Scalable and Secure Message Recovery through Identity Based Secured Cryptographic System

Tinam Sharma¹, Prof. Samta Gajbhiye²

¹SSTC-SSGI
²CSVTU

Abstract: Cryptography is the art and science of concealing the messages to introduce secrecy in information security. This paper focuses on scalable and secure message encryption, message storage and recovery from cloud based storage system. Here we are using advanced Identity Based Secured Cryptographic System for message encryption in which we are using RSA algorithm for key generation, Diffie-Hellmann algorithm for key exchange, Elliptic curve cryptography for encryption and decryption process. For storage in cloud one have to pay charges, so we are using Huffman coding for compression and decompression procedure which makes the size of message less. The scheme prevents replay attacks and privacy preserving access control for securing data in clouds. We are representing the response time of storage through a graph; we also calculate total costs for storage.

I. INTRODUCTION

Human being from ages had two inherent needs: (a) to speak and share data and (b) to speak selectively. These two wants gave rise to the art of secret writing the messages in such a means that solely the supposed individuals might have access to the data. Unauthorized people might not extract any data, even if the scrambled messages fell in their hand. Cryptology, the study of cryptosystems includes Cryptography and Cryptanalysis.

Public-key cryptography may be a radical departure from all that has gone before. Right up to modern world all cryptanalytic systems are based on the elementary tools of substitution and permutation. Using public key algorithmic rule a shared secret is established on-line between communication parties without the requirement for exchanging any secret information. In public key cryptography every user or the device participating within the communication have a pair of keys, a public key and a private key. Considering Public Key in more detail we have a source A that produces plaintext X destined for B. B generates a pair of keys KUb (a public key) and KRb (a private key). With X and KUb as inputs, A forms the ciphertext Y:

\[ Y = EKUb(X) \]

The intended receiver B is able to invert the transformation with his private key:

\[ X = DKRb(Y) \]

A prepares a message to B using his private key to cipher and B will decode it using A’s public key.

\[ Y = EKRa(X) \]
\[ X = DKUa(Y) \]
There are many ID-based secured cryptographic system in which many different public key cryptographic algorithm is used. In this proposed method we used RSA algorithm for key generation which make use of large prime number. In this we also used Diffie Hellman key exchange algorithm which helps in secure interchange of the keys between sender and receiver. Elliptic Curve Cryptography is used for encryption & decryption of the message, the encrypted message is compressed with the help of Huffman coding. After the secure transmission of message the message is stored in Cloud.

II. RELATED WORK

(Ateniese.G et.al, 2005) [6] in this author proposed that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. The characteristics and security guarantees of previously known schemes, and compared them to a suite of improved re-encryption schemes we present over bilinear maps. These pairing-based schemes realize important new features, such as safeguarding the master secret key of the delegator from a colluding proxy and delegate. One of the most promising applications for proxy re-encryption is giving proxy capabilities to the key server of a confidential distributed file system; this way the key server need not be fully trusted with all the keys of the system and the secret storage for each user can also be reduced. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Author present new re-encryption schemes that realize a stronger notion of security, and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. This idea in the context of the Chefs file system, and showed experimentally that the additional security benefits of proxy re-encryption can be purchased for a manageable amount of run-time overhead. We leave open the theoretical problem of finding a proxy re-encryption scheme that does not allow further delegations.

(Kamara.S and Lauter.K, 2009) [7] in this the author proposed the problem of building a secure cloud storage service on prime of a public cloud infrastructure wherever the service supplier is not fully trusty by the client. We have a tendency to describe, at a high level, many architectures that mix recent and non-standard scientific discipline primitives so as to realize our goal. we have a tendency to survey the benefits such associate design would supply to each customers and repair suppliers and provides an outline of recent advances in cryptography driven specially by cloud storage. In addition to straightforward storage, several enterprise customers can have a requirement for a few associated services. These services will embody any variety of business processes as well as sharing of knowledge among trusty partners, legal proceeding support, watching and compliance, back-up,archive and audit logs. We have a tendency to ask a scientific discipline storage service at the side of associate acceptable set of enterprise services as a secure extranet and believe this might offer a valuable service to enterprise customers.

(Gu.C ,Zhu.Y ) [3] author reported an efficient ID-Based proxy signature scheme from pairing. The number of paring operation involved in the verification procedure of our scheme is only one, so our scheme is more efficient comparatively. The new scheme can be proved secure with the hardness assumption of the k-Bilinear Diffe-Hellman Inverse problem, in the random oracle model. Fruitful achievements [2,4] have been made in enhancing the computation of pairings, the computation of pairings are still a heavy burden for schemes from pairings. The number of paring operation involved in the verification procedure of our schemes is only one, so our scheme is more efficient comparatively.

