International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20 (2017) pp. 9515-9524

Bayes Certificateless Signcryption Based Secured Data Integrity for Cloud Service Provisioning

Densy John V.
Research Scholar, Department of Computer Science,
Karpagam Academy of Higher Education, Pollachi Main Road, Eachanari Post,
Coimbatore, Tamil Nadu, India.
Orcid Id: 0000-0002-0117-5641

Dr. Agnise KalaRani, X.
Associate Professor, Department of Computer Applications,
Karpagam Academy of Higher Education, Pollachi Main Road, Eachanari Post,
Coimbatore, Tamil Nadu, India.
Orcid Id: 0000-0002-1465-0595

Abstract

Large amount of sensitive data is shared to other cloud users in cloud computing environment. To maintain data integrity, security, confidentiality, the data owners encrypt their data before transmission. However, the existing encryption techniques do not provide more security and data integrity rate. In order to overcome such limitations, Bayes Certificateless Signcryption Based Data Integrity (BCS-DI) technique is proposed. It is designed with the objective of improving the security of cloud service provisioning with higher data integrity rate. At first, the cloud users send data request to cloud server. Then, the cloud server analyzes the user request and provides required data. Before transmitting the data to corresponding users, Certificateless Signcryption is used to encrypt the user required data to be transmitted over a cloud network with sender private key which resulting in cipher text. This cipher text is send to the appropriate cloud user in cloud computing environment. Finally, digital signature verification process is carried out at the receiver side to access the original data by using Bayes theorem. The authorized cloud receiver can only obtain the original data when the signature of both sender and receiver is valid. This helps for BCS-DI technique to improve the security and data integrity rate. This technique conducts the experimental works on the parameters such as data security rate, execution time, memory utilization and data integrity rate. The experimental result shows that the BCS-DI technique is able to improve the data security rate and integrity rate of cloud service provisioning.

Keywords: Cloud computing, Certificateless Signcryption, security, data integrity, digital signature verification, Bayes theorem, Elliptical Curve Cryptography, Attribute-Based Sincryption.

INTRODUCTION

Cloud Computing used for sharing the resources over internet in a sophisticated manner. The major issue is to be solved in cloud computing environment is the security and data integrity during data sharing. Therefore, different encryption algorithms were designed for securing service provisioning over public clouds. But, existing algorithms suffer from key escrow problem which lacks in the security and data integrity rate. Hence, there is a need for new technique in order to improve the security and data integrity of cloud service provisioning.

Recently, many research works have been designed for improving the security of data sharing in cloud. A Mediated Certificateless public key encryption (mCL-PKE) scheme was developed [1] for securely sharing the sensitive data in public clouds. The mCL-PKE scheme ensured the confidentiality of data stored in public clouds while enforcing the access control requirements. However, data security rate was not sufficient. An Identity-Based Signcryption (IBSC) scheme was intended [2] with proxy re-encryption function to verify the integrity and authentication of the data in cloud computing. But, time taken for achieving the secured cloud provisioning was more.

An effective scheme was designed [3] to verify the correctness of user's data on cloud data storage by using Signcryption based on elliptic curves. But, the data security level was poor. An Elliptical Curve Cryptography - Based Blind Signcryption Scheme was developed [4] for reducing the low communication overheads and improving the security level and preserving sensitive data in cloud computing environments. However, the data integrity rate was not in a required level.

An Effective Signcryption Based Authentication model was presented [5] to reduce the computational cost and to provide secure data communication over public clouds. An efficient Certificateless encryption technique was implemented [6]for

the secure data sharing over public clouds with lesser encryption time. But, Memory utilization was more.

Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) scheme was introduced [7] to secure the data stored at cloud servers and to provide confidentiality against chosen ciphertext attacks in selective-predicate model. However, data integrity remained unaddressed. An efficient approach was designed [8] in which Signcryption technique was employed for improving cloud computing security. But, reducing the security threat on cloud was not considered.

Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) was presented [9] for secure sharing of personal health data in cloud computing. The CP-ABSC affords confidentiality, authenticity, unforgeability, anonymity and collusion resistance in cloud. However, data integrity was remained unaddressed. A certificate-based proxy re-encryption scheme was intended [10] without bilinear pairings to improve the security and computational cost of data sharing in cloud computing environment.

In order to overcome the existing issues, Bayes Certificateless Signcryption Based Data Integrity (BCS-DI) technique is developed. The main objective of BCS-DI technique is to achieve secure cloud service provisioning with higher data integrity rate.

The research objective of BCS-DI technique is formulated as follows,

- To enhance the integrity rate of cloud service provisioning with lower execution time, Certificateless Signcryption and Un-signcrpyion is performed in BCS-DI technique.
- To improve the security of cloud service provisioning in cloud environment, digital signature verification is performed in BCS-DI technique using Bayes theorem.
- To minimize the space complexity in cloud service provisioning, vectorized model is used in setup phase of Certificateless Signcryption.

The rest of this paper is ordered as follows. Section 2 explains Bayes Certificateless Signcryption Based Data Integrity (BCS-DI) technique with the aid of architecture diagram. Section 3 and Section 4 presents the experimental section with the detailed performance analysis. Section 5 explains the related works. Finally, Section 6 concludes this paper.

