order to generate the signature, a random number 'R' is chosen.

$$G = D^R \quad (3)$$

By using (3), the signature is generated as follows,

$$D_s \text{ (d)} = h\ (G\ \|d) \quad (4)$$

From (4),D_s (d) denotes a signature generated by the data 'd', ($\|$) denotes a concatenation, G denotes a bit string, h is the cryptographic hash function. The cloud server sends the encrypted data and digital signature to the cloud user.

2.3 Digital signature verification and decryption

After receiving the encrypted data to cloud server, the digital signature verification and decryption is performed at the receiver side. The flow process of the digital signature verification and decryption is illustrated in the figure 5. .

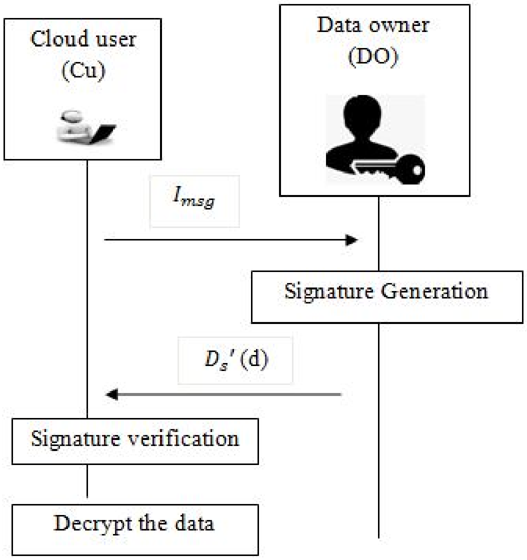

Figure 5: Signature verification and decryption

Figure 5 illustrates the flow process of signature verification and decryption. After receiving the encrypted data and signature, the cloud user sends the intimation message (I_{msg}) to data owner. Then the data owner again generates the signature for that particular data as given below,

$$D'_s(d) = h\ (G_v \|d) \quad (5)$$

Where, $D'_s(d)$ denotes a new signature, G_v denotes a bit string, h is the cryptographic hash function. Then the generated signature is sent to the cloud user for verification. The data verification is given below,

$$f(x) = \begin{cases} if\ \left(D_s(d) = D'_s(d)\right)\ ;\ signature\ is\ valid \\ otherwise; \quad signature\ is\ not\ valid \end{cases} \quad (6)$$

From (6),$f(x)$ denotes verification function. When the signature is valid, then the cloud user decrypts the data. The cloud user decrypts the cipher text using their ephemeral private key as follows,

$$O(d) \leftarrow DE(EP_{rk}, M(d)) \quad (7)$$

From (7),$O(d)$ denotes a plain text, DE indicates the decryption, EP_{rk} denotes a ephemeral private key, $M(d)$ is the cipher text. In this way, the secure data transaction is carried out from cloud server to cloud user with higher data confidentiality rate. The algorithmic process of proposed ESS-SDC method is described as follows.

```
Input: Number of cloud users $Cu_1, Cu_2, Cu_3 \ldots . Cu_n$, data $d_1, d_2, d_3 \ldots . d_m$, cloud server (CS), data owner (DO)
Output: Secure cloud data transaction
Begin
\\ Ephemeral key pair generation
    For each cloud user $Cu_i$
        Register their details to cloud server
        CS sends key pair $EP_{rk}, EP_{bk}$ to user
    End for
\\ Authentication
    Cloud user sends $Req\ msg$ to the DO
        DO perform authentication
            If $(ID_E = ID_R)$ then
                User is said to be authorized
            else
                User is said to be unauthorized
            end if
    If user is said to be authorized then
            DO sends $Res\ msg$ to cloud user
        End if
        Cloud user sends $Ack$ to DO
        DO sends Req to cloud server
\\ Signcryption
    For each data $d$
        Server perform encryption $M\ (d) \leftarrow EN(EP_{bk}, d)$
        Generate the digital signature $D_s$ (d) with private key $EP_{pk}$
        CS sends $M\ (d)$, $D_s$ (d) to user
    End for
\\ Signature verification and decryption
            Cloud user sends $I_{msg}$ to DO
            DO generate signature $D'_s$ (d) and send to cloud user
            If $(D_s(d) = D'_s(d))$ then
                Signature is valid
                Decrypt the data using secret private key
        else
            Signature is invalid
            Decryption is not performed
        end if
End
```

