ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Elliptic Curve Based Cloud Storage Security

Shital Joshi, Vidyullata Devmane

ME Student, Dept. of Computer Engineering, SAKEC, Mumbai University, Mumbai, India

Assistant Professor, Dept. of Computer Engineering, SAKEC, Mumbai

Pacific Academy of Higher Education & Research, India

ABSTRACT: Cloud computing the most popular technology of today includes ease of access and mobility but Cloud outsourcing is vulnerable to attack, as data is deployed at Third Party Vendors. So, they need to be tamper resistant and most secure. As the data is stored at the remote location in encrypted form to provide security, data operations on encrypted data is a new challenge. So, new technique of homomorphism is developed for encrypted data operations which give the same results on original data and encrypted data. Here we are going to improve the cloud security by introducing most secure Elliptical Curve Cryptography for end-to-end data security assurance. It provides a basic outsourcing solution. We are going to use bilinear mapping which support the homomorphic property to provide untampered operations over the data. We are introducing Identity based cryptography as it will reduce complex key management and certificate management stress. Elliptic curve discrete logarithm problem (ECDLP) ensures the difficulty against different attacks. It also provides smaller key size(160 bits) with equal security(equal to 1024 RSA key security) which makes the cryptosystem very efficient for practical use. Our project is initiative to provide a better data storage security over cloud with minimal efforts in management to make it easily available from small to large scale businesses.

KEYWORDS: Elliptic Curve Cryptography; Cloud storage security; Identity based cryptography.

I. INTRODUCTION

In the era of cloud, data storage, compute resources are easily available with very less capital as cloud follows pay as you use pattern. But it has emerged many concerns related to security about your data. Lot of technical advances are happening around security of resources and data. Here, in our project we are focusing on the data storage security concerns and remediation.

From the literature survey and market survey, we observed that there are many technologies emerging to beat the challenge of data security over the cloud. But all small scale businesses may not avail the existing technologies to secure their data because of many constraints such as key management, certificate requirements etc. In our project, we have developed an Identity based and simple key management cryptography with enhanced security of Bilinear pairing based Elliptical Curve Concept. This gives a better performance with less key sizes. As studies have proved, Elliptical curve cryptography is resistant to many attacks because of ECDLP(Elliptical Curve Discrete Logarithm Problem) hardness, we can build a reliable cloud security model with use of it.

II. RELATED WORK

In [2] authors used average residual battery level of the entire network and it was calculated by adding two fields to Cloud storage is a data outsourcing storage service in recent years, derived and developed from the cloud computing concept, which achieved widespread concern in IT industry depending on its advantages that low cost, convenient interface and high expansibility. However, cloud storage has given rise to user's widespread concerns of security, when it provided convenience. I started my study with different cloud service models, challenges for all service models, security concerns, impact of these constraints, emerging technologies to make cloud storage secure and different technologies for integrity check of cloud data.

In the cloud paradigm, data owners move the large data files from their local computing systems to the remote servers, in which the data owners avoid the initial investment of expensive infrastructure setup, large equipment, and

DOI: 10.15680/IJIRCCE.2016. 0407063

daily maintenance cost. But, security becomes one of the major concerns for all entities in cloud services. Data owners have no idea where the data is stored in cloud. So, they need a way to verify the data is not tampered time to time. But data kept over cloud is an encrypted data, so data operations on encrypted data is a challenge. In order to solve the problem of data integrity verification, many provable data possession (PDP) schemes are proposed under different systems and security models. Shacham et al. [4] proposed MAC-based batch verification for multiple data blocks. In 2007 Ateniese, et al[5] proposed a PDP model to solve the storage problems of files. They divided the file into blocks, and computed a homomorphic tag [6] for each block, completed the proof of the data integrity by sampling and verifying the correspondence of the tags and blocks randomly. A PDP protocol checks that an outsourced storage site retains a file, which consists of a collection of n blocks. The data owner pre-processes the file, generating a piece of metadata that is stored locally, transmits the file to the server and deletes its local copy. Therefore correct possession of data is verified in a challenge-response protocol between the data owner and the server that stores the file. Ateniese et al.[5] are the first to construct and formally define public verifiability PDP model which is provably secure for remote data checking. They introduce the concept of RSA-based homomorphic verifiability tags(HVTs) which are a building block for PDP scheme. But PDP does not provide the data retrievability. A POR is a protocol in which a server proves to a data owner that a target file is intact, in the sense that the client can retrieve the entire file from the server with high probability. Hence, POR guarantees not only correct data possession but it also assures retrievability upon some data corruptions[8]. A POR system by Juels and Kaliski [7] includes six functions – KeyGen, Encode, Challenge, Respond, Verify and Extract. These schemes make integrity check possible but they add a communication complexity for an algorithm.