Bayes Certificateless Signcryption Based Data Integrity Technique

The Bayes Certificateless Signcryption Based Data Integrity (BCS-DI) technique is designed to improve the security of cloud service provisioning with higher data integrity rate. The Signcryption is a public key cryptographic technique that employs an Encrypt-then-Sign approach to enhance the security of cloud service provisioning. The encryption and digital signature are two essentials cryptographic tools that exploited in Signcryption to achieve the confidentiality, integrity. This Signcryption is a public-key primitive which accomplish the both digital signature and encryption. Besides, Certificateless cryptography is an ID-based cryptography which is used to avoid the key escrow problem in cloud. The overall architecture diagram of Bayes Certificateless Signcryption Based Data Integrity (BCS-DI) technique is shown in below Figure 1.

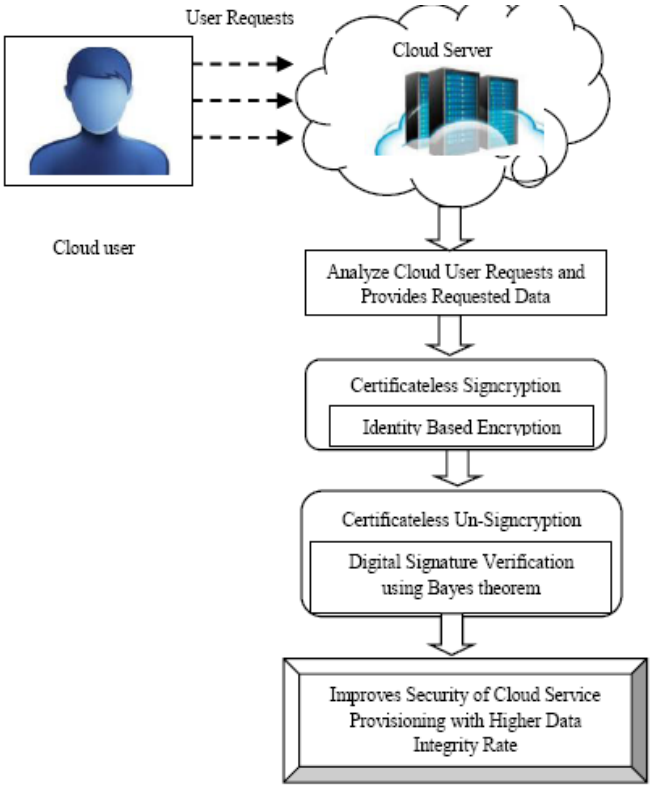

Figure 1: Architecture Diagram of Bayes Certificateless Signcryption Based Data Integrity Technique

As shown in the Figure 1, initially cloud user send data requests to the cloud server. The cloud server analyzes the user request and then provides user request data. Before data transmission, BCS-DI technique encrypts the data using Certificateless Signcryption and produce cipher text. This cipher text is transmitted to the consequent cloud user in cloud computing environment. Finally, BCS-DI technique performs Certificateless Un-Signcryption process where the digital signature verification is carried out to get the original data. Therefore, BCS-DI technique increases the security and data integrity rate of cloud service provisioning in an efficient manner. The detailed explanation about BCS-DI technique is described in forthcoming section.

Certificateless Signcryption

The BCS-DI technique used Certificateless cryptography to minimize the key escrow problem when performing cloud service provisioning. The Certificateless cryptography is a key exchanging process where the key is stored with the aid of third party. The key is only used for sender and receiver to encrypt the data for improving the security of cloud service provisioning. As a result, BCS-DI technique reduces the illegal user accessing the data in cloud computing environment. The BCS-DI technique necessitates that the sender in Certificateless environment to broadcast data to a receiver by using Identity Based Cryptography.

In BCS-DI technique, a Signcryption scheme includes of three processes namely Key Generation, Signcryption, and UnSigncryption. In Key Generation, a pair of keys is created for a cloud user who contributed in Signcryption process. The Signcryption is a probabilistic algorithm which is employed to generate the cipher text for a given data by using both the public and private keys. The UnSigncryption is the deterministic which is utilized to decrypt the cipher text (i.e. original data). The process of the Certificateless Signcryption for the secured cloud service provisioning is shown in below Figure 2.

