CONGRUENCE COEFFICIENT EPHEMERAL NIEDERREITER CRYPTOGRAPHY FOR SECURED AND PRIVACY PRESERVED DATA TRANSMISSION IN CLOUD

R.Krishnaveni[a] and Dr.S.Shakila[b]

[a]Guest Lecturer,Department of Information Technology,Government Arts and Science college,Kumulur,Lalgudi,
Trichy-621 712,Tamil Nadu,India.
E-mail:krishnavenirajagopal13@gmail.com
[b]Assistant Professor and Head,Department of Computer Science,Government Arts College,
Trichy-620 022,Tamil Nadu,India.
E-mail:shakilamuthusamy@gmail.com

ABSTRACT

Cloud computing is the process of utilizing the hardware and software to deliver various services over the network.Due to the huge development of big data that exists in the cloud servers, security and privacy are two fundamental factors about cloud technology. Cloud security is a vital concern for cloud storage services. Cloud data security is the process of protecting the data stored in the server from unauthorized access. Many researchers carried out their research on secured data communication in the cloud. But, the data confidentiality was not improved and encryption time was not minimized. A novel Congruence coefficient Ephemeral Niederreiter Cryptography-based Secured and Privacy Preserved Data Transmission (CCENC-SPPDT) technique is introduced for improving data confidentiality in a cloud environment. CCENC-SPPDT technique comprises four processes, namely key generation, authentication, encryption, and decryption for improving the security and privacy during the patient data transmission in the cloud. In the CCENC-SPPDT technique, the cloud user (i.e., patient) registers detail to the cloud server (CS) (i.e., hospital) for performing the secured patient data communication. After registration, CS generates the ephemeral key pair (i.e., the ephemeral public key and ephemeral private key) in the key generation step for every registered cloud user. After receiving the ephemeral key pair, the cloud user encrypts the data with the ephemeral public key and transmits the encrypted patient data to the cloud server. When a cloud user needs to access the stored patient data from CS, the cloud user sends a request message to CS. After receiving the request, CS verifies the cloud user authenticity through the Congruence similarity coefficient with the dynamic session password. The authorized user allows accessing the data from the cloud server. Finally, patient data gets decrypted with the ephemeral private key of the cloud user. In this way, the patient data gets preserved from unauthorized access for improving the security level and data integrity by using the CCENC-SPPDT technique. Experimental evaluation is carried out on factors such as encryption time, data confidentiality rate, and data integrity with respect to a number of patient data.

Keywords: Cloud computing, Secured and Privacy Preserved Data Transmission, Ephemeral Niederreiter Cryptography, Congruence similarity coefficient

1. INTRODUCTION

Cloud computing offers cost-effective and powerful data storage and executive service through the Internet. With the rapid growth of information and communication, data security and trusted computing is still the major challenges in recent cloud computing applications. Recently, cloud computing is applied in the healthcare applications system that permits the data transmission of patient health records through a portal designated by a healthcare specialist. A patient's health data are centrally stored in the cloud server and is shared with numerous healthcare stakeholders. During the data transmission, several issues, including data security and privacy concerns remain unresolved.

A robust and lightweight, secure access scheme was introduced in (1) for cloud-based electronic healthcare services. The designed scheme avoiding unauthorized users accessing the health-related information stored in the cloud.Therefore the designed scheme reveals the security property of data confidentiality but the higher integrity rate was not attained. A Cloud-Based Secure and Efficient Framework (CSEF) was designed in (2) for Medical systems using elliptic curve cryptography (ECC). The designed framework minimizes the computation and communication cost but the data confidentiality rate was not improved.

A novel cloud-based user authentication system was introduced in (3) to improve the secure authentication of medical data. However, the designed system failed to offer the better performance of the security. Secure Authentication and Data Sharing in Cloud (SADS-Cloud) was introduced in (4) for improving privacy and data security with big data sharing. However, the method failed to further speed up the encryption and decryption process.

Ciphertext policy attribute-based encryption (CP-ABE) method was introduced in (5) to offer fine-grained access control for enhancing privacy and security. The designed method reduces the computation time but accurate authentication was not performed. A Multi-Scheme Privacy-Preserving Deep Learning method was introduced in (6) to reduce the communication and computational cost. But, the method failed to consider the authentication for improving the confidentiality of data access in the cloud. An Escrow-Free Identity-based Aggregate SignCryption (EF-IDASC) method was developed in (7) to perform secure data transmission. However, the computation cost of secure data transmission was not reduced.

A lightweight and privacy-preserving medical services access approach were introduced in (8) for the healthcare cloud. The approach was used to apply on large-scale remote medical services and minimizes the storage overhand but the authenticity verification was not performed. The blockchain integrated with attribute-based signcryption was introduced in (9) for enhancing secure data distribution. It provides secure data confidentiality but the integrity was not improved.

A blockchain-assisted verifiable outsourced attribute-based signcryption method (BVOABSC) was introduced in (10) for the secure distribution of health records. Though the method reduces the time cost, the performance of the confidentiality rate was not improved.

1.1 Contributions

The novel contributions of the CCENC-SPPDT technique are summarized as given below,

- To improve the security of the medical data transmission in cloud-based architecture, a novel technique CCENC-SPPDT is introduced with different phases namely the Registration phase, encryption phase, authentication phase, and decryption phase.
- Ephemeral Niederreiter Cryptographic technique is applied in CCENC-SPPDT to generate the pair of the Ephemeral keys for each registered user to encrypt and decrypt the patient data. Initially, the patient data are encrypted and stored in the cloud server.
- To improve the authentication accuracy, CCENC-SPPDT uses the Congruence similarity coefficient for authenticating the users to avoid unauthorized data access and modification. This helps to improve the confidentiality and integrity rate of data transmission.
- Finally, widespread experiments are performed to evaluate the performance of our CCENC-SPPDT and other related security works. The estimated result reveals that our CCENC-SPPDT technique outperforms well than the conventional security methods.

1.2 Paper organization

The remaining paper is arranged into different sections as follows: Section 2 discusses the literature review of existing security mechanisms whereas Section 3 presents the system model of the proposed technique with different processes. Section 4 describes the experimental setup with the medical dataset. Section 5 provides the security and comparative analysis followed by conclusions in Section 6.