As many advances are happening over the integrity check of the cloud data, many new technologies are getting emerged with better encryption security than traditional cryptosystems which can satisfy the cloud requirements. Elliptical curve technique introduced in cloud storage security is an evolving field in cryptography. Many variations are happening around elliptical curves. In a statistical analysis, a 163 bit key of ECC is considered to be as secure as 1024 bits key in RSA[9]. ECDLP(Elliptic Curve Discrete Logarithm Problem) is immune to many different attacks. Elliptical Curve cryptography when used with a bilinear pairing, it provides an integrity check support with better encryption security. There are different methods of pairing such as Weil pairing, Tate pairing for bilinearity. Weil pairing requires much more than twice the running time of the Tate pairing in the cryptographic applications[11].

In 2001, Boneh and Franklin [10] announced a viable method using the Weil pairing in Identity based Encryption. This method, while demonstrable, still lacked a pragmatic implementation which could be considered widely usable. FullIdent scheme with Tate pairing has made the implementation practically possible from theories.

By study of all the background technologies, there are still issues in implementing a successful, user friendly and secure cloud storage technology. Whenever storage security is considered as main objective it resulted in a complicated structures for key managements with large key sizes, certificate management etc. User friendly cloud storage security techniques such as IBE(Identity Based Encryption) failing in practical implementation. So, I have proposed a system which gives a better security with Elliptical Curve cryptography and ease of use because of IBE(Identity Based Encryption) with compressed Tate Pairing technique.

III. Proposed Algorithm

A. *Design Considerations:*

- NIST standards for Elliptical curve selection
- Java pairing based cryptographic libraries used directly for pairing calculations

B. *Description of the Proposed Algorithm:*

Aim of the IBE protocols are based on the idea that the public key of an entity can be derived from a public, unique identifier, e.g. an e-mail address etc. When someone wants to send an encrypted message to another user, he thus only has to know this identifier. He doesn't need to store any number stream record for public keys. The recipient requests the corresponding private key from a global Trusted Key Generation Module (called KGM, Even PKG can be used) when he receives a message encrypted with his ID for the first time. In our project we have done variation at the encryption level. We have implemented the Bilinear pairing (Using compressed Tate pairing) ECC with Identity based encryption. This provides a maximum security with smaller key sizes and simple key management.

There are four basic modules for proposed system:

Setup: The KGM chooses

1. the public groups G1 (with generator P) and G2 with the size of q depending on security parameter k
2. the corresponding pairing e,
3. a random private master-key $Km = s$ Ɛ Zq^*
4. a public key $Kpub = sP$,
5. a public hash function $H1 : \{0, 1\}^* \rightarrow G1^*$,
6. a public hash function $H2 : G2 \rightarrow \{0, 1\}n$ for some fixed n and additional hash-functions:
7. $H3 : \{0, 1\}n \times \{0, 1\}n \rightarrow Zq^*$
8. $H4 : \{0, 1\}n \rightarrow \{0, 1\}n$
9. Here X-OR is used for Hash function calculation. The advantage to cryptography is that if you XOR a number with itself it disappears from the equation, e.g.

Message ® a ® a = Message
Message ® 97 ® 97 = Message

Extract:

To create the public key for ID Ɛ $\{0, 1\}^*$ the KGM computes

1. QID = H1(ID) and
2. the private key dID = sQID which is given to the user.

Encrypt :

It encrypts messages using the public key ID. During encrypt phase, the particular user ID is converted into the point on the curve of order q. This is done using MapToPoint function defined in JPBC library available in Java[12]. It Chooses a random sigma using Random bit generator and calculate SHA-512 hash (r) using message M and sigma. Cipher text will have (rP, sigma xor hash (gID^r), M xor hash(sigma)).

Decrypt :

It decrypts messages using the corresponding private key. Once it receives ciphertext (U, V, W), it computes: e(sQ,U), where sQ is the user private key and e is the bilinear mapping.
sigma = V xor hash (e(sQ, U))
Set $r = H1(\sigma, M)$. Test that $U = rP$. If not, reject the ciphertext.