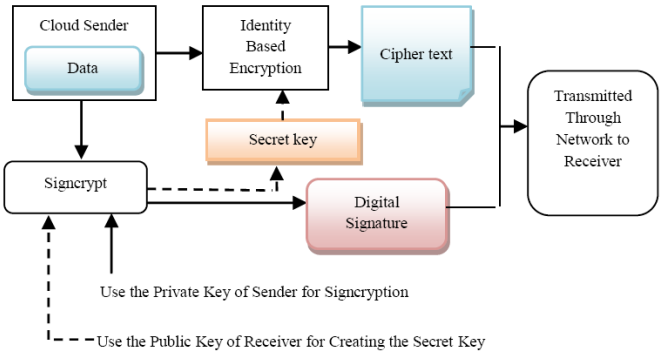

Figure 2: Process of Certificateless Signcryption

As shown in the Figure 2, the Certificateless Signcryption cryptography initially takes the data which is transmitted over a cloud network as input. Afterward, Certificateless Signcryption cryptography performs Identity Based Encryption and Signcryption process by using the secret key and private key of cloud sender and then generates the cipher text, digital signature. The resultant cipher text, digital signature is transmitted to the corresponding cloud user in the cloud computing environment. The Certificateless Signcryption cryptography technique employs the secret key in order to encrypt the data. In BCS-DI technique, Certificateless cryptography technique affords more benefits, for example higher security, high speed, lowers storage space and less bandwidth. This in turn supports the reducing of the time taken for encrypting the data in order to achieve the secured data communication in cloud service provisioning. In addition, authorized cloud user can access the data by performing the signature verification process. Therefore, transmitted data through a cloud network is uncorrupted and can only be accessed or modified by authorized users. This in turn assists for improving the security and data integrity of cloud service provisioning in an efficient manner.

The Certificateless UnSigncryption process to obtain the original data is shown in below Figure 3.

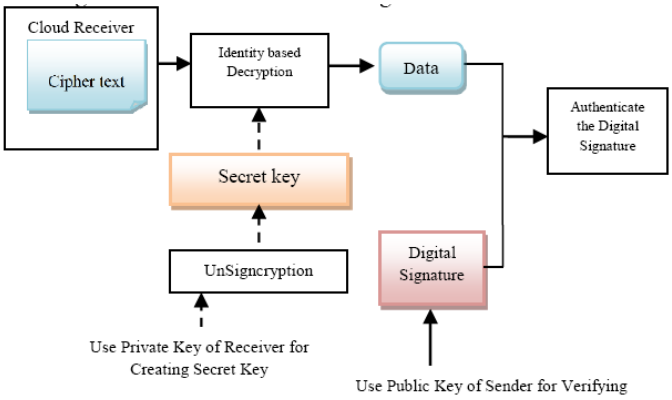

Figure 3: Process of Certificateless Unsigncryption

Figure 3 shows the Certificateless UnSigncryption process for obtaining the original data. The cloud receiver initially obtains the cipher text and then performs digital signature verification process. If the signature of cloud receiver is matched with sender digital signature, then the signature is valid. Otherwise, the signature is invalid. The cloud receiver can access the original data if the signature is valid. Therefore, BCS-DI technique enhances the security of cloud service provisioning.

In Certificateless Signcryption cryptography, the trusted third party is considered as Key Generation Center. The trusted third party provides a partial private key for a cloud user which formulates from the user's identity (ID) and a master key. The Identity-based encryption system allows the cloud user to make a public key from a well-known identity value. A trusted third party produces the equivalent private keys. At first, the private key generator allocates a master public key, and preserves the related master private key. By grouping the master public key through the identity value, the cloud user evaluates a public key associated to the identity ID. The authorized cloud user utilizes the ID relates the private key generator for accessing the data in cloud to obtain a consequent private key. This in turn assists to reduce the unauthorized cloud user to access the cloud data.

In BCS-DI technique, Certificateless Signcryption algorithm is described by using seven processing steps namely Setup phase, Partial private key extraction , Generate user key, Set full

private key, Extract-key- Identity Based Cryptography, Signcryption and UnSincryption.

Step 1: Setup phase

In Setup phase, assume that the input security parameter K and outputs of the system parameters (P) and a master secret key $mkey_1$ and $mkey_2$. The Trusted third party and Private Key generator implements this setup algorithm to get the secret keys $SKey_1$ and $SKey_2$. Subsequently the Trusted third party chooses the multilinear group $GRP_1, GRP_2 \ldots . . GRP_n$ which is produced through Additive Group (AG). In Certificateless Signcryption cryptography, four hash functions (H) are utilized to accomplish the secure cloud service provisioning which is formulated as,

$$H_1: \{0,1\}^* \rightarrow GRP_1 \quad \text{----- (1)}$$

$$H_2: \{0,1\}^* \rightarrow \{0,1\}^K \quad \text{----- (2)}$$

$$H_3: \{0,1\}^* \rightarrow GRP_1 \quad \text{----- (3)}$$

$$H_4: \{0,1\}^* \rightarrow GRP_1 \quad \text{----- (4)}$$

When the number of input data increases, the Private Key generator chooses the random vector model $U = u_{1,}u_2, \ldots . u_n$ and $V = v_{1,}v_2, \ldots . v_n$. These two vectors are employed for handling the multiple data simultaneously transmitted to the cloud receiver. The vector elements are chosen arbitrarily from the multi linear group GRP_1. The trusted third party selects the random value 'R'. The public parameters $< GRP_{1,}GRP_{2,}p, e, P_{pub}, g, H_1, H_2H_3, H_4 >$ are employed to carry out Signcryption process in cloud environment.

Step 2: Partial Private Key Extraction

A cloud user in cloud computing environment submits ID as identity to an algorithm executed by trusted third party that get input as Master secret key and Parameters (P), When the cloud user identity is $CU_{ID} \in \{0,1\}^*$. After that, the trusted third party sets CU_{ID} and generates the partial private key which is mathematically formulated as,

$$CU_{ID} = SKey_1\, H_1\,(ID) \quad \text{----- (5)}$$

The hash function of cloud user Identity $H_1\,(ID)$ and secret key $SKey_1$ is utilized for generating the partial private key in a secure way.

