# An Efficient Signcryption Based Data Sharing in Public Clouds with Message Verification

Marrium Yusuf
Department of Computer Science
Technocrats Institute of Technology
Bhopal, India
marrium.yusuf@gmail.com

Dr. Bhupesh Gour
Department of Computer Science
Technocrats Institute of Technology
Bhopal,India
Bhupesh_gour@rediffmail.com

**Abstract—** Cloud Computing is a new way of providing sharing of resources over internet in a more easily and sophisticated manner. But with the advent of this new technology (Cloud Computing) various limitations and issues arises. The major issue that is visible is the security achieved during data sharing over cloud. Hence various security and encryption algorithms are implemented for the secure data sharing over public clouds. An efficient Certificate less encryption technique is implemented for the secure data sharing over public clouds. But the existing technique implemented suffers from escrow problem and there is no concept of proxy re-encryption used in the methodology. Here in this paper a new and efficient technique for the data sharing over public clouds is proposed which is based on the concept of Signcryption using Elliptic Curves. The proposed methodology implemented here provides security from various attacks as well as provides less computational overhead and encryption time as well as takes less storage space.

**Index Terms—** Cloud Computing, Amazon, Signcryption, Data Sharing, Attribute Policies, Cryptography.

## I. Introduction

The recent advancements in technology have changed the way how electronic data is stored and retrieved. Nowadays, individuals and enterprises are increasingly utilizing remote services (such as Dropbox [1], Google Cloud Storage [2] and Amazon Simple Storage Service [3]), mainly for economical benefits. These services not only enable information sharing but also ensure availability of data from anywhere at any time. However, the growing use of remote services raises serious privacy issues by putting personal data at risk, particularly when the server's offering such services are untrusted. Unfortunately, servers get direct access to the data they store and process. For protecting sensitive data from servers in untrusted environments, data could be encrypted before leaving trusted boundaries. Regardless of whether the data is encrypted or not, the server will need to decide who will gain access to it. For regulating access to the data, access control policies could be specified. These are access control policies that will describe who can gain access to the data. State-of-the-art policy-based systems can ensure enforcement of these policies. However, the matter becomes complicated when sensitive policies, which may leak private information, have to be enforced in untrusted environments. The Cloud Computing paradigm originates mainly from research on distributed computing and virtualization, as it is based on principles, techniques and technologies developed in these areas. Although there may still be some confusion as to what exactly Cloud Computing means, and no general consensus on a definition for Cloud Computing has been reached [4, 5], for the scope of this work we shall adopt the informal definition of Cloud Computing proposed in [6] and reported below:

Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement.

## CLOUD COMPUTING

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort. The underlying concept of cloud computing is the separation of applications from the operating systems and the hardware on which they run. Cloud computing convey applications via the internet, which are accessible from web browsers and desktop and mobile apps, while the software and data are stored on servers at a remote location.

In the past, many of us worried about losing our documents, photos and files if something bad happened to our computers, like a virus or a hardware malfunction. Today, our data is migrating beyond the boundaries of our personal computers and all our data would still safely reside on the web, accessible from any Internet-connected computer, anywhere in the world because of cloud computing.