IV. PSEUDO CODE

```
Step 1:  Input file for encryption and User ID
Step 2:  Receive user public and private keys from key generator
Step 3:  Divide file into chunks of 128 bytes with padding
Step 4:  Calculate hash using SHA512 algorithm and save the meta-data. Encrypt file using ECC. Save cipher file at remote location
Step 5: At the time of decryption, use private key and User ID as input.
Step 6:  Calculate SHA512 hash and match it with metadata to check integrity of data.
Step 7: If hash is matched then download file or else throw error.
Step 8: End.
```

V. Simulation Results

Here, we have compared our proposed scheme with Public Key cryptosystem RSA. We have majorly compared the time required for algorithms to run and the encrypted file size, as these are the main concerns.
The results have shown that the proposed system takes more time for Bilinear ECC encryption than RSA. The encrypted file size for Bilinear ECC is less as compared with RSA generated encrypted file. Theories have already proved that the 160 bit Elliptic Curve Cryptography is as secure as 1024 bit RSA cryptography. So, overall Bilinear ECC performs better practically. Following fig.8.1 to fig.8.3 shows the numerical and graphical representation of analysis.

Table.5.1: Numerical results of RSA and Bilinear ECC

	Kilobytes		**Milliseconds**		
Algorithm	**Original File length**	**Encrypted file length**	**Encryption time**	**Decryption time**	**Total Time**
Bilinear ECC	1.34765625	3.859375	4	1	5
RSA	1.34765625	6.6328125	1	1.329	2.329

Table.8.2: Numerical results of RSA and Bilinear ECC for different input file sizes

	File size(KB)		
	1	100	1000
Encryption time for bilinear ECC(In milliseconds)	0.5	2	5
Encryption time for RSA(In milliseconds)	1	6	11

Following figures show graphical result analysis. Fig.5.1 shows graphical results for time in RSA and Bilinear ECC. It shows that the proposed Bilinear ECC takes more time for encryption because of pre-processing time but it takes very less time for decryption than RSA. Fig.5.2 shows Graphical results for encrypted file size in RSA and Bilinear ECC. It shows that encrypted file size for Bilinear ECC is more than RSA. Fig.5.3 shows Graphical results for different file sizes in RSA and Bilinear ECC in terms of time required. The graph shows that Bilinear ECC more efficient in terms of time.