Step 3: Generate user key

This is an algorithm in which the cloud user Identity (ID) is combined with the public parameter (P) to create a secret value. The secret value of the cloud user identity is represented by α_{ID} which employed for generating the user private key and public. The secret value of the cloud user identity is also produce the public Key (P_{key}). The secret value α_{ID} and public key are utilized to make the full private key.

Step 4: Set full private key

This is a deterministic algorithm run by the cloud user where the cloud user Inputs Identity (ID), secret value α_{ID} and public parameters. The Set full private key is computed by using following mathematical formula,

$$FPR_{key} = (\alpha_{ID}\,, CU_{ID}) \text{ ------ (6)}$$

Step 5: Extract-key-identity based cryptography

The cloud user inputs identity to the private key generator who employs the extract algorithm to produce the corresponding private key in a secure way.

Step 6: Signcryption

The input to the Signcryption process is cloud data $D_{1,}D_{2,\ldots}D_n \epsilon P$, cloud sender full private key PR_{key1}, Identity ID1 and public key P_{key1}, cloud receiver identity ID2, public key P_{key2} and the global parameter (p). The Signcryption process generates the cipher text (C) by using following mathematical formula,

$$C = \left(D_i, PR_{key1}, ID1,\ P_{key1}, ID2, P_{key2}, p\right) \text{ --- (7)}$$

From the equation (7), the obtained cipher text is obtained. This resultant cipher text and their digital signature are transmitted to appropriate cloud user in cloud computing environment.

Step 7: UnSigncryption

Finally, UnSigncrption process is carried out to get the original data. At cloud receiver side, the proposed BCS-DI technique initially performs digital signature verification process to verify the signature of cloud receiver to obtain the sensitive cloud data. The BCS-DI technique carries out the signature verification by using Bayes Theorem. The Bayes theorem for signature verification is shown below,

$$P\,(A/B) = \frac{P(B/A)P(A)}{P(B)} \text{ ------ (8)}$$

From the equation (8), A refers the digital signature of cloud sender and B is the digital signature of cloud receiver and $P(A)$ and $P(B)$ are the probabilities of matching A and B without regard to each other. Here, $P\,(A/B)$ represents the probability of cloud sender digital signature is matched with receiver whereas $P(B/A)$ denotes the probability of cloud receiver digital signature is matched with cloud sender. If the result of $P\,(A/B) = 1$, then the signature both the cloud sender and receiver is valid. Otherwise, invalid signature. The cloud receiver can obtain the original data when the signature is valid which in turn helps in enhancing the cloud data security. In BCS-DI technique, the UnSigncryption process takes the input as ciphertext (C), receiver full private key PR_{k2} , Identity ID2 and public key P_{key2} , the senders identity ID1, public key P_{key1} and the global parameters (P) to access the original data. The UnSigncryption process for

accessing the original data is mathematically formulated as follows,

$$D = \left(C, PR_{key1}, ID2, P_{key2}, ID1, p \right) \text{ ----- (9)}$$

By using equation (9), the original data (D) is obtained at the cloud receiver side with the aid of the public parameters and cloud sender's public key and identity. The algorithmic process of Bayes Certificateless Signcryption and UnSigncryption is shown below,

// Bayes Certificateless Signcryption algorithm

Input: Number of data, security parameter K, sender private key PR_{key1}, receiver private key PR_{key2}, sender identity (ID1), receiver identity (ID2), sender public key P_{key1}, receiver public key P_{key2}

Output : Enhanced Security of Cloud Service Provisioning with higher Data Integrity rate

Step 1: Begin

Step 2: For each cloud sender and data (D)

Step 3: Generate the partial private key with identity (ID1) using (5)

Step 4: Generate the secret value α_{ID} to create private and public key

Step 5: Construct full private key using (6)

Step 6: Perform Signcryption process using (7) and resultant cipher text is transmitted to Corresponding cloud users in cloud environment

Step 7: Accomplish Digital Signature Verification using Bayes theorem (8)

Step 8: If $P(A/B) == 1$ then

Step 9: Valid signature

Step 10: Else

Step 11: Invalid signature

Step 12: End if

Step 13: If signature is valid then

Step 14: Unsigncrypt the cipher text (C) using (9)

Step 15: Obtain the original data

Step 16: Else

Step 17: Cloud receiver cannot access the original data

Step 18: End if

Step 19: End for

Step 20: End

Algorithm 1: Bayes Certificateless Signcryption and Unsigncryption algorithm

By using the above algorithmic process, BCS-DI technique ensures the secure cloud service provisioning. The BCS-DI technique initially employs the private key of the cloud sender in order to encrypt the data into cipher text. For handling the multiple data in cloud service provisioning, the vectorized model is used in setup the phase which in turn helps in reducing the memory utilization. The generated cipher text is sent to corresponding cloud user in cloud environment. In receiver side, digital signature verification is performed with assist of Bayes theorem. If digital signature of both cloud sender and receiver is similar, then the original data is obtained. Otherwise, the original data is cannot access by cloud receiver. This helps for improving the data security rate in cloud service provisioning.