(Singh. H and Verma. G , 2011) [1] proposed ID-based proxy signature scheme with message recovery and we have proved that our scheme is secure as existential forgery-adaptively chosen message and ID attack. This scheme desires smaller information measure in distinction to previous ID-based proxy signature schemes. Hence this theme will be a decent different for certificate primarily based proxy
signatures used for mobile agent. The scheme has been proven DS-EUF-ACMIA beneath the assumption of hardness of the CDHP in random oracle model. The efficiency comparison, also given for showing quality of proposal. Although, scheme has designed for a message of fastened length, non the less it provides an innovation regarding proxy signatures for low information measure. This scheme will be extended to a message of discretional length, using partial message recovery.

(Wickremasinghe.B .et.al) [10] in this the author reported Advances in Cloud computing parades several new possibilities for web applications developers. With the appearance of the Cloud, deployment and hosting became cheaper and easier with the employment of pay-per-use versatile elastic infrastructure services offered by Cloud suppliers. as a result of many Cloud suppliers are obtainable, all providing completely different rating models and set in numerous geographic regions, a replacement concern of application developers is choosing suppliers and knowledge center locations for applications. However, there's an absence of tools that alter developers to judge necessities of large-scale Cloud applications in terms of geographic distribution of each computing servers and user workloads. To fill this gap in tools for analysis and modeling of Cloud environments and applications, we have a tendency to propose Cloud Analyst. It absolutely was developed to simulate large-scale Cloud applications with the aim of finding out the behavior of such applications underneath varied readying configurations. Cloud Analyst helps developers with insights in a way to distribute applications among Cloud infrastructures and price additional services like improvement of applications performance and suppliers incoming with the employment of Service Brokers. Cloud Analyst can be used to model and evaluate a real world problem through a case study of a social networking application deployed on the cloud. We have illustrated how the simulator can be used to effectively identify overall usage patterns and how such usage patterns affect data centers hosting the application.

(Lukas Malina and Jan Hajny) [11] in this the author proposed a novel privacy-preserving security solution for cloud services. The user anonymous access to cloud services and shared storage servers. The solution provides registered users with anonymous access to cloud services.Also offers anonymous authentication. This means that users’ personal attributes (age, valid registration, successful payment) can be proven without revealing users’ identity. Thus, users can use services without any threat of profiling their behavior. On the other hand, if users break provider’s rules, their access rights are revoked. The current privacy is analyzed preserving solutions for cloud services and outline the solution based on advanced cryptographic components. Solution also offers anonymous access, unlinkability and the confidentiality of transmitted data. Moreover, we implement our solution and we output the experimental results and compare the performance with related solutions.

III. METHODOLOGY

The proposed model generates the key using the symmetric cryptography by which both the sender and receiver has two keys. After generation of keys the keys are exchanged and encryption of the message is done through elliptic curve cryptography. Now the message or the data is transferred through the secure channel. If the message being large then data compression technique is used. After applying the compression technique the data which is to be sent becomes shorter and for storing the data in cloud it also take the less space and fewer amounts.

Due to the insecure transmission of message & because of large storage area in the cloud through ID based proxy signature scheme it is necessary to make the secure transmission of message by public key cryptography and compress the given message so as to reduce the storage space and cost. The following
steps are to be followed to make the secure transmission for Scalable & Secure Message Recovery through ID- Based Proxy Signature Scheme.

**Figure 1:** Scalable & Secure Message Recovery model through ID- Based Proxy Signature Scheme

### IV. KEY GENERATION

We make use of RSA key generation algorithm as it is Very fast and Easy to implement. RSA Algorithm is based on the issue of factorizing large numbers that have two and only two factors (Prime numbers). Two large distinct prime numbers p and q should be generated. The product of those, we call n could be an element of the general public key. It should be large enough such that the numbers p and q cannot be extracted from it - 512 bits at least i.e. numbers larger than 10154. We tend to then generate the encoding key e that should be co-prime to the number m = ρ(n) = (p -1)(q - 1). We tend to then produce the decryption key d such that d mod m = 1. Let Y = E(x) be the encoding perform where x is an integer and y is that the encrypted form of x.

\[ Y = x^e \mod n \]
V. KEY EXCHANGE

Key exchange additionally referred to as "key establishment" technique. If sender and receiver would like to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decipher messages received. We make use of Diffie Hellman algorithm for Key Exchange. The first step is for Alice and Bob to agree on an oversized prime \( p \) and a nonzero integer \( g \) modulo \( p \). Alice and Bob build the values of \( p \) and \( g \) public knowledge; for instance, they could post the values on their websites, thus Eve is aware of them, too. For numerous reasons to be mentioned later, it's best if they select \( g \) such its order in \( \mathbb{F}_p^* \) could be a large prime. The next step is for Alice to choose a secret integer \( a \) that she doesn't give away to anyone, while at the same time Bob picks an integer \( b \) that he keeps secret. Bob and Alice use their secret integers to compute

\[
A \equiv g^a \pmod{p} \quad \text{and} \quad B \equiv g^b \pmod{p}.
\]

They next exchange these computed values, Alice sends \( A \) to Bob and Bob sends \( B \) to Alice. Note that Eve gets to examine the values of \( A \) and \( B \), since they're sent over the insecure communicating. Finally, Bob and Alice again use their secret integers to compute

\[
A' \equiv B^a \pmod{p} \quad \text{and} \quad B' \equiv A^b \pmod{p}.
\]