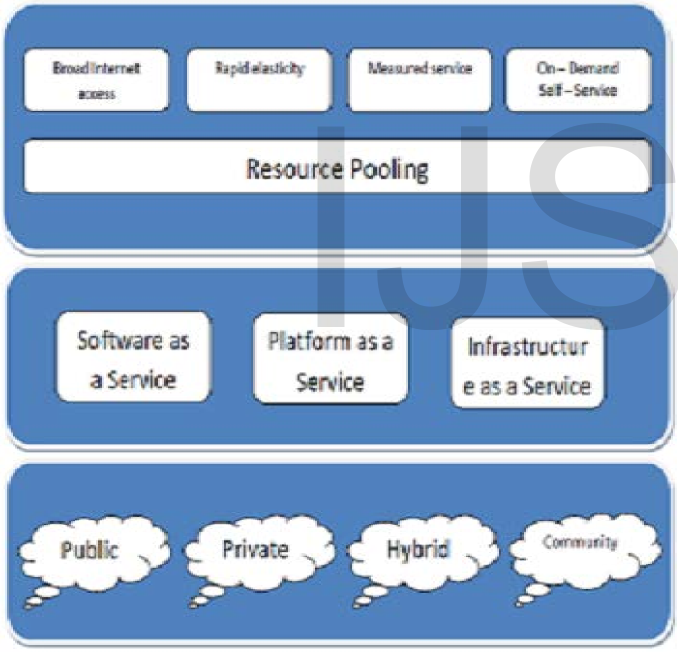


Figure 1: Cloud Computing

## SHARED KEY CRYPTOGRAPHY

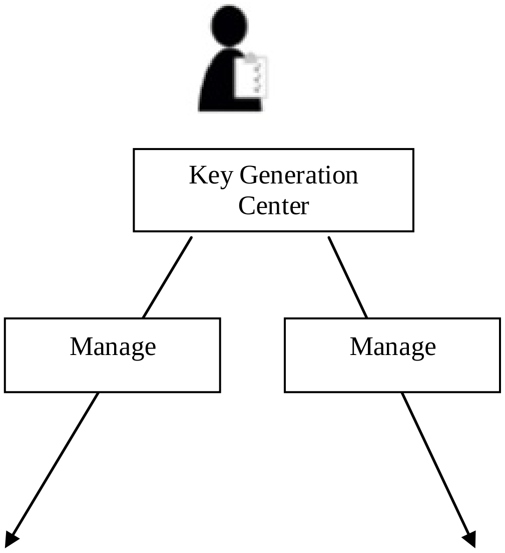
Symmetric key ciphers (i.e., shared key ciphers) have the advantage of relatively short keys and the ability of high rates of throughput. In such systems, secret crypto keys must be shared among those entities that are to communicate confidentially, so regarding two-party communication, the key must remain secret in both ends. In large networks, there would be many keys to be managed, and each user would have to securely manage a list containing the key pairs for each of his or her contacts. This could be impractical and troublesome, and lack ∞edibility concerning new and leaving users.

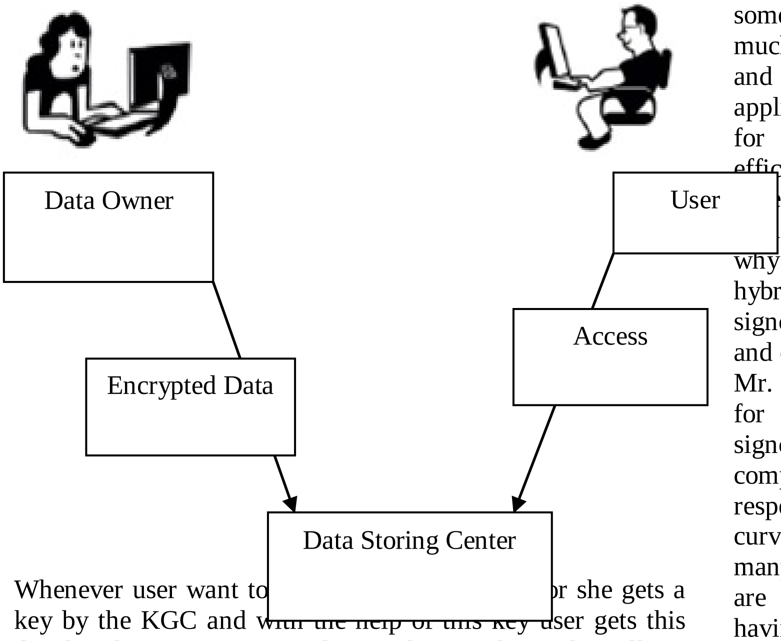
Sharing long-term secret keys among a number of users is an impractical and troublesome assumption due to increased vulnerability from the aging of keys, and lack of flexible user constellations due to the shared keys. This could be mitigated by an online trusted third party (TTP) so that all communication goes through the TTP that shares a secret key pair with all relevant users. Nevertheless, this would in many cases be undesirable. It would correspondingly be a problem to distribute and establish new shared keys to new contacts over an insecure network if the key distribution protocol (that is, the key establishment protocol) is based on symmetric key ciphers, since this would require that a symmetric key is already shared between the distributor and the receiver.