EXPERIMENTAL SETTINGS

In order to evaluate the performance of proposed, Bayes Certificateless Signcryption Based Data Integrity (BCS-DI) technique is implemented in Java language using CloudSim Simulator. The BCS-DI technique employed Amazon Simple Storage Service (Amazon S3) dataset for performing the experimental work. The Amazon S3 is consistent, speedy, less expensive, and scalable for cloud service provisioning.

RESULTS AND DISCUSSIONS

In this section, the result analysis of BCS-DI technique is estimated. The efficiency of BCS-DI technique is compared against with existing two methods namely mediated Certificateless public key encryption (mCL-PKE) scheme [1] and Identity-Based Signcryption (IBSC) scheme [2]. The performance of BCS-DI technique is evaluated along with the metrics such as data security rate, execution time, memory utilization and data integrity rate.

Measurement of Execution Time

In BCS-DI technique, execution time measures the amount of time taken for encrypting data for achieving secured cloud service provisioning. The execution time is measured in terms of milliseconds (ms) and mathematically represented as below:

$$Execution\ Time = end\ time\ of\ encryption - start\ time\ of\ encryption \quad \text{---- (10)}$$

From the equation (10), encryption time taken for secured cloud service provisioning is obtained. While the execution time is lower, the method is said to be more efficient.

Table 1: Tabulation for Execution Time

File size (KB)	Execution Time (ms)		
	mCL-PKE scheme	IBSC scheme	BCS-DI technique
10	20.2	16.9	11.5
20	22.5	19.8	13.2
30	25.9	20.5	14.9
40	28.1	22.6	16.2
50	30.6	23.2	18.5
60	34.8	26.5	20.8
70	37.5	30.8	21.3
80	40.7	32.4	23.6
90	42.3	35.1	25.8
100	46.4	37.7	26.4

Table 1 shows the execution time results obtained for secure cloud service provisioning based on the diverse data file size in the range of 10-100 KB. From the table value, it is clear that the execution time using proposed BCS-DI technique is lower when compared to the existing mCL-PKE scheme [1] and IBSC scheme [2].

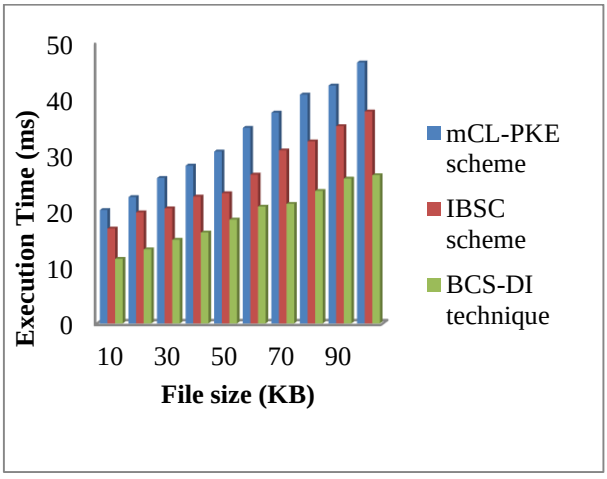

Figure 4: Measure of Execution Time

Figure 4 depicts the impact of execution time with respect to different data file size in the range of 10-100 KB using three methods. As demonstrated in the figure, proposed BCS-DI technique provides lower execution time for achieving secured cloud service provisioning when compared to two existing methods namely mCL-PKE scheme [1] and IBSC scheme [2]. In addition while increasing the data file size of data for encryption process, the execution time is also gets increased using all the three methods. But comparatively execution time using BCS-DI technique is lower. This is owing to application of Bayes Cerificateless Signcryption algorithm in the proposed BCS-DI technique. By using this algorithmic process, proposed BCS-DI technique encrypts the cloud data using the private key of the cloud sender in cloud computing environment. This process takes lesser amount of time to transmit the multiple cloud data concurrently with a secured manner. This helps in reducing the execution time in an efficient manner. Therefore, the proposed BCS-DI technique reduces the execution time by 42% when compared to mCL-PKE scheme [1] and 28% when compared to IBSC scheme [2] respectively.

Measurement of Data Security Rate

In BCS-DI technique, the cloud data security measures the amount of security offered to the data by the cloud users and server on performing data transmission over the networks. While the cloud data security rate is higher, the method is said to be more efficient.

Table 2 Tabulation for Data Security Rate

File size (KB)	Data Security Rate (%)		
	mCL-PKE scheme	IBSC scheme	BCS-DI technique
10	67.16	74.58	82.56
20	69.78	77.85	83.87
30	72.05	78.92	85.14
40	75.12	81.25	86.78
50	76.25	83.68	88.91
60	78.21	85.97	89.65
70	81.02	88.16	90.98
80	82.65	89.97	91.24
90	84.19	91.06	93.36
100	86.54	92.18	95.18

The data security rate result is obtained with respect to the different data file size in the range of 10-100 KB is demonstrated in the Table 2. From the table value, it is expressive that the execution time using the proposed BCS-DI technique is lower as compared to the existing mCL-PKE scheme [1] and IBSC scheme [2].