The values that they compute, \( A_0 \) and \( B_0 \) respectively, are actually the same, since

\[
A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' \pmod{p}.
\]

VI. DATA ENCRYPTION

In this proposed method we use Elliptic Curve Cryptography for encryption of the given message. Elliptic Curve Cryptography provides an excellent resolution not just for the data encryption but additionally for the secure key transport between two communication parties and authentic session.
key establishment protocols. Elliptic Curve Cryptography (ECC) makes use of the elliptic curve during which the variables and coefficients are all restricted to components of the finite fields. If two communicating parties Sender and Receiver wish to communicate the messages then they agree upon to use an elliptic curve $E_p(a,b)$ where $P$ may be a prime number and a random point $C$ on the elliptic curve. Sender selects a large random number $\alpha$ that is a smaller amount than the order of $E_p(a,b)$ and a point $A$ on the elliptic curve. Sender computes $A_1 = \alpha (C + A)$ and $A_2 = \alpha A$. She keeps the random number $\alpha$ and also the point $A$ as her private keys and publishes $A_1$ and $A_2$ as her general public keys. Similarly Bob selects a large random number $\beta$ and a point $B$ on the elliptic curve. He computes $B_1 = \beta (C + B)$ and $B_2 = \beta B$. He keeps the random number $\beta$ and the point $B$ as his private keys and publishes $B_1$ and $B_2$ as his general public keys. Once publishing the public keys, the communicating parties again calculate the subsequent quantities and publish them as their specific public keys of each other. If Receiver desires to communicate the message $M$ then all the characters of the message are coded to the points on the elliptic curve using the code table that is arranged by the communicating parties Sender and Receiver. Then each message point is encrypted to a pair of cipher points $E_1, E_2$. He uses a random range $\gamma$ that is completely different for the encryption of various message points.

$$E_1 = \gamma C$$
$$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + AB$$

**Figure 4: Elliptic Curve Cryptography for Encryption**

**VII. DATA COMPRESSION**

Data compression is especially helpful in communications because it allows devices to transmit or store identical quantity of information in fewer bits. The process of reducing the dimensions of information file is mentioned as data compression. In the context of information transmission, it's referred to as source coding. The design of information compression schemes involves trade-offs among various factors, as well as the degree of compression, the amount of distortion introduced and also the computational resources needed to compress and decompress the information.

**Figure 5: .TXT file after Huffman Algorithm**
VIII. CLOUD STORAGE

Cloud storage offers an oversized pool of storage was offered to be used, with three vital attributes: access via net services apis on a non-persistent network connection, immediate availability of very massive quantities of storage, and obtain what you utilize. Cloud storage is an offering of cloud computing. The evolution of Cloud Storage supported traditional network storage and hosted storage. Advantage of cloud storage is that the access of your knowledge from anyplace. Cloud storage providers give storage varying from small amount of information to even the whole warehouse of a company. Subscriber pays to the cloud storage supplier for what they’re victimization and the way a lot of they are transferring to the cloud storage. Basically the cloud storage subscriber copies the info into anybody of the info server of the cloud storage supplier.

Figure 6: Cloud data storing cost

IX. MESSAGE DECODING

A sequence of 0’s and 1’s can be decoded into string of characters going in backward direction.

Figure 7: Decoding of Message

X. MESSAGE DECRYPTION

After receiving the cipher text, sender converts the cipher text into the points on the elliptic curve and recognizes the points E1 and E2 of each character. Then sender decrypts the message as follows:

\[ M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) \]
XI. RESULT

In this section we show the result of the experiment performed for Identity based cryptographic system. The message is encrypted with Elliptic curve system & compressed by Huffman encoding system. In this with the help of graph we show how the data is encrypted, compressed and stored in cloud.

Figure 9: Encryption v/s String Length

Figure 10: Nodes v/s Delay Time

Figure 12: Error Rate v/s Data
XII. CONCLUSION

The main focus of this project was on the secure transmission of the message through Identity based secured cryptographic system. In this method we have used RSA key generation Algorithm and Deffie Hellman key exchange Algorithm for the secure transmission of the message. We have also used Elliptic curve cryptography for encryption of the message which is to be sent. For compression we use Huffman code so that the message which is to be passed becomes smaller in size and take less space in the cloud database. With this proposed model we are able to transmit the message in more secured way and also by using compression technique it takes less storage space.

REFERENCES

3. Chunxiang Gu and Yuefei Zhu“ An Efficient ID-based Proxy Signature Scheme from Pairings” Network Engineering Department Information Engineering University.
6. Giuscppe Ateniese, Kevin Fu, Mattew Green, Susan Hohenberger “Improved Proxy Reencyption Schemes with Applications to secure Distributed storage” Journal ACM Transactions on Information and system security, Vol.9, Issue 1, Feb 2006, PP. 1-30
10. Lukas Malina, Jan Hajmy, “Efficient security solution for privacy preserving cloud services” 2013, 36th International conference on TSP.