In practice, symmetric key ciphers are mostly applied session-wise due to their capabilities of high throughput and efficiency. The shared session keys would be established by means of some secure key establishment protocol. Such protocols could be based on symmetric key ciphers or public key ciphers. However, a key establishment protocol based on symmetric key ciphers would still require that the two parties going to establish a shared secret session key still share a long-term secret key. Key establishment protocols based on public key ciphers eliminate the disadvantages of sharing long-term secret keys.

## DATA SHARING

Today's computing technologies have attracted more and more people to store their private data on third-party servers either for ease of sharing or for cost saving. When people enjoy the advantages these new technologies and services bring about, their concerns about data security also arise. Every people want that their data may be secure by the unauthorized user. In this figure we are performing data sharing. We are using three level of sharing key generation center, data owner and user. In data storing center all the data keep store in encrypted form.





Whenever user want to [illegible]r she gets a key by the KGC and with the help of this key user gets this data but the user is registered user otherwise he or she will not having this key. So by this we perform data sharing in small level.

Whenever we performing data sharing we have to maintain the data policies and time to time update these policies. One solution of this issue is using a policy which is good in performing encryption that is Cipher text policy attribute-based encryption (CP-ABE). This policy provides that every user had to define their own policy and enforce that policy on the data distribution.

**SIGNCRYPTION**

In cryptography, Signcryption is a public-key encryption scheme that performs the functions of digital signature as well as of encryption simultaneously. The two fundamental cryptographic tools are Encryption and Digital signature which can guarantee confidentiality, integrity, and non-repudiation . Until the late early 2000s, both of them have been viewed as important but different basic requirement of various cryptographic systems. In public key schemes, a traditional method is signature-then-encryption i.e. to digitally sign a message then followed by an encryption. But it can intend us to two problems: Low efficiency and high cost, and the case that no arbitrary scheme can guarantee the security. Signcryption is a cryptographic technique that fulfills the functionalities and properties of digital signature and encryption in a single logical step i.e. both at the same instance and can decrease the computational costs very effectively and it also decreases communication overheads when we compare it with the traditional signature-then-encryption schemes.

Signcryption is a scheme that provides the properties and functionality of both encryption and digital signatures schemes in such a way so that it becomes more efficient than signing and encrypting separately one by one. The meaning of all this is that under a particular model of security at least some aspect of its efficiency (e.g. the computation time) is much better than any hybrid combination of digital signature and encryption schemes. Sometimes hybrid encryption can be applied in place of simple encryption, and a single session-key for several encryptions is reused to attain better overall efficiency for many signature-encryptions than a signcryption scheme but the reuse of session key results in breach of security under even the relatively weak CPA model . That is why a random session key is used for each message in a hybrid encryption scheme but for a given level of security, a signcryption scheme has to be more efficient than other simple and easy signature-hybrid encryption combination.

Mr. Yuliang Zheng was the one who introduced signcryption for the first time in 1997 [7].An elliptic curve-based signcryption scheme was also proposed by Zheng which saves computational and communication costs by 58% and 40% respectively when it is compared to the traditional elliptic curve-based signature-then-encryption schemes. Meanwhile many other signcryption schemes are also proposed but there are many problems and limitations that each of them are having, on the other sidethe also offer different level of computational costs and security services.