Algorithm 1: Ephemeral Schnorr Signcryption based Secured Data Transaction

Algorithm 1 describes a step by step process of Ephemeral synorr signcryption to improve the secure data transaction in cloud. Initially, Ephemeral private key and public key are generated to perform signature generation and decryption. Whenever the user wants to access the data, first the authenticity is verified. The data owner performs the authentication to identify the authorized user for data access. After that, the cloud server performs the encryption to convert the original data into plain text and send to the cloud user. Followed by, the signature generation is carried out to perform secure data transaction. If the user is authorized user, then the data owner request the cloud server to send the encrypted data and signature to the cloud user. After receiving the signature, the cloud user sends the intimation message to the data owner. Then the data owner again generates the signature and verifies the two signatures at the user side. If the two signatures get matched, then the cloud user decrypts the cipher text and obtains the original data. This helps to improve transaction security and data confidentiality level.

3. EXPERIENTIAL EVALUATION

Experimental evaluation of proposed ESS-SDC and existing MACP-ABSC [1], BDNA [2] is implemented in Java Language with cloudsim simulator. To conduct the experimental evaluation, Amazon Access sample Dataset [21] is used to perform the secure data transaction in cloud. The dataset is taken from the UCI machine learning repository. Amazon Access sample dataset is a sparse dataset which includes the users and their assigned access files. These file comprises 4 types of attributes such as Person_Attribute, Resource_ID, Group_ID and System_Support_ID are stored on the cloud server. The cloud server performs 'remove_access' or 'add_access based on the user authentication. This dataset is used to identify the authorized user to access or store the data to the cloud server. Otherwise, the cloud server removes the access. The experimental results of three methods are discussed in following sections with different performance metrics.

4. EXPERIMENTAL RESULTS AND DISCUSSION

The results of the proposed ESS-SDC and existing MACP-ABSC [1], BDNA [2], are discussed in this section with different parameters such as authentication accuracy, processing time and data confidentiality rate. The experimental result of proposed method is compared to two state-of-the-art works with the help of graphical representation. For each section, the mathematical calculation is provided for illustrating the performance of the proposed technique and existing methods.

4.1 Impact of authentication accuracy

Authentication accuracy is referred to as a number of users who are correctly verified as authorized or unauthorized for accessing the data from the cloud server to the total number of users taken as input. The formula for calculating the authentication accuracy is given below,

$$AA = \left(\frac{number\ of\ users\ currently\ authenticated}{n}\right) * 100 \quad (8)$$

Where, AA denotes a authentication accuracy, 'n' represents the number of cloud users. The authentication accuracy is measured in terms of percentages (%). Higher the authentication accuracy, the method is said to be more efficient.

Sample mathematical calculation

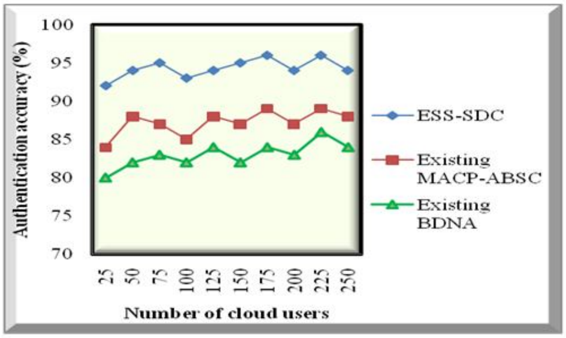

Figure 6: Comparative results of authentication accuracy

Figure 6 depicts the comparative results of authentication accuracy with respect to number of cloud users. As shown in the graph, the authentication accuracy of three methods ESS-SDC method, MACP-ABSC [1], BDNA [2] are represented in three different colors namely blue, red and green. The results clearly show that the authentication accuracy is increased using proposed ESS-SDC method than the existing methods. This is because of, the proposed ESS-SDC method performs the identity based authentication.