2. LITERATURE REVIEW

A secure and privacy-preserving distributed deep learning (SPDDL) method was introduced in (11) to preserve the users' privacy and an authentication scheme. However, the system failed to construct more efficient cryptography schemes for improving security. A bilinear key aggregate cryptography technique is introduced in (12) tooffer the security of data communication with lesser computation complexity. But the technique failed to guarantee data integrity.

A blockchain-based ciphertext-policy attribute-based encryption method was introduced in (13) for cloud data secure distribution. However, the data integrity rate was not improved by attribute-based encryption architecture. A blockchain-based integrity protection approach was introduced in (14) to minimize the storage overhead and time overhead. But the method was not efficient to perform the authentication.

A secured and dependable architecture was designed in (15) for electronic health information to guarantee efficiency. But this structural design was not efficient to build a secured, dynamic and reliable approach for E-Health. An efficient and secure sharing of data was introduced in (16) for improving the security of collaborative health data. However, data confidentiality and integrity verification of collaborative health data were not performed.

A revocable-storage hierarchical attribute-based encryption (RS-HABE) system was presented in (17) for improving the secure data distribution of health data. However, the encryption time consumption was not minimized. A novel lightweight cryptographic algorithm was introduced in (18) to improve the data security applications on cloud computing. But, the data confidentiality level was not improved by a lightweight cryptographic algorithm. The lattice-based access policy method was developed in (19) for access control. However, it failed to consider the very bigger size of patient's records.

Elliptical Curve Certificateless Aggregate Cryptography Signature method (EC-ACS) was introduced in (20) to improve the security of health records using the authorized blockchain method. The designed method reduces the computation cost but the data confidentiality rate was not improved.

3. PROPOSAL METHODOLOGY

Cloud computing is a modern paradigm in digital technology and is being widely applied in the healthcare industry. It is a computing technology that provides efficient storage of medical information but also helps to provide the easy exchange or transmission of health data. Besides, cloud computing technology also helps to store, manage, protect, and distribute patient health records, laboratory data, pharmacy data, and medical images. The main problems of the cloud by healthcare providers are security, confidentiality, and trust issues. A variety of privacy maintaining approaches to promise the privacy and security of health records in the cloud. But the higher levels of security are needed to prevent the patient confidential data from unauthorized access to the healthcare system. Based on motivation, a novel CCENC-SPPDT technique is introduced.

3.1 System model

In this section, the system model of the CCENC-SPPDT technique is presented based on the cloud-based infrastructure. Cloud computing architecture is a promising technology that helps to improve security in the healthcare industry.

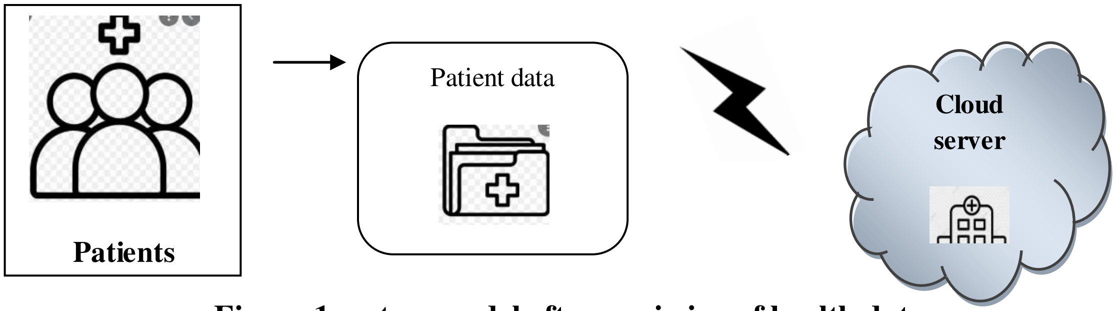

Figure.1 system model oftransmission of health data

Figure 1 given above illustrates the system model of transmission of health data in a secure manner. The cloud computing architecture comprises two entities such as cloud users (i.e. patients) and cloud servers (i.e. hospital). The cloud users $P_1, P_2, P_3 \ldots\ldots P_n$ who has the data $pd_1, pd_2, pd_3, \ldots. pd_m$to be stored in the cloud server 'CS' provides the cloud storage services in a secured manner. The proposed technique consists of major processes namely registration, encryption, authentication, and decryption. These processes are explained in the following subsections.

3.2 Congruence coefficientEphemeral Niederreiter Cryptographic Secured and Privacy Preserved Data Transmission in Cloud

A novel CCENC-SPPDT technique is introduced for improving data confidentiality in a cloud environment. In the CCENC-SPPDT technique, the EphemeralNiederreiter Cryptography is public-key cryptography. On the contrary to the conventional Cryptography technique, Ephemeral keys are encryption keys that are generated randomly and used for a certain amount of time. This helps to avoid unauthorized users from accessing the data.