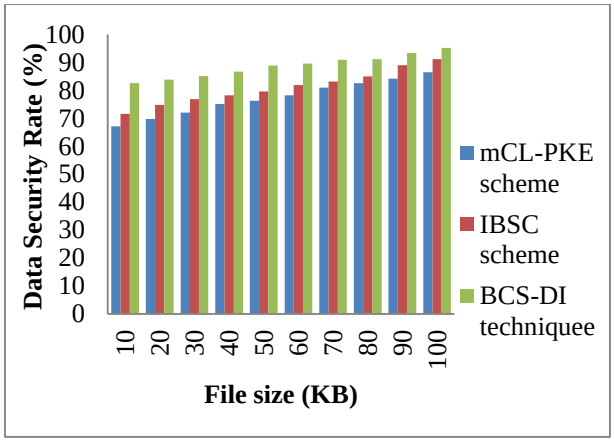

Figure 5: Measure of the Data Security Rate

Figure 5 demonstrates the impact of data security rate obtained with respect to the diverse data file size in the range of 10-100 KB using three methods. As exposed in the figure, proposed BCS-DI technique provides higher data security rate for cloud service provisioning when compared to the two existing methods namely mCL-PKE scheme [1] and IBSC scheme [2]. As well, while increasing the data file size for transmission, the data security rate is also gets increased using all the three methods. But comparatively data security rate using BCS-DI technique is higher. This is due to application of Bayes Certificateless Signcryption algorithm in the proposed BCS-DI technique. By using this algorithmic process, the proposed BCS-DI technique initially encrypt the data by using the private key of the cloud sender. The resultant cipher text is broadcasted to the consequent cloud user in the cloud environment. At the receiver side, digital signature verification is carried out with the aid of Bayes theorem. If the digital signature of both the cloud sender and receiver is identical, then the original data is accessed. Otherwise, the original data is cannot accessed by the cloud receiver. This in turn supports for enhancing the data security rate in cloud service provisioning in a significant manner. As a result, the proposed BCS-DI technique improves the data security rate by 15% when compared to mCL-PKE scheme [1] and 10% when compared to IBSC scheme [2] respectively.

Measurement of Space Complexity

In BCS-DI technique, space complexity measures the amount of memory utilized for storing the encrypted data. The space complexity is measured in terms of Kilo Bytes (KB) and mathematically formulated as given below,

$$space\ complexity = total\ memory\ space - unused\ memory\ space \quad \text{---- (11)}$$

From the equation (11), memory taken for storing the encrypted data is obtained. While the space complexity is lower, the method is said to be more efficient.

Table 3: Tabulation for Space Complexity

File size (KB)	Space Complexity (KB)		
	mCL-PKE scheme	IBSC scheme	BCS-DI technique
10	41.86	35.12	23.15
20	45.32	37.86	27.14
30	47.16	40.15	30.56
40	48.97	41.98	31.68
50	49.65	43.11	33.86
60	50.14	48.74	35.92
70	55.18	50.66	38.17
80	58.29	52.54	40.15
90	61.06	54.87	41.88
100	62.15	57.13	43.11

The space complexity is obtained for storing the encrypted data based on the diverse data file size in the range of 10-100 KB is presented in the Table 3. From the table value, it is illustrative that the space complexity using proposed BCS-DI technique is lower when compared to the existing mCL-PKE scheme [1] and IBSC scheme [2].

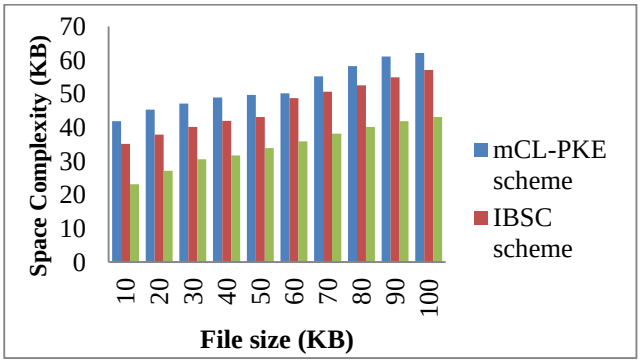

Figure 6: Measurement of Space Complexity

Figure 6 presents the impact of space complexity obtained with respect to varied file sizes in the range of 10-100 KB using three methods. As illustrated in the figure, proposed BCS-DI technique provides lower space complexity for the secured cloud service provisioning when compared to the two existing methods namely mCL-PKE scheme [1] and IBSC scheme [2]. Besides, while increasing the file size, the space complexity is also gets increased using all the three methods. But comparatively space complexity using BCS-DI technique is lower. This is because of the application of Bayes Certificateless Signcryption algorithm in the proposed BCS-DI technique. With the aid of this algorithm, the data is encrypted where the vectorized model is used in the setup phase for handling the multiple data in cloud service provisioning. This in turn helps in reducing the memory utilization. Thus, the

proposed BCS-DI technique reduces the space complexity by 34% when compared to mCL-PKE scheme [1] and 26% when compared to IBSC scheme [2] respectively.

Measurement of Data Integrity Rate

In BCS-DI technique, the data integrity rate measures the accuracy and consistency of data stored in the cloud when performing the service provisioning. The data integrity rate is measured in terms of percentages (%). When the data integrity rate is higher, the method is said to be more efficient.