Whenever, the cloud user wants to access the data from the cloud, initially the user verifies their authenticity for secured data transaction. Since the unauthorized user did not receive any data from the cloud server. The data owner performs the authentication based on the user identity. The current ID of the user is exactly matched with the already stored ID at the time of registration. If these two ID's are matched, then the data owner request to cloud server for service provisioning. In this way, the proposed ESS-SDC method accurately identifies the authorized or unauthorized users. The authentication accuracy of proposed ESS-SDC method is compared to the existing results. The average of comparison results clearly shows that the proposed ESS-SDC method increases the authentication accuracy by 8% and 14% as compared to existing MACP-ABSC [1], BDNA [2] respectively.

Sample mathematical calculation

4.2 Impact of data confidentiality rate

Data confidentiality rate is defined as the numbers of cloud data that are correctly accessed by the authorized users to the total number of data taken as input. The mathematical formula to compute the data confidentiality rate is given below,

$$Rate_{DC} = \left(\frac{m_{accessed\ by\ AU}}{m}\right) * 100 \qquad (9)$$

Where, $Rate_{DC}$ represents the data confidentiality rate, 'm'' indicates the number of cloud data, $m_{accessed\ by\ AU}$ is the number of cloud (%). Therefore, the data confidentiality rate is measured in percentage data accessed by the authorized users Higher the data confidentiality rate, the method is said to be more efficient.

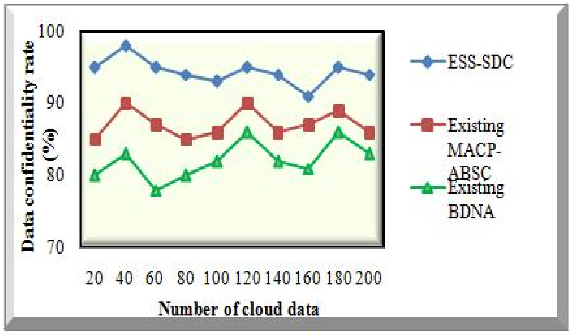

Figure 7 Comparative results of data confidentiality rate

Figure 7 depicts the comparative analysis of data confidentiality rate using three methods. As shown in figure, the different results of the data confidentiality rate are found to be improved using proposed ESS-SDC method than the other two existing methods. This is because of the proposed ESS-SDC method efficiently performs both encryption and signature generation for hiding the data from the unauthorized access. In addition, the proposed technique also performs the identity authentication for verifying the accessed users is authorized or unauthorized. Then the signature verification is also used for improving the data confidentiality. If the signature generated by data owner and existing signature get matched, then the original data is obtained by the cloud users. Otherwise, the data are not accessed by the users. This process of proposed ESS-SDC method improves the data confidentiality rate. The results of proposed ESS-SDC method are compared to the existing methods. The average of ten results shows that the data confidentiality rate is said to be improved by 8% using proposed ESS-SDC method as compared to MACP-ABSC [1] and 15% when compared to BDNA [2].

4.3 Impact of processing time

Processing time is defined as an amount of time taken by the algorithm to perform secure data transaction from server to the cloud users. The time is calculated with the number of cloud data which is given below.

$$PT = m * T(d_t) \quad (10)$$

Where, PT indicates the processing time, m represents the number of cloud data, T denotes a time for secure data access from server. Lesser the processing time, the method is said to be more efficient.