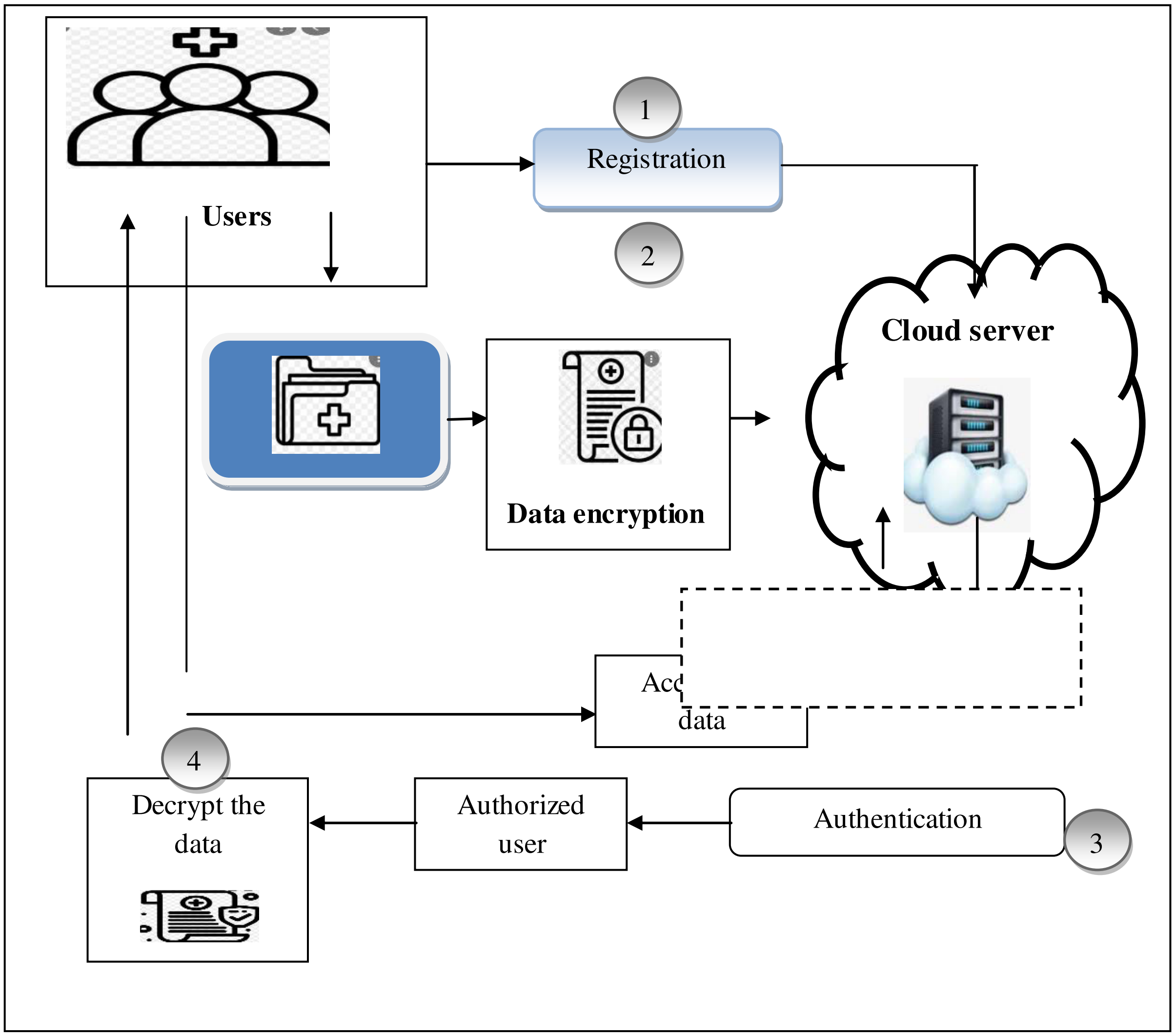

Figure 2 demonstrates the architecture diagram of the proposed CCENC-SPPDT technique to offer secure data communication in the cloud. The architecture consists of four major processes namely registration, encryption, authentication, and decryption. These processes are explained in the following subsections.

3.2.1 Registration

At first, the proposed CCENC-SPPDT technique starts to perform the registration before storing the data into the cloud server. Let us consider the healthcare application to securely store the patient data into the server. For each user in the cloud server, they first need to perform the registration which is provided by the cloud server. During the registration phase, the patient personal information such as original name, middle name, last name, date of birth, gender, mobile number, age, height, weight, and so on. It also includes information regarding their past and current health or illness, treatment history, and so on.

After the registration, the cloud server generates the pair of Ephemeral keys for each registered user. The pair of keys is generated using the Ephemeral Niederreiter Cryptographic technique.

$$b_k = (R, m) \quad (1)$$

$$R = WKV \quad (2)$$

$$P_k = (W, K, V) \quad (3)$$

Where, P_k denotes a private key, b_k denotes a public key, W denotes a binary non-singular matrix, K denotes a parity check matrix, V denotes a permutation matrix, m denotes a weight. In this way, different pairs of Ephemeral keys are generated for all the registered users in the cloud.

3.2.2 Ephemeral Niederreiter Encryption

In the CCENC-SPPDT technique, data encryption is the method of encrypting data before transferring it from one place to another over the network. It is a significant process in healthcare applications because unauthorized people (hackers) have access to patient information, which creates a data problem. Besides, the data is stolen during the transfer to the cloud server (i.e. hospital). Therefore, the CCENC-SPPDT technique uses the Ephemeral Niederreiter Encryptionmethodin healthcare systems for guaranteeing security in the cloud. Ephemeral Niederreiter Encryptionis an asymmetric key cryptographic algorithm that uses a pair of related keys such as public key and private key. To hide the patient data from unauthorized access or use, encryption is performed using the receiver public key.

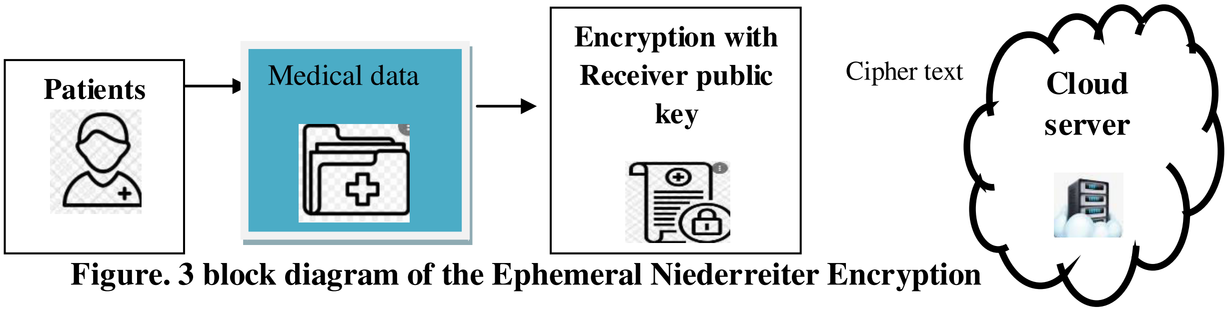

Figure. 3 block diagram of the Ephemeral Niederreiter Encryption

Figure 3 depicts the block diagram of the Ephemeral Niederreiter Encryption process to improve the security of data transmission in the cloud. Let us consider the patient data$pd_1, pd_2, pd_3, \dots . pd_m$. The input data is encoded into a string of bits ($s_i = s_1, s_2 .. s_m$). The patient data is encrypted with the receiver public key is given below,

$$\rho_c = R\ s^T \quad (4)$$

Where, ρ_c denotes a ciphertext, s denotes a bit of data, T denotes a transpose, R denotes an Ephemeralpublic key. The equation (4) is used to obtain the ciphertext of the message bit 's'.

3.2.3 Congruence coefficient based authentication

When cloud user needs to access the stored patient data from the cloud server, they first need to verify their authenticity. After receiving the request, the cloud server verifies the cloud user authenticity by sending the dynamic session password.