## II. Literature Survey

Since encryption can provide confidentiality of the message and digital signature can provide authentication and non repudiation of a message. To simultaneously provide two roles in reality, in 1997, Zheng [7] first proposed a new crypto graphical primitive: signcryption, by which digital signature and PKE can be performed in a logic step, at lesser communication overheads and lower computational cost than the above sign-then encrypt way. Since then, there are many signcryption schemes proposed. It is only recently that a formal security proof model [8] is formalized providing security proof for Zheng's scheme [12] in the random oracle model. By combining ID-based cryptology [9] and signcryption, Malone-Lee proposed a first ID-based signcryption scheme. But Libert and Quisquater [10] pointed out that Malone-Lee's scheme is not semantically secure, since the signature of the message is visible in the signcrypted message. Chow et al [11] proposed an ID-based signcryption scheme that can provide both public verifiability an forward security. In 2003, Boyen [12] proposed a secure identity-based signcryption scheme with cipher text anonymity and provable secure in the random oracle model. Their security proof model is slightly different from that of [8] which includes the cipher text anonymity. In 2004, Libert and Quisquater modified Boyen's security proof model to non-identity based signcryption scheme and proposed a signcryption scheme [13]. They proved that their signcryption scheme is secure in the random oracle model with the following properties: semantically security against adaptive chosen cipher text attacks, cipher text anonymity and key invisibility.

Here in this paper [14] author has proposed a new arbitrated certificateless encryption method without pairing process for strongly distribution sensitive information in open clouds.

Here they use Mediated certificateless public key encryption (mCL-PKE) explains the key escrow difficulty in identity based encryption and certificate revocation difficulty in public key cryptography. On the other hand, existing mCL-PKE methods are also in-competent because of utilize of costly pairing process or susceptible beside incomplete decryption attacks. With the intention of concentrate on the presentation and protection concerns, here in this paper they apply their mCL-PKE method to build a realistic explanation to the difficulty of sharing sensitive information in public clouds. The cloud is utilized as a protected storage space and a key generation center. In their method the data owner encrypts the susceptible data using the cloud generated users' public key supported on its right to use manage policies and uploads the encrypted data to the cloud storage space. Due to unbeaten permission, the cloud moderately decrypts the encrypted data for the cloud consumers. The cloud consumers consequently completely decrypt the in some measure decrypted data using their own private keys. The privacy of the content and the keys is protected regarding the cloud, for the reason that the cloud cannot entirely decrypt the information. They also suggest an expansion to the exceeding approach to get better the competence of encryption at the data owner on cloud. Experimental result shows that proposed system has it's enhance security and performance and that schemes are proficient and practical use in real time application.

A. Sahai and B. Waters proposed Fuzzy Identity-Based Encryption. They present two constructions of Fuzzy IBE schemes. This construction can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. This IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. They prove the security of this scheme under the Selective-ID security model. They first introduced attribute based encryption (ABE) for encrypted access control. In an ABE system, both the user secret key and the ciphertext are associated with a set of attributes. Only if at least a threshold number of attributes overlap between the ciphertext and his secret key, can the user decrypt the ciphertext [15].

V. Goyal et al. [16] first introduced the concept of CP-ABE based on ABE. The main idea is to develop a much richer and secure type of attribute-based encryption cryptosystem. In this system each ciphertext is labeled by the encryptor with a set of expressive attributes. Each private key is connected with an access construction that specifies which type of ciphertexts the key can decrypt. They call such a idea a Key-Policy Attribute-Based Encryption (KP-ABE), since the access structure is specified in the private key, while the ciphertexts are simply labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if the attributes associated with a ciphertext satisfy the key's access structure. Their construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) [16].

## III. PROPOSED METHODOLOGY

The methodology implemented here for providing Dynamic Data at Data centers with Multi Receiver Identity based Signcryption. The proposed methodology implemented will consists of following phases:

1. First of all create a cloud Environment.
2. The cloud Environment Setup consists of 'N' number of Cloudlets 'Ci', Data Centers 'DCi', Virtual Machines 'VMi', Brokers 'Bi'.
3. Now the user of the cloud starts sharing of data to other users of the cloud.
4. During the sharing of data over cloud environment four steps are performed initialized with Setup Phase and Key Generation Phase and Encryption Phase and Decryption and Verification Phase.