Table 4: Tabulation for Data Integrity Rate

File size (KB)	Data Integrity Rate (%)		
	mCL-PKE scheme	IBSC scheme	BCS-DI technique
10	68.11	73.65	84.15
20	70.25	75.01	85.92
30	71.68	76.65	87.16
40	73.62	78.16	88.74
50	74.16	79.86	90.14
60	76.15	81.06	91.36
70	78.63	83.14	92.35
80	79.90	85.71	94.11
90	81.08	86.26	95.65
100	84.35	89.52	96.78

The data integrity rate result is obtained based on different data file size in the range of 10-100 KB is illustrated in the Table 4. From the table value, it is descriptive that the data integrity rate using the proposed BCS-DI technique is higher when compared to existing mCL-PKE scheme [1] and IBSC scheme [2].

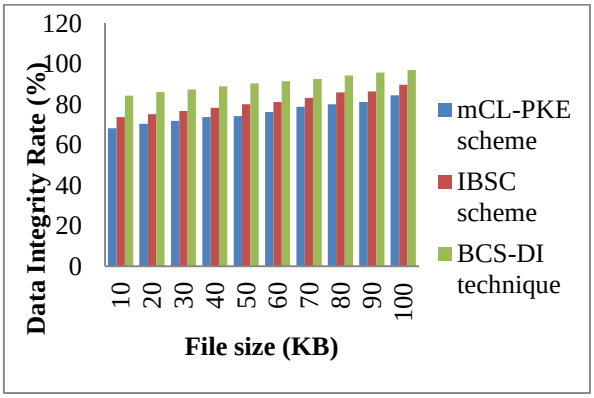

Figure 7: Measurement of Data Integrity Rate

Figure 7 portrays the impact of data integrity rate is obtained based on the different file sizes in the range of 10-100 KB using three methods. As exposed in the figure, proposed BCS-DI technique provides higher data integrity rate for achieving the secured cloud service provisioning when compared to two existing methods namely mCL-PKE scheme [1] and IBSC scheme [2]. Also, while increasing the data file size, the data integrity rate is also gets increased using all the three methods. But, comparatively, the data integrity rate using BCS-DI technique is higher. This is owing to the application of Bayes Certificateless Signcryption algorithm in the proposed BCS-DI technique. By using this algorithmic process, BCS-DI technique encrypts the data which transmitted over a cloud network using the private key of the cloud sender. The cloud receiver can access the original data, if the signature is valid. Therefore, an unauthorized user cannot modify or change the data during the transmission. This assists in improving the data integrity rate in an effectual manner. Hence, the proposed BCS-DI technique increases the data integrity rate by 20% when compared to mCL-PKE scheme [1] and 12% when compared to IBSC scheme [2] respectively.

RELATED WORKS

A Secure Certificateless Public Integrity Verification Scheme (SCLPV) was designed [11] to validate the integrity of the outsourced data. However, the computation cost was higher. A Certificateless Aggregate Signcryption Scheme (CLASC) was introduced [12] for improving the security in data transmission and attaining data confidentiality, integrity, mutual authentication, privacy and anonymity.

An Identity Based Signcryption (IBSC) was intended [13] to secure cloud service that allows users to preserve their data private from the cloud service provider through accomplishing the security preserving operations. But, data security rate was poor. An efficient and provably-secure Certificateless proxy re-encryption scheme was presented [14] for achieving the secure cloud data sharing. However, this scheme takes the executing time for achieving the secure cloud data sharing.

A novel technique was designed [15] to improve the data security with the aid of Signcryption and to attain minimal computational cost and communication overhead. But, the computational cost was more. A data security scheme was developed [16] using Signcryption and hyper elliptic curves to achieve the secure cloud service provisioning and to reduce the computational time and communication cost. But, the computational time was higher.

A novel method was intended [17] that allows the secure data sharing and processing between the collaborating infrastructures and services of public entities. Though, the data integrity was remained unaddressed. Cryptography system model was used [18] for secure data sharing on cloud and affording data confidentiality, access control of share data,

removes the burden of key management and file encryption/decryption by users.

Attribute Based Encryption was introduced [19] for improving the security of cloud service provisioning. However, the data integrity was remained unsolved. Key Derivation Policy (KDP) was presented [20] for enhancing data security and integrity in cloud. But, the execution time was higher.

CONCLUSION

An efficient Bayes Certificateless Signcryption Based Data Integrity (BCS-DI) technique is designed with the aim of improving the security of cloud service provisioning with the higher data integrity rate. Initially, the cloud users transmit the data request to cloud server. After that, the cloud server examines the user request and affords the required data. Before sending the data to the corresponding users, Certificateless Signcryption is employed. The Certificateless Signcryption encrypts the user's required data with the private key of cloud sender which resulting in cipher text. This cipher text is broadcasted to the corresponding cloud user in the cloud computing environment. At last, the digital signature verification process is performed in the receiver side to obtain the original data with the support of Bayes theorem. The authorized cloud receiver can only get the original data when the signature of both sender and receiver is legitimate. This in turns assists in improving the security and data integrity rate of cloud service provisioning in an effective manner. The performance of BCS-DI technique is tested with the metrics such as data security rate, execution time, memory utilization and data integrity rate. With the experiments conducted for BCS-DI technique, it is observed that the data security rate and integrity rate provided more precise results for the secured cloud service provisioning when compared to the state-of-the-art works. The experimental results show that BCS-DI technique provides better performance with an enhancement of data security rate and reduction of execution time as compared to the state-of-the-art works.