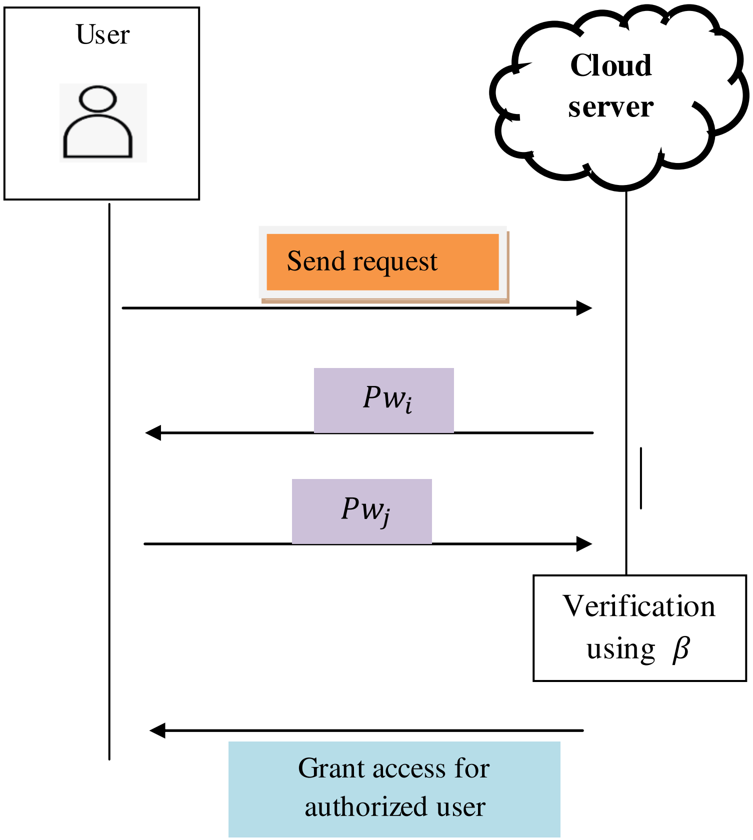

Figure. 4 flow process of the authentication

Figure 4 displays the authentication process of each user in the cloud. The cloud user sends a request message to the server. After receiving the request, the cloud server sends the dynamic session password (Pw_i). If cloud user-entered password (Pw_j) gets matched with server sent a password, then the cloud user is said to be an authorized user and allowed to access the data from the cloud server. The dynamic session password is matched through the

Congruence coefficient. Congruence coefficient is a similarity index used for verifying the dynamic session password. The congruence correlation is measured as follows,

$$\beta = \frac{\sum Pw_i * Pw_j}{\sqrt{\sum Pw_i^2 \sum Pw_j^2}} \quad (5)$$

Where,β indicates congruence similarity coefficient, $\sum Pw_i * Pw_j$ indicates a sum of the product of paired score of two session passwords, $\sum Pw_i^2$ symbolizes a squared score of Pw_i and $\sum Pw_j^2$ signifies a squared score of Pw_j. The congruence correlation coefficient (β) provides the values between '-1' and '+1'. If the similarity coefficient provides '+1' indicates a two-session password is correctly matched and then the user is said to be an authorized user. Otherwise, it provides '-1', and then the user is said to be an unauthorized user.

3.2.4 Ephemeral Niederreiter Decryption

After the cloud user authentication, Ephemeral Niederreiter Decryptionis performed by the authorized user to obtain the original patient data. The decryption is performed with the private key also known as a secret key.

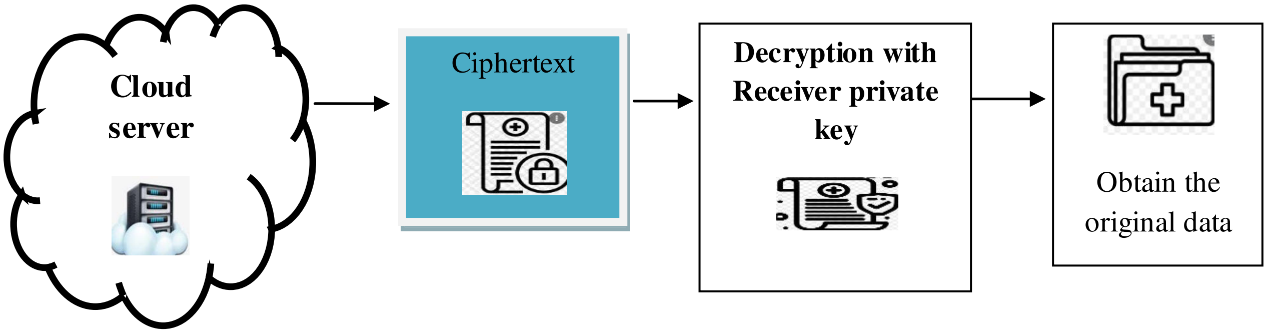

Figure. 5 block diagram of the Ephemeral Niederreiter decryption

Figure 5 depicts the block diagram of the Ephemeral Niederreiter decryption process to obtain the original data. The decryption is performed with the Ephemeral private key. The original bit message $\{0,1\}$ is obtained as given below. First, the receiver computes,

$$W^{-1}\rho_c = K\ V\ s^T \quad (6)$$

Where W denotes a binary non-singular matrix, K denotes a parity check matrix, V denotes a permutation matrix,ρ_c denotes ciphertext, s denotes a bit of data, T denotes a transpose. By applying the error correction algorithm (i.e. syndrome decoding), the error patterns $e = V\ s^T$ is obtained. Then the original plaintext is obtained as follows,

$$s\ via\ \ s^T = V^{-1}V\ s^T (7)$$

Where s denotes an original bit of the patient data. In this way, secure patient data transmission is performed with higher security. As a result, the confidentiality of the data transmission gets improved. The algorithmic process of the CCENC-SPPDT technique is described as given below,

// Algorithm 1 Congruence coefficient Ephemeral Niederreiter Cryptography based Secured and Privacy Preserved Data Transmission