### Cloud Environment Setup

Here the cloud environment is setup and simulate using Cloud Simulator in which first of all Cloudlets and Data Centers and Virtual Machines and Brokers are created.

a) If 'N' be the number of Requests to be send from Cloudlets 'Ci' to the Data Centers 'DCi' through Brokers 'Bi'.
b) Let us suppose 'Ri' number of resources to used during the sharing of data from Cloudlets 'Ci' to Data Centers 'DCi'.
   Ci → Bi → DCi
c) For each of the Resource to be shared to data Centers
   Ri → DCi
d) End

### Security Algorithm

The technique implemented for the Secure Data Sharing uses Multi Receiver Identity Based Signcryption using Elliptic Curves which consists of Following Phases:

### Setup

During the setup phase of the Signcryption methodology implemented here for data security. Here in the setup phase Elliptic Curves are created using the equation:

$$y^2 = ax^3 + bx + c$$

Where,

$$4a^3 + 27b^2 \neq 0$$

Elliptic Curve Cryptography contains the following Parameters over the finite field $F^p$.

| Symbol | Description |
|---|---|
| q | The prime number of the order of p |
| a,b | The curve coefficient |
| B | is the base point or the common point $(B_x, B_y)$ |
| n | Is the order of the base point B. |

| | |
|---|---|
| h | $\frac{E(F_q)}{n}$ |
| Sk1 | The secrete key of first user with (X,Y) Co-ordinates. |
| Sk2 | The secrete key of other user with (X, Y) Co-ordinates. |
| P1 | Is the generated public key of first user. |
| P2 | Is the generated public key of other user. |
| * | Is the point multiplication |

Table 1. Various Notations Used

### Key Generation

If User'Ui' of the Cloudlet 'Ci' wants to share data with other users of the Cloud then during the setup of the elliptic curves both the users of the cloud shared a Common Base Point of the elliptic Curve 'B'. Now one User chooses a random point over the elliptic curve that would be the secrete key of the first user as 'Sk1'. The Chosen Secrete Key is the combination of 'X' and 'Y' axis parameters as Sk1(X, Y). Similarly other user of the cloud also shares random point over the elliptic Curve of another secrete key as Sk2. The Chosen Secrete Key is the combination of 'X' and 'Y' axis parameters as Sk2(X, Y). With the help of the Secrete Key Public Key Parameters are generated using.

$$P1(X,Y) = Sk1(X,Y) * B(X,Y)$$
$$P2(X,Y) = Sk2(X,Y) * B(X,Y)$$

Here Point Multiplication '*' used here is the combination of point addition and point doubling.

Point Addition is the addition of two point $L = J + K$

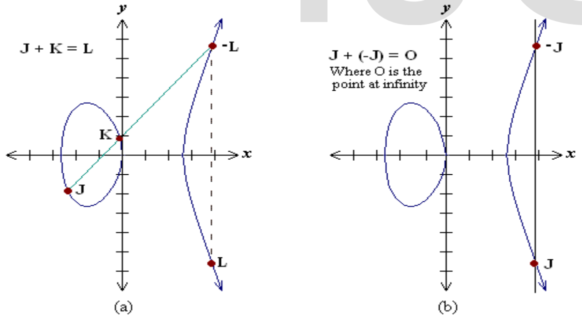


Figure 3. Point Addition

Point Doubling is the addition of point J to itself to obtain another point $L = 2 * J$.