REFERENCES

[1] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding and Elisa Bertino. "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" IEEE Transactions on Knowledge and Data Engineering, Volume 26, Issue 9, Pages 2107 – 2119, 2014

[2] Fagen Li, Bo Liu, Jiaojiao Hong. "An efficient Signcryption for data access control in cloud computing" Computing, Springer, Pages 1–15, 2017

[3] Jahnvi S. Kapadia, Mehul P. Barot. "Public Verifiability in Cloud Computing Using Signcryption Based on Elliptic Curves". Journal of Computer Engineering, Volume 11, Issue 1, Pages 39-45, 2013

[4] Chien-Hua Tsai and Pin-Chang Su. "An ECC-Based Blind Signcryption Scheme for Multiple Digital Documents Security and Communication Networks" Hindawi cooperation publication, Volume 2017, Article ID 8981606, Pages 1-14, 2017

[5] Richa Singh Dangi, Amit Saxena, Manish Manoria. "An Effective Signcryption Based Authentication for Security in Cloud Computing" International Journal of Computer Science and Information Technologies, Volume 6, Issue 6, Pages 5284-5288, 2015

[6] Marrium Yusuf, Bhupesh Gour. "An Efficient Signcryption Based Data Sharing in Public Clouds with Message Verification" International Journal of Scientific & Engineering Research, Volume 7, Issue 2, Pages 1236-1243, February-2016

[7] Y. Sreenivasa Rao. "A secure and efficient Ciphertext - Policy Attribute - Based Signcryption for Personal Health Records sharing in cloud computing" Future Generation Computer Systems, Elsevier, Volume 67, Pages 133–15, February 2017

[8] Nikhil Bhalerao, Pravin Nagare. "An Efficient Approach: Signcryption technique for cloud computing security" Spvryan's International Journal of Engineering Sciences & Technology (SEST), Volume 3, Issue 1, Pages 1-6, 2015

[9] Jianghua Liu, Xinyi Huang, Joseph K. Liu. "Secure Sharing of Personal Health Records in Cloud Computing: Ciphertext-Policy Attribute-Based Signcryption" Future Generation Computer Systems, Elsevier, Pages 1-29, 2015

[10] Yang Lu, Jiguo Li. "A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds" Future Generation Computer Systems, Elsevier, Volume 62, Pages 140–147, September 2016

[11] Yuan Zhang, Chunxiang Xu, Shui Yu, Hongwei Li, and Xiaojun Zhang. "SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems against Malicious Auditors" IEEE Transactions on Computational Social Systems, Volume 2, Issue 4, Pages 159-170, December 2015

[12] Sultan Basudan, Xiaodong Lin, Karthik Sankaranarayanan. "A Privacy-preserving Vehicular Crowdsensing based Road surface Condition Monitoring System Using Fog Computing" IEEE Internet of Things Journal, Volume PP, Issue 99, Pages 1-11, 2017

[13] Bo Qin, HuaqunWang, QianhongWu, Jianwei Liu, Josep Domingo-Ferrer. "Simultaneous authentication and secrecy in identity-based data upload to cloud" Cluster Computing, Springer, Volume 16, Issue 4, Pages 845–859, December 2013

[14] Wang Liang-Liang, Chen Ke-Fei, Mao Xian-Ping, Wang Yong-Tao. "Efficient and Provably-Secure Certificateless Proxy Re-encryption Scheme for Secure Cloud Data Sharing" Journal of Shanghai Jiaotong University (Science), Springer, Volume 19, Issue 4, Pages 398–405, August 2014

[15] Sunil Maggu, V.K. Gupta, Meenu Dhingra. "Data security using Signcryption & Relocation Techniques in Cloud Computing" International Journal of Advances in Engineering Sciences Volume 3, Issue 2, Pages 8-12, April 2013

[16] Samson B. Akintoye, Kayode A. Akintoye. "Data Security Scheme For Cloud Computing Using Signcryption Based On Hyperelliptic Curves" Journal of Research and Development, Volume 2, Issue 7, Pages 10-19, 2015

[17] Bojan Suzic, Andreas Reiter, Florian Reimair, Daniele Venturi, Baldur Kubo. "Secure Data Sharing and Processing in Heterogeneous Clouds" Procedia Computer Science, Elsevier, Volume 68, Pages 116 – 126, 2015

[18] Anjali Patel, Nimisha Patel, Dr. Hiren Patel. "Secure Data Sharing Using Cryptography in Cloud Environment" IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 1, Pages 58-62, 2016

[19] Phyo Thandar Thant. "Security of Cloud Service Provisioning using Attribute Based Encryption" International Journal of Emerging Trends & Technology in Computer Science, Volume 1, Issue 1, Pages 96-100, May-June 2012

[20] P. Senthil Kumari, A. R. Nadira Banu Kamal. "Key Derivation Policy for Data Security and Data Integrity in Cloud Computing" Automatic Control and Computer Sciences, Springer, Volume 50, Issue 3, Pages 165–178, 2016.