Input: cloud users $P_1, P_2, P_3 \ldots\ldots P_n$ and data $pd_1, pd_2, pd_3, \ldots.pd_m$, cloud server 'CS'
Output: Secured Data Transmission

```
Begin
// Registration
For each patient $P_i$
    $CS$ ask to enter thepatient details
    $CU$ enters their details and send to '$CS$'
    Servergenerates the pair of Ephemeral keys $P_k$, $b_k$
end for
\\data encryption
For each patient data $pd_i$
    Divide into a bit of strings$s_i = s_1, s_2 .. s_m$
    Encrypt the string with the public key
    Obtain the ciphertext '$\rho_c$'
End for
\\ User authentication
User login into the system with dynamic session password
$CS$ verifies the dynamic session password using a similarity measure
if $(\beta = 1)$ then
    The user is said to be an authorized
else
    The user is said to be an unauthorized
end if
//decryption
For each ciphertext '$v_i$'
    Decrypt the data with an Ephemeral private key
    Obtain the plain text
end if
```

Algorithm 1 given above describes the step-by-step process of Congruence coefficient Ephemeral Niederreiter Cryptography-based secure data transmission in the cloud. For each user register their details to the cloud server. In the registration phase, the user sends their details to the cloud server. Consequently, the server generates a pair of Ephemeral keys for registered users. Whenever the cloud user wants to access the stored data, the cloud server first verifies the authenticity of the user using the Congruence similarity coefficient. The coefficient returns '+1' and then the user is said to be an authorized user. Otherwise, the user is said to be an unauthorized user. Finally, the authorized user receives the original data. This helps to increase data confidentiality.

4 EXPERIMENTAL SETTINGS

Experimental evaluation of proposed CCENC-SPPDT and existing method Robust and lightweight, secure access scheme (1), CSEF (2) is implemented using Java language with CloudSim simulator. To conduct the experimentation, the medical Dataset called Cardiovascular Disease dataset is taken from the kagglehttps://www.kaggle.com/sulianova/cardiovascular-disease-dataset for secure data transmission on the cloud server. The dataset comprises 70,000 records of patient's data and12 features such as age, height, weight, gender, Systolic blood pressure, Systolic blood pressure, Cholesterol, Glucose, Smoking, Alcohol intake, Physical activity, Presence or absence of cardiovascular disease. These data are used to perform secure communication in a cloud environment.

5 COMPARATIVE PERFORMANCE ANALYSIS

In this section, the performance of the proposed CCENC-SPPDT and existing Robust and lightweight, secure access scheme (1), CSEF (2) are discussed with respect to a number of metrics such as confidentiality rate, integrity rate, authentication accuracy, and time.

5.1 Data confidentiality rate

Confidentiality rate is one of the significant parameters that are measured as the ratio of a number of patient data is protected from unauthorized access. The confidentiality rate of patent data is calculated as given below,

$$CR = \left[\frac{PDP}{NPD}\right] * 100 \quad (8)$$

Where CR denotes a confidentiality rate, PDP indicates the number of patient data protected, NPD denotes the number of patient data. Therefore, the confidentiality rate is measured in the unit of percentage (%).

Table .1. Performance results of confidentiality rate

Number of patient data	Confidentiality rate (%)		
	CCENC-SPPDT	Robust and lightweight secure access scheme	CSEF
100	91	88	85
200	90	87	84
300	89	85	82
400	91	88	85

500	90	87	84
600	89	86	83
700	91	87	84
800	90	86	85
900	92	88	86
1000	91	87	85

Table 1 given above illustrates the performance of data confidentiality rate versus the number of patient data taken in the ranges from 100 to1000. The patient data are taken from the Cardiovascular Disease dataset. The data confidentiality rate is measured during the data transmission from user to cloud server. The confidentiality rate of the patient data transmission is estimated as the ratio of the number of data accessed by an authorized user. As shown in Table 1, the confidentiality rate of the proposed CCENC-SPPDT is higher than the Robust and lightweight secure access scheme (1), CSEF (2). Let us consider 100 patient data to calculate the data confidentiality. By applying the CCENC-SPPDT, 91 patient data are correctly accessed by the authorized user and the data confidentiality rate is 91%. Whereas, the data confidentiality rate of Robust and lightweight secure access scheme (1), CSEF (2) are 88% and 85% respectively. For each method, the ten various results are observed with different counts of the input patient data. After getting the ten various results, the results of CCENC-SPPDT are compared to the results of existing methods. Finally, the average is taken for the comparison results. The comparison value is taken into consideration of the final results. The final result shows that the data confidentiality rate of CCENC-SPPDT is increased by 4% when compared to (1) and 7% when compared to (2) respectively.

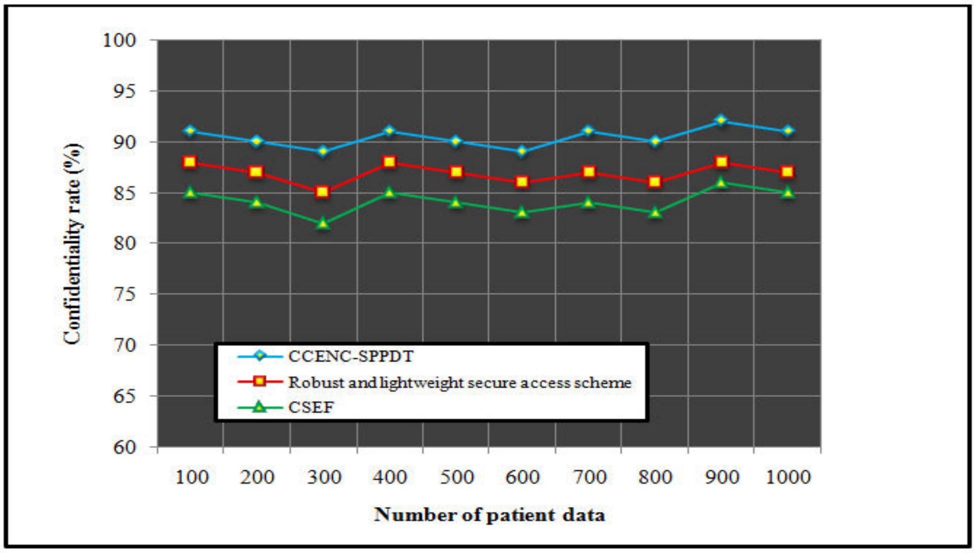

Figure. 6 graphical illustration of confidentiality rate

Figure 6 graphical illustration of confidentiality rate versus a number of patient's data taken in the ranges from 100 to 1000. As shown in the graphical plot, the confidentiality rate of CCENC-SPPDT is represented by a blue-colored line whereas the confidentiality rate of the existing Robust and lightweight secure access scheme (1), CSEF (2) are represented by red and green color respectively. The number of patient data is taken as input in the 'x' axis and the results of confidentiality rate are observed at the 'y' axis. Among three methods, the CCENC-SPPD outperforms well. The major reason is to apply the Ephemeral Niederreiter Cryptographic technique in CCENC-SPPD. The Cryptographic technique performs encryption and decryption with help of Ephemeral public and private keys. This helps to avoid unauthorized users and access the legitimate users in the hospital such as doctors, patients, and nurses. This process helps to increase the data confidentiality rate.