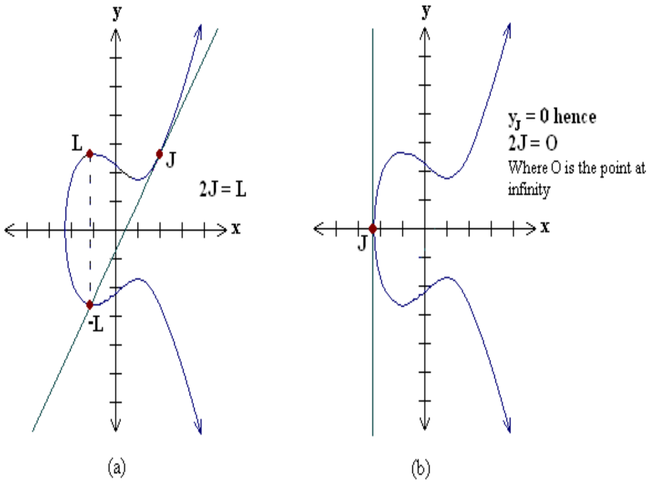


Figure 4. Point Doubling

### Signcryption Phase

The signcryption algorithm implemented here uses the Identity of the other users 'ID1'.

1. First of all select a random Integer 'r', $r \in R[1, n - 1]$
2. Compute P 🡐 [k] B
3. T 🡐 [k] Sk1
4. Generate a set of keys from the key Derivation Function (k1||k2) 🡐 KD(T,l)
5. Generate Cipher Text using the first Key c 🡐 Ek1(m)
6. Generate Signature using the other key using Message Authentication Code Sg 🡐 MACk2(c).
7. Sends the signcrypted text (P, C, Sg) to receiver.

| Symbol | Description |
|---|---|
| R | Selected random integer. |
| R | Prime order number |
| P | Is the public key selected from the elliptic curve. |
| Sk1 | Is the generated Secrete key of the first user |
| K | Generated private key of the user |
| KD | Is the Key Derivation Function. |
| B | Is the Common Base Point |
| E | Is the Encryption Algorithm |
| M | Message to be encrypted |
| k1 | Key 1 |

| | |
|---|---|
| k2 | Key 2 |
| C | Cipher text |
| Sg | Generated Signatures |
| MAC | Message Authentication Code Hash Function. |

Table 2. Various Annotations Used

**UnSigncryption Phase**

As soon as the signcrypted message (P, C, Sg) is received to the Receiver with Identity 'IDi'.

1) Generate a message String T using T ← [x] P
2) Generate a set of Key pairs using Key Derivation Function

(k1||k2) ← KD(T,l)

3) Decrypt the message using Key k1, m ← Dk1(c).
4) Generate Signature using the other key using Message Authentication Code Sg1 ← MACk2(m).
5) Now verify the message by checking if the generated signatures from the user Sg == Sg1
6) If equal then message is verified message else invalid.

The figure shown below is the basic flow chart of the proposed methodology. The data to be shared between various Data Owners of the cloud is first encrypted and digital signed using the proposed Elliptic Curve based Signcryption methodology using the private key of the sender. The message to be signcrypted is then send to the respective receiver for the UnSigncryption but before the Digital Signatures is matched.

## I. RESULT ANALYSIS

The Table shown below is the analysis and comparison of prevention from various attacks during the authentication between user and server. The existing methodology implemented here for the authentication between user and server using Elliptic Curves provides security from various attacks while the mutual authentication technique implemented is still vulnerable to certain attacks.

| S. No. | Security Attacks | Existing Work | Proposed Work |
|---|---|---|---|
| 1 | Password Impersonation | No | Yes |
| 2 | Password Guessing Attack | Yes | Yes |
| 3 | Confidentiability | No | Yes |
| 4 | Public Verifiability | Yes | Yes |
| 5 | DoS Attack | Yes | Yes |
| 6 | Insider Attack | No | Yes |
| 7 | Denning Sacco Attack | Yes | Yes |
| 8 | DDoS Attack | No | Yes |
| 9 | Outsider Attack | Yes | Yes |
| 10 | Online Dictionary Attack | Yes | Yes |
| 11 | Offline Dictionary Attack | Yes | Yes |
| 12 | Server Masquerade Attack | Yes | Yes |
| 13 | Integrity | Yes | Yes |
| 14 | Unforgeability | Yes | Yes |
| 15 | Non-Repudiation | Yes | Yes |
| 16 | Forward Secrecy | Yes | Yes |
| 17 | Additional Authentication | No | Yes |