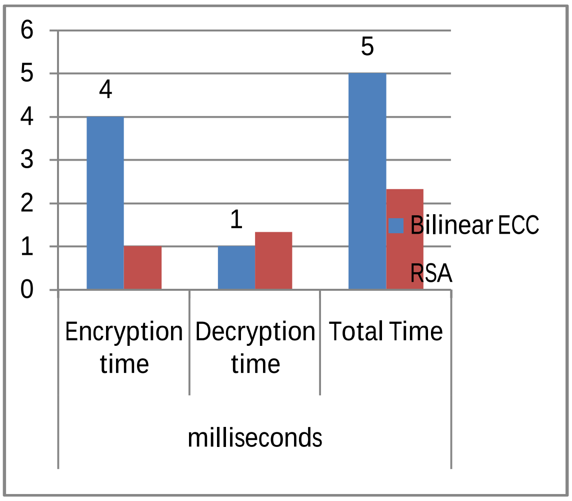

Fig.5.1: Graphical results for time in RSA and Bilinear ECC

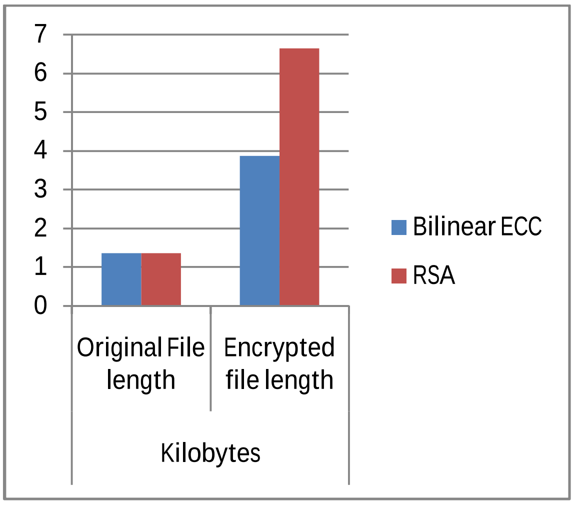

Fig.5.2: Graphical results for encrypted file size in RSA and Bilinear ECC

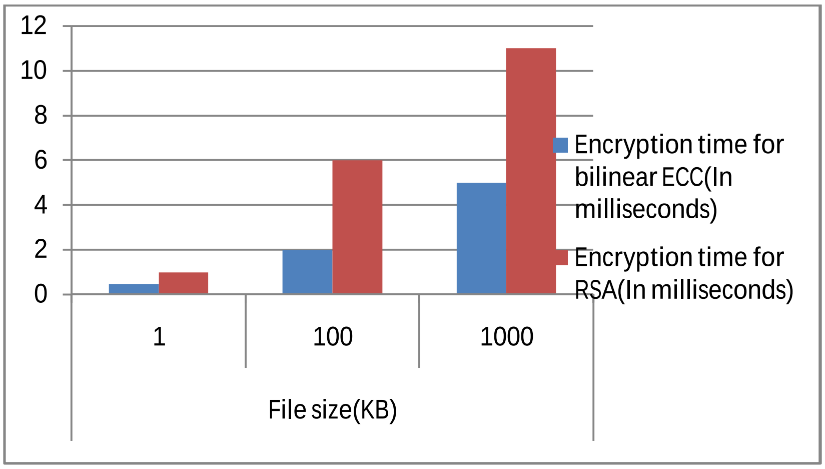

Fig.5.3: Graphical results for different file sizes in RSA and Bilinear ECC

VI. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric Our proposed scheme uses most secured encryption techniques Bilinear ECC which assures data storage security with very less management. It also uses homomorphic property with encryption for data integrity. Combination of these two techniques together has boosted up confidence for using cloud data storage. Result analysis has showed the practical efficiency of a proposed system. The extension of this proposed basic system can definitely provide a strong cryptographic solution for cloud systems.

Ongoing research and future work in this area should include

- New fixed block size file retrieval methods should be implemented to perform integrity check without querying the complete file. This can be achieved by implementing the Merkel hash tree or tiger hash tree algorithms for fixed size file blocks management.
- Right now proposed system is implemented for a single user and single Key Management Module environment. It can be extended to multiuser and multi-KGM environments.
- Proposed scheme is using a single identity based encryption. It can be made more secure by performing a Role based authentication.

REFERENCES

1. Certicom “Catch the curve” White paper series,International Journal of An Elliptic Curve Cryptography Primer, June 2004.
2. https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/, September 2015
3. Joppe W. Bos, Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Eric Wustrow, “Elliptic Curve Cryptography in Practice.”, IEEE 2011.
4. Shacham, B Waters. “Compact proofs of retrievability,” Proc. ASIACRYPT 2008, Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.
5. Ateniese, et al., "Provable data possession at untrusted stores," presented at the Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2007.
6. R Johnson, D Molnar, D song, D wagner. “Homomorphic signature schemes,” In Proc. of CT-RSA, volume 2271 of LNCS, Springer, 2002, pp. 244-262.
7. A. Juels and J. Burton S. Kaliski, "Pors: proofs of retrievability for large files," presented at the Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2007.
8. Solomn Guadie worku, Zhong Ting, Qin Zhi-Guang, “Survey on Cloud Data Integrity Proof Techniques”, IEEE 2012.
9. An Elliptic Curve Cryptography Primer, Certicom “Catch the curve” White paper series, June 2004.
10. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing, extended abstract. In Crypto ’2001, volume 2139 of Lecture Notes in Computer Science, pages 213-229. Springer-Verlag, 2001.
11. Fieker, Claus, Kohel, David R. “Algorithmic Number Theory”, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002.
12. Lynn, B., Pairing-based cryptography library, http://crypto. stanford.edu/pbc/, (2013), v-0.5.14. C language, LGPL license.

BIOGRAPHY

Shital Joshi is a Masters student in Computer engineering, Mumbai University. She received Bachlor of Engineering (BE) degree in 2011 from Shivaji University, India. Her research interests are Cloud storage security, cryptography etc.

Vidyullata Devmane is an assistant professor in Computer engineering department of SAKEC, Mumbai & pursuing PhD in Computer Engineering from PAHER University, Rajasthan, India.