5.2 Data integrity rate

It is another important security performance metric that helps to measure the ratio of the number of patient data that are not modified by unauthorized users. The patientdata integrity of the data transmissions is formulated as given below,

$$IR = \left[\frac{PDNM}{NPD}\right] * 100 \quad (9)$$

Where IR indicates an Integrity Rate, $PDNM$ denotes patient data not modified by an authorized user, NPD denotes the number of patient data. The integrity rate is measured in terms of percentage (%).

Table. 2. Performance results of Integrity rate

Number of patient data	**Integrity rate (%)**		
	CCENC-SPPDT	**Robust and lightweight secure access scheme**	**CSEF**
100	90	87	84
200	89	85	83
300	88	83	81
400	90	87	84
500	89	86	83
600	88	83	81
700	90	85	83
800	89	86	82
900	91	87	84
1000	90	86	83

Table 2 portrays a clear comparison of the previous and the proposed CCENC-SPPDT. The integrity rate of the proposed and existing methods is estimated based on the number of patient data in the ranges from 100 to 1000. As shown in the observed results, the proposed CCENC-SPPDT achieves better performance in the integrity calculation. As shown in the table value, the data integrity rate of CCENC-SPPDT is 90% and the data integrity rate of existing Robust and lightweight secure access schemes (1), CSEF (2) is 87% and 84% respectively by considering the 100 patient data. Similarly, nine remaining data integrity rates are observed for each method. Totally, ten integrity results are observed and the results are compared. The average of ten comparison results indicates that the data integrity rate of CCENC-SPPDT is improved by 5% and 8% when compared to existing (1) (2) methods respectively.

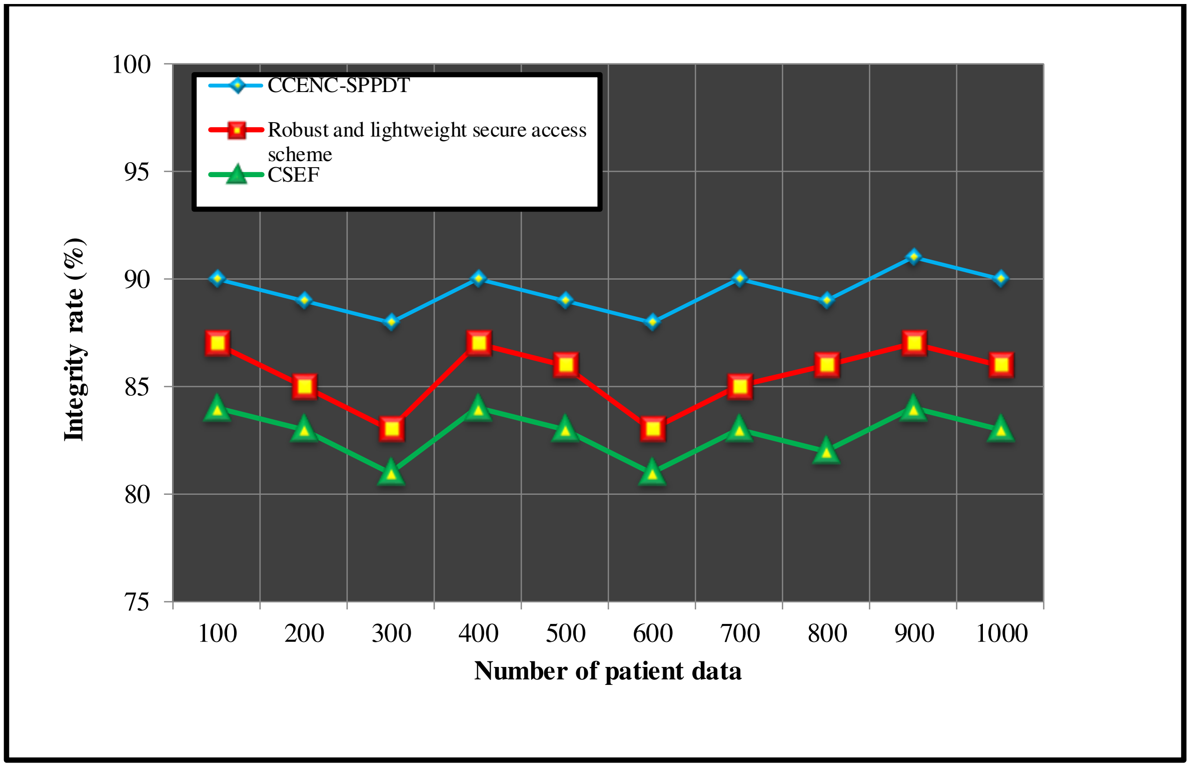

Figure. 7 graphical illustration of integrity rate

Figure 7 illustrates the comparative analysis on integrity rate using three different security mechanisms namely CCENC-SPPDT, Robust and lightweight secure access scheme (1), CSEF (2). Therefore, the experimental results reveal that the proposed CCENC-SPPDT is better and well than all other existing ones. The reason behind the CCENC-SPPDT performs encryption and decryption. The original patient data gets encrypted and obtain the ciphertext. This ciphertext of the data is transmitted into a cloud server. This process helps to avoid data modification. As a result, the integrity rate of CCENC-SPPDT is improved.

5.3 *Authentication accuracy*

Authentication accuracyis measured as the ratio of the number of users that are correctly authenticated as authorized or unauthorized users in the cloud. The formula for calculating the authentication accuracy is formulated as given below,

$$Accuracy = \left(\frac{NUCA}{n}\right) * 100 \quad (10)$$

Where $NUCA$ denotes the number of users correctly authenticated, 'n' represents the number of cloud users. Therefore, the overall accuracy is measured in terms of percentages (%).