Sample mathematical calculation

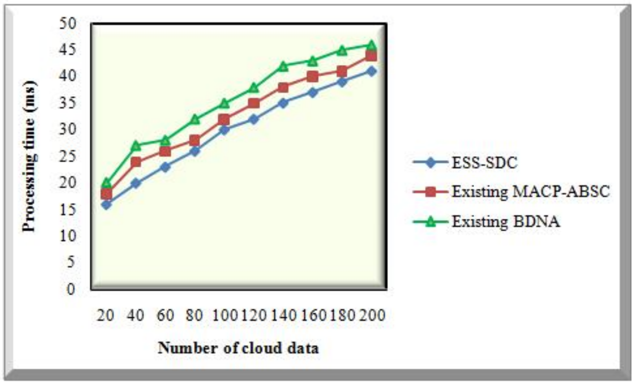

Figure 8 : Comparative results of processing time

Figure 8 depicts the comparative analysis of processing time using three methods. The processing time is to take the amount of time taken for performing the secured data access from the cloud server. The above graphical result clearly illustrates that the processing time is considerably minimized using ESS-SDC method when compared to other methods. This is because of the ESS-SDC method generates the key pair for each user and performs both signature generations as well as the data encryption. Therefore, the proposed signcryption method minimizes the processing time and improves the transaction security in cloud. Let us consider the 20 cloud data, the processing time of secured data access is $16ms$ using ESS-SDC method whereas the processing time of other and MACP-ABSC [1] and BDNA [2] are $18ms$ and $20ms$ respectively. Totally ten various results are obtained and compared to the other two existing methods. The comparison results prove that ESS-SDC method considerably reduces the processing time by 9% and 17% when compared to MACP-ABSC [1] and BDNA [2] respectively.

From the above discussion, the performance of the proposed ESS-SDC method effectively performs the secure data transaction with higher confidentiality, authentication accuracy and minimum processing time.

5. CONCLUSION

An efficient cryptography technique called ESS-SDC method is developed for secure data transaction in cloud with minimum time. The secure data transaction from server to cloud user is done by applying Ephemeral Schnorr Signcryption. The user wants to access the data from the cloud server and the data owner verifies the authenticity for improving the security in cloud. The signature generation and encryption is used to hide the data from the unauthorized user for achieving the higher data confidentiality. Then the receiver decrypts the cipher text and obtains the original data only the digital signature is valid at the time of verification. Experimental evaluation is performed using Amazon access sample dataset with different parameters such as authentication accuracy, Data confidentiality rate and processing time. The discussed results analysis confirms the ESS-SDC method achieves higher data confidentiality rate, authentication accuracy with minimum processing time than the state-of-art methods.

REFERENCES

[1] Qian Xu , Chengxiang Tan , Zhijie Fan ,Wenye Zhu, Ya Xiao , Fujia Cheng, “Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption”, IEEE Access , Volume 6, 2018, Pages 34051 – 34074

[2] Manreet Sohal and Sandeep Sharma, “BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing”, Journal of King Saud University - Computer and Information Sciences, Elsevier, 2018, Pages 1-9

[3] Guofeng Wang , Chuanyi Liu , Yingfei Dong , Peiyi Han ,Hezhong Pan , Binxing Fang, “IDCrypt: A Multi-User Searchable Symmetric Encryption Scheme for Cloud Applications”, IEEE Access ,Volume 6, 2017, Pages 2908 – 2921

[4] Niharika Singh and Ashutosh Kumar Singh, “Data Privacy Protection Mechanisms in Cloud”, Data Science and Engineering, Springer, Volume 3, Issue 1, 2018, Pages 24–39

[5] Suyel Namasudra, “An improved attribute-based encryption technique towards the data security in cloud computing”, Concurrency Computation Practice Experience, Wiley, Volume 31, Issue 3, 2019, Pages 1-15

[6] Nurmamat Helil1, and Kaysar Rahman, “CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy”, Security and Communication Networks, Hindawi, Volume 2017, September 2017, Pages 1-13