Table 3 Analysis of Prevention from Various Attacks

The table shown below is the analysis and comparison of existing mutual authentication based technique and the proposed methodology applied for authentication between user and server on cloud computing. The existing Mutual Authentication Technique implemented provides in total 12hash functions for the encryption to occur while proposed methodology only provides 1hash function for the encryption to occur for the Registration Phase. The various steps involved in Existing Mutual Authentication Technique take 1, 8, 3 Hash functions at the user side and 5, 0, 9 hash functions at the server end. While the proposed methodology takes 1, 0, 1 hash function at user side and 1, 0, 1 hash functions at the server side. The existing methodology in total takes 12 hash function at the user end and 14 hash functions at the server end while the proposed methodology takes 2 hash functions at the user end and 2 hash functions at the server end. Since the proposed methodology implemented takes less hash function hence the overall cost will be less as compared to the existing methodology.

| Scheme | Existing Work | | Proposed Work | |
|---|---|---|---|---|
| | User | Server | User | Server |
| Registration | 1xh | 5h | 1h | 1h |
| Login | 8h | | | |
| Authentication | 3h | 9h | 1h | 1h |

| | | | | |
|---|---|---|---|---|
| Total | 12h | 14h | 2h | 2h |

Table 4. Comparison of Cost

The figure shown below is the analysis and comparison of Signcryption and Un-Signcryption in Milli Second of the proposed methodology. The Signcryption time is computed for various bits on 112, 160, and 256 bits.

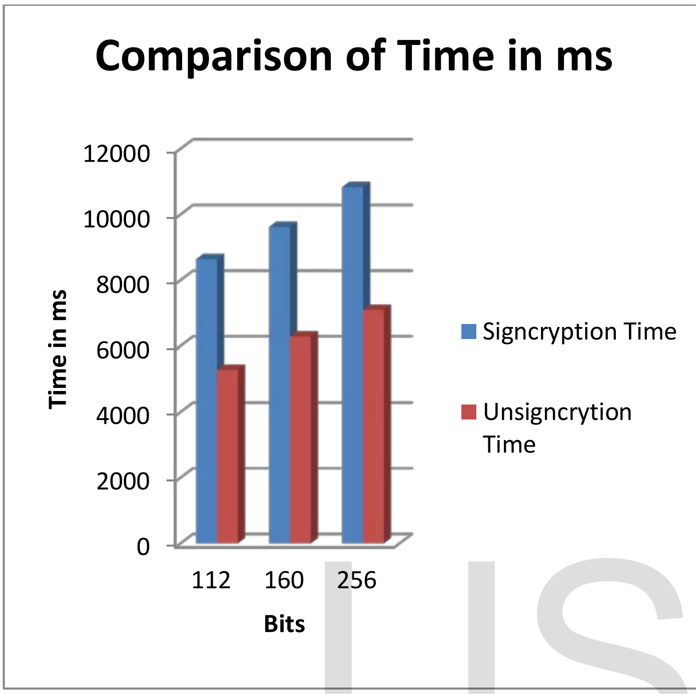


Figure 6. Comparison of Signcryption & UnSigncryption Time in ms

The figure shown below is the analysis and comparison of Storage Cost between Existing and proposed methodology. The proposed methodology implemented takes less Storage cost as compared to existing methodology implemented Mutual Authentication.