Table. 3. Performance results of Authentication accuracy

Number of cloud users	Authentication accuracy (%)		
	CCENC-SPPDT	Robust and lightweight secure access scheme	CSEF
50	88	86	84
100	90	87	85
150	91	86	84
200	90	87	85
250	91	88	86
300	92	87	85
350	93	89	84
400	92	88	86
450	93	90	87
500	92	89	86

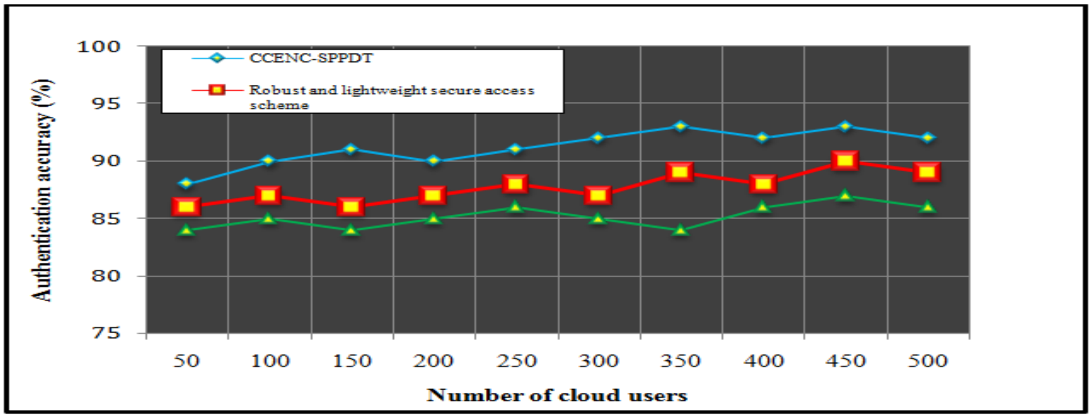

Figure. 8 graphical illustration of authentication accuracy

Table 3 and figure 8 indicate the performance analysis of authentication accuracyof CCENC-

SPPDT, Robust and lightweight secure access scheme (1), CSEF (2). The observed outcome of three security mechanisms helps to validate that the authentication accuracyis found to be higher using the CCENC-SPPDT than the other existing methods. This is proved through the statistical measure. In the first run, the experiment is conducted with 50 cloud users, 44 users are correctly authenticated as authorized users or unauthorized users and the authentication accuracyis 88%. In addition, 86 and 84 users are correctly authenticated and authentication accuracy is 86% and 84% using (1)(2) respectively. Likewise, various results are observed and different results are attained. Therefore, the overall authentication accuracyof the CCENC-SPPDT technique is compared to the other two methods. The average of ten various results noticeably proved that the authentication accuracyis considerably increased using CCENC-SPPDT technique by 4% and 7% when compared to existing (1), (2) respectively.

The CCENC-SPPDT uses Congruence Coefficient-based user authentication. When a cloud user wants to access the stored patient data from a cloud server, the user sends a request message server. After receiving the request, the server verifies the cloud user authenticity based on the dynamic session password. The Congruence Coefficient accurately finds the authorized and unauthorized users. As a result, the authentication accuracy gets increased.

5.4 Computation time

Computation time is defined as the amount of time taken by an algorithm to perform secure patient data transmission. The overall time consumption for secure data transmission is expressed as follows,

$$CT = N * t\,[STD] \quad (11)$$

Where CT denotes a computation time, N denotes the number of patient data, 't' represents the time, STD denotes a securely transmits the data. Therefore, the overall computation time is measured in terms of milliseconds (ms).

Table. 4. Performance results of Computation time

Number of patient data	**Computation time (ms)**		
	CCENC-SPPDT	**Robust and lightweight secure access scheme**	**CSEF**
100	17	19	22
200	22	24	26
300	26	28	33
400	28	33	36

500	32	35	38
600	35	38	42
700	39	41	44
800	42	46	49
900	47	50	54
1000	51	53	56

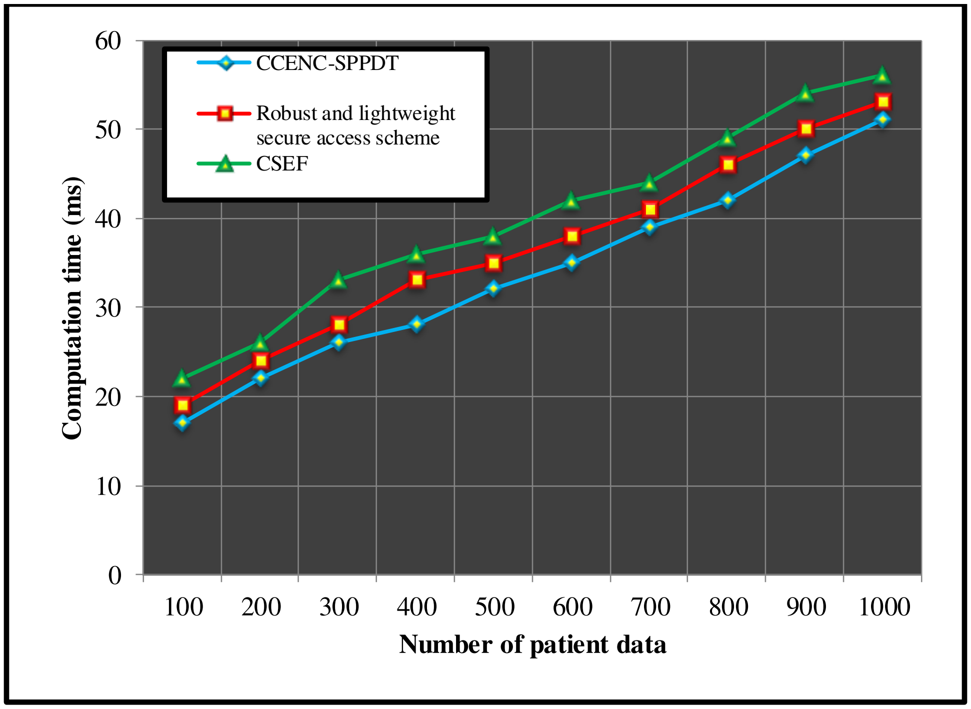

Figure. 9 graphical illustration of computation time

Table 4 and figure 9 illustrate the results of graphical illustration of computation time versus a number of patient data taken in the range from 100 to 1000. The attained experimental assessment results demonstrate the computation time of all three methods gets increased while increasing the number of patient data. But comparatively the CCENC-SPPDT consumes lesser time for the secure transmission of patient data. This is confirmed by the statistical example. With '100' patient data taken as input, the CCENC-SPPDT consumes '$17ms$' of time to perform secure data transmission. Similarly, the other two existing methods Robust and lightweight secure access scheme (1), CSEF (2) consumes '$19ms$' and '$22ms$' of time consumption to perform the secure patient data transmission. The average of ten comparison results indicates that the overall computation time of the CCENC-SPPDT is considerably minimized by 8% and 16% when compared to existing methods. This is due to the application of the Ephemeral Niederreiter Cryptographic technique for efficiently performed the encryption and decryption with minimum time consumption.