[7] Smarajit Ghosh and Vinod Karar, “Blowfish Hybridized Weighted Attribute-Based Encryption for Secure and Efficient Data Collaboration in Cloud Computing”, Applied Science Volume 8, Issue 7, 2018, Pages 1-15

[8] B. B. Gupta and Megha Quamar, “An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards”, Procedia Computer Science, Volume 132, 2018, Pages 189–197

[9] Chenyu Wang, Ke Ding, Bin Li, Yiming Zhao, Guoai Xu, Yanhui Guo, and Ping Wang, “An Enhanced User Authentication Protocol Based on Elliptic Curve Cryptosystem in Cloud Computing Environment”, Wireless Communications and Mobile Computing, Hindawi, Volume 2018, October 2018, Pages 1-13
https://doi.org/10.1155/2018/3048697

[10] Jianghong Wei , Wenfen Liu, Xuexian Hu, “Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption”, IEEE Transactions on Cloud Computing (Volume 6 , Issue 4 , 2018 , Pages 1136 – 1148

[11] K. Rajesh Rao, Indranil Ghosh Ray ,Waqar Asif, Ashalatha Nayak , Muttukrishnan Rajarajan, “R-PEKS: RBAC Enabled PEKS for Secure Access of Cloud Data”, IEEE Access , Volume 7, 2019, Pages 133274 – 133289

[12] Sana Belguith, Nesrine Kaaniche, Mohammad Hammoudeh, Tooska Dargahi, “PROUD: Verifiable Privacy-preserving Outsourced Attribute Based SignCryption supporting access policy Update for cloud assisted IoT applications”, Future Generation Computer Systems, Elsevier, 2019, Pages 1-23

[13] Yinghui Zhang, Jin Li, Xiaofeng Chen, Hui Li, “Anonymous attribute-based proxy re-encryption for access control in cloud computing”, Security And Communication Networks, Volume 9, Issue 14, 2016, Pages 2397-2411

[14] Vinod Kumar, Musheer Ahmad, Adesh Kumari, “A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol for Cloud-assisted TMIS”,

Telematics and Informatics, Elsevier, Volume 38, 2019, Pages 100-117

[15] Durbadal Chattaraj, Monalisa Sarma, Ashok Kumar Das, "A new two-server authentication and key agreement protocol for accessing secure cloud services", Computer Networks, Elsevier, Volume 131, 2018, Pages 144-164

[16] Mang Su, Liangchen Wang, Anmin Fu, Yan Yu, "Proxy Re-Encryption Based Multi-Factor Access Control for Ciphertext in Cloud", Journal of Shanghai Jiaotong University (Science), Springer, Volume 23, Issue 5, 2018, Pages 666–670

[17] Jongkil Kim and Surya Nepal, "A Cryptographically Enforced Access Control with a Flexible User Revocation on Untrusted Cloud Storage", Data Science and Engineering, Springer, Volume 1, Issue 3, 2016, Pages 149–164 https://doi.org/10.1007/s41019-016-0014-0

[18] orteza Amini and Farnaz Osanloo, "Purpose-Based Privacy Preserving Access Control for Secure Service Provision and Composition", IEEE Transactions on Services Computing, Volume 12 , Issue 4 , 2019, Pages 604 – 620

[19] Shilpi Harnal and R.K. Chauhan, "Hybrid Cryptography based E2EE for Integrity & Confidentiality in Multimedia Cloud Computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume 8 Issue 10, 2019, Pages 918-924

[20] Xiong Li, Saru Kumari, Jian Shen, Fan Wu, Caisen Chen, SK Hafizul Islam, "Secure Data Access and Sharing Scheme for Cloud Storage", Wireless Personal Communications, Springer, Volume 96, Issue 4, 2017, Pages 5295–5314 https://doi.org/10.1007/s11277-016-3742-6

[21] Amazon access sample dataset: https://archive.ics.uci.edu/ml/datasets/Amazon+Access+Samples#

(Author[1] Institutional Journal Communication Number: Dr. NGPASC 2020-21 CS002)