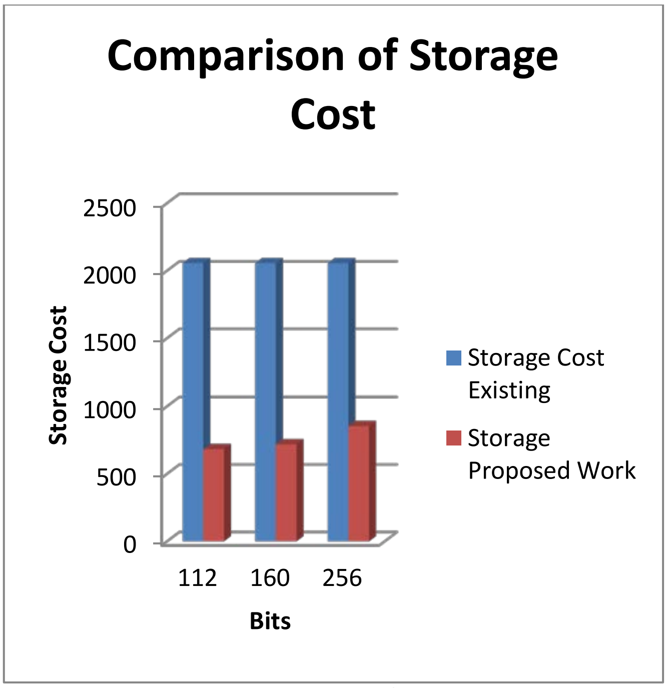


Figure 7. Comparison of Storage Cost

## II. CONCLUSION & FUTURE WORK

The proposed methodology implemented here provides efficient sharing of data over public clouds. The proposed methodology is compared with the existing Certificateless encryption scheme on the basis of various parameters such as computational cost and security attacks and overall computational encryption and decryption time. The experimental results shows the performance of the proposed methodology.

## REFERENCES

[1] “Dropbox.” https://www.dropbox.com/ . October 30, 2013.
[2] Google, “Google cloud storage pricing.” https://cloud.google.com/pricing/cloud-storage, February 2013.
[3] Amazon, “Amazon simple storage service (Amazon S3).” http://aws.amazon.com/s3/#pricing, February 2013.
[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM, 53:50–58, April 2010.
[5] Q. Zhang, L. Cheng, and R. Boutaba. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1:7–18, 2010. 10.1007/s13174-010-0007-6.
[6] P. Mell and T. Grance. The NIST Definition of Cloud Computing (Draft)–Recommendations of the National Institute of Standards and Technology. Special publication 800-145 (draft), Gaithersburg (MD), Jan. 2011.

[7] Y.Zheng. “Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+cost(encryption)”, Crypto'97, LNCS 1294, pp. 165-179, Springer-Verlag, 1997.

[8] J.Baek, R.Steinfeld, and Y.Zheng, “Formal proofs for the security of signcryption”, PKC'02, LNCS 2274, pp. 80-98, Springer-Verlag, 2002.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes", Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53, 1984.

[10] Libert and J.Quisquater, “Efficient signcryption with key privacy from gap Diffie-Hellman groups”, PKC'04, LNCS 2947, pp. 187-200, Springer-verlag, 2004.

[11] Chi-How TAN, “On the Security of Signcryption Scheme with key Privacy”, IEICE TRANS. FUNDAMENTALS, Vol E88-A, No.4, pp. 1093-1095, 2005.

[12] X.Boyen, “Multipurpose identity-based signcryption: A Swiss ary knife for identity-based cryptology”, Crypto'03, LNCS 2729, pp. 383-399, Springer verlag, 2003.

[13] S.M.Chow, S.M.Yiu, L.Hui, and K.Chow, “Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity”, ICISC 2003, LNCS 2971, pp. 352-369, 2003.

[14] Seung-HyunSeo, Mohamed Nabeel, Xiaoyu Ding,Elisa Bertino,”An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds”, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 26, September 2014.

[15] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption”, *Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt ’05)*, pp. 457-473, 2005.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data”, *Proceedings of ACM Conference on Computer and Communication Security*, pp. 89-98, 2006.