6. CONCLUSION

Cloud-based secure healthcare services are becoming increasingly popular due to the simple availability and mobility of the patient's medical records. A novel CCENC-SPPDT is introduced to guarantee the security of patient data stored in the cloud server. The CCENC-SPPDT technique firstly performs the registration process. Then the server generates the par of private and public keys for each registered user. Then the Ephemeral Niederreiter encryption is performed with the public key and the patient data is stored into the cloud server in the form of ciphertext. When the user accesses the data, they first verify the authenticity through the Congruence similarity coefficient. Finally, the authorized user receives the original text through the Ephemeral Niederreiter decryption with the private key. This process helps to improve data confidentiality and integrity. Finally, the proposed CCENC-SPPDT is experimented with cloudsim to estimate the performance of authentication accuracy, confidentiality rate, integrity, and minimizing the computation time when compared to the state-of-the-art works.

REFERENCES

MehediMasud, Gurjot Singh Gaba, KaranjeetChoudhary, RoobaeaAlroobaea&ShamimHossain M., (2021). A
robust and lightweight secure access scheme for cloud-based E- healthcare services, *Peer-to-Peer Networking*
and Applications, Springer,1-15.

AdeshKumari, Vinod Kumar, YahyaAbbasi M., SaruKumari, PradeepChaudhary, Chien- Ming Chen (2020).
CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC, *IEEE Access,*
Volume 8, 107838 – 107852.

JangiralaSrinivas, Ashok Kumar Das, Neeraj Kumar, Joel J. P. C. Rodrigues (2020). Cloud Centric Authentication
for Wearable Healthcare Monitoring System, *IEEE Transactions on Dependable and Secure Computing,*
Volume 17, Issue 5, 942 – 956.

Uma Narayanan, Varghese Paul, Shelbi Joseph (2020). A novel system architecture for secure authentication and
data sharing in cloud enabled Big Data Environment, *Journal of KingSaud University – Computer and*
Information Sciences, Elsevier, 1-20.

Kennedy Edemacu, Beakcheol Jang, Jong Wook Kim (2020). Collaborative Ehealth Privacy and Security: An
Access Control With Attribute Revocation Based on OBDD Access IEEE Structure,*Journal of Biomedical and*
Health Informatics,Volume 24, Issue 10, 2960 – 2972.

Owusu-AgyemangKwabena, Zhen Qin, TianmingZhuang, Zhiguang Qin (2019). MSCryptoNet:Multi-Scheme Privacy-Preserving Deep Learning in Cloud Computing, *IEEE Access, Volume 7, 29344 – 29354.*

MahenderKumar, Satish Chand (2020). A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System With Public Verifiability, *IEEE Internet of Things Journal, Volume 7, Issue10, 10650 – 10659.*

Jingwei Liu, Huifang Tang, Rong Sun, Xiaojiang Du, Mohsen Guizani (2019). Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud, *IEEE Access, Volume 7, 106951 – 106961.*

NabeilEltayieb, RashadElhabob, Alzubair Hassan and Fagen Li (2020). A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud, *Journal of Systems Architecture, Elsevier, Volume 102, 1-28.*

Xiaodong Yang, Ting Li, Wanting Xi, Aijia Chen, Caifen Wang (2020). A Blockchain-Assisted IEEE Verifiable Outsourced Attribute-Based SigncryptionScheme for EHRs Sharing in the Cloud, Access, Volume 8, 170713 – 170731.

Yiran Li, Hongwei Li, GuowenXu, Tao Xiang, Xiaoming Huang and Rongxing Lu (2020). Towards Secure and Privacy-Preserving Distributed Deep Learning in Fog-Cloud Computing*, IEEE Internet of Things Journal, Volume 7, Issue 12,11460 – 11472*

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

YutingZuo, Zhaozhe Kang, JianXu and Zhide Chen (2021) .BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing,*International Journal of Distributed Sensor Networks, 1-16.*

PengCheng Wei, Dahu Wang, Yu Zhao, Sumarga Kumar SahTyagi, Neeraj Kumar (2020). Blockchain data-based
cloud data integrity protection mechanism, Future Generation Computer Systems, *Elsevier, Volume 102, 902-911*

NureniAyofeAzeez and Charles Van der Vyver (2019).Security and privacy issues in e-health cloud-based system:
A comprehensive content analysis, Egyptian Informatics Journal, *Elsevier, Volume 20, Issue 2, 97-108.*

Kennedy Edemacu, Beakcheol Jang, Jong Wook Kim, CESCR: CP-ABE for efficient and secure sharing of data in
collaborativeehealth with revocation and no dummy attribute, *PLoS , Volume 16, Issue 5, 1-24.*

Jianghong Wei, Xiaofeng Chen, Xinyi Huang, Xuexian Hu, Willy Susilo (2019). RS-HABE: Revocable-storage and
Hierarchical Attribute-based Access Scheme for Secure Sharing of e-Health Records in Public Cloud, *IEEE Transactions on Dependable and Secure Computing,1-15.*

FursanThabit, SharafAlhomdy, Abdulrazzaq H. A, Al-Ahdal, SudhirJagtap (2021). A new lightweight
cryptographic algorithm for enhancing data security in cloud computing, *GlobalTransitions Proceedings, Elsevier, Volume 2, 91-99.*

Saravanan N., Umamakeswari Dr. A., (2021). Lattice Based Access Control for Protecting UserData in Cloud
Environments with Hybrid Security, *Computers & Security, Elsevier, Volume 100, 2021, 1-22.*

Benil T., Jasper J., (2020). Cloud based security on outsourcing using blockchain in E-health systems,*Computer Networks, Elsevier, Volume 178, 2020, 1-13*