An Elliptic Curve Cryptography based Encryption Scheme for Securing the Cloud against Eavesdropping Attacks

Anshuman Chhabra[1] and Shivam Arora[2]

[1]Division of Electronics and Communication Engineering
Netaji Subhas Institute of Technology
University of Delhi
New Delhi, India
Email: anshumanc.1996@gmail.com

[2]Department of Computer Science
Guru Gobind Singh Indraprastha University
New Delhi, India

***Abstract*—Cloud computing has recently become an extremely useful facet of modern distributed systems. Some of its many applications lie in the development of web services, its federation with the Internet of Things (IoT) and services for users in the form of storage, computing and networking facilities. However, as more services start utilizing the Cloud as a viable option, security concerns regarding user data and privacy also need to be tackled. In this paper, a security scheme for preventing eavesdropping attacks in Cloud environments is proposed. The encryption scheme is based on Elliptic Curve Cryptography and is specifically tailored for securing Cloud services providing storage facilities. As it is based on Elliptic Curve Cryptography, subsequent results obtained show that it reduces the computational overhead incurred in the encryption of data. The performances of other traditional security schemes such as RSA are also compared with the proposed encryption scheme. It is observed that the proposed scheme outperforms the other schemes in terms of the chosen performance characteristics.**

Keywords—Cloud security; Cryptography; Elliptic Curve Cryptography; Cloud storage; Encryption; RSA

I. Introduction

Cloud environments have become an indispensible technology today, with services ranging from software, storage, computing and networking being offered to users. Large companies such as Amazon, Google, Cisco and Microsoft have allowed many users to utilize the Cloud to store and access their personal data. This widespread use of Cloud storage services inadvertently opens users up to a multitude of security threats such as breaches of privacy and unauthorized use of personal data. Despite rapid growth in the development of Cloud services, such security concerns have not received the same attention. Another concern with Cloud storage is the sheer amount of user data that has to be dealt with. As more users join and start storing and accessing their data in the Cloud, the size of the data that has to be managed and secured keeps on increasing. Moreover, most traditional security mechanisms require long and arduous calculations to efficiently secure data and can slow down the entire system as a result. Thus, it is imperative that schemes for securing data in the Cloud are lightweight and at the same time, are able to provide users with a high degree of security.

In this paper, a lightweight security scheme to prevent eavesdropping attacks in the Cloud has been proposed. The scheme is based on Elliptic Curve Cryptography (ECC), and is able to provide a strong level of security as well as reduce computational overhead. This is primarily so because ECC itself is lightweight in nature – it has been observed that ECC generates keys of smaller size compared to the size of keys generated by RSA, for the same level of encryption.

Also, security breaches carried out in the form of eavesdropping attacks can be damaging to users and can lead to misuse of the personal data of the user. In essence, an eavesdropping attack involves a passive external party that listens in and intercepts data being transferred from the user to the Cloud. These external parties might be malicious entities or even those working for the Cloud providers. The proposed scheme is able to limit such individuals from accessing and misusing the private data of the users.

The rest of the paper is structured as follows – Section 2 details research work related to cloud security and Section 3 presents the proposed scheme and the working of the algorithm. Section 4 describes the results obtained when RSA and the proposed scheme are compared experimentally and Section 5 lists the conclusions.

II. Related Work

Recently, research has been undertaken to come up with mechanisms to secure the Cloud. Attribute based Encryption or ABE, has been used effectively by Li et al. in [1] to secure the distribution of patient's personal health records using the Cloud. Their work describes an ABE based technique to provide scalable security for patient files in partially trusted Cloud environments. In [2], Li et al. detail an approach to reducing breach of user privacy and data over-collection in mobile smartphones constituting a Smart City. Another ABE based

approach to privacy and security in Cloud environments, was undertaken by Liu et al. in [3]. The authors present a time-based proxy re-encryption approach called TimePRE in which users are given certain access times to access data after which their access rights are revoked. Other ABE based approaches are listed in [4-6].

Moreover, encryption schemes based on elliptic curve cryptography and its variations have also been used to secure the Cloud. Tirthani and Ganesan in [7] present a scheme for data security in the Cloud using both Diffie Hellman cryptography and ECC. Mukhopadhyay et al. propose an approach using hyper-elliptic curve cryptography to achieve the same in [8].

Other approaches are also detailed in literature. Rewagad et al. in [9] use an approach based on Diffie Hellman cryptography and the Advanced Encryption Standard (AES). Previously, Venkatesh et al. in [10] have also described an approach based on RSA that was useful for encrypting large file sizes. However, this method is cumbersome and slow when it comes to retrieving the data that has been stored. More importantly, none of these approaches effectively tackle concerns regarding eavesdropping attacks, which are a growing concern.

III. Proposed Scheme

A. Elliptic Curve Cryptography

Before detailing the proposed scheme, the basics of ECC are enumerated. ECC is based on Galois Field algebra with either prime fields or binary extension Galois fields. The elliptic curve over which the ECC system is based is defined by the equation over the parameters (Q, C, D, G, P) –

$$y^2 = x^3 + Cx + D \qquad (1)$$

The reason that the ECC cryptosystem is considered tough to crack is because of the Elliptic Curve Discrete Logarithms problem, which states that it is extremely difficult to find a relation between two points A and B on the elliptic curve of equation (1) if both A and B are given. That is, it is computationally very hard to find a g that satisfies the equation below (where A and B are points on the elliptic curve) –

$$A = g.B \qquad (2)$$

In this paper, the ECC cryptosystem is used to generate keys for encryption. Here, the protocol can help generate a sharing secret for the user (over the same ECC system (Q, C, D, G, P)), which can be used as the encryption key.

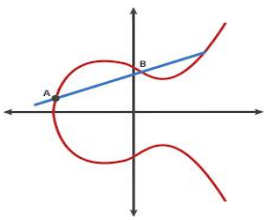

Fig.1 Elliptic Curve of eq. (1) with points A and B of eq. (2).

B. Security Scheme for Storing Data

The proposed security scheme for when the user initially tries to store data is explained in the steps below -

- *Step 1:* The first step of the algorithm involves dividing the data that the user wishes to upload into seven packets of equal size. Moreover, this step is necessary to prevent eavesdroppers who have somehow got hold of the encryption key.
- *Step 2:* Along with the seven data packets obtained in the last step, three bits are added at the end, signifying 1 (001), 2 (010), 3 (011), 4 (100), 5 (101), 6 (110), 7 (111). These 3 bit combinations can be added to any of the data packets randomly and they signify which cloud server the data packet will be stored in eventually. Thus, even eavesdroppers with keys will be unable to access the data, as it will be stored in fragments after being encrypted.
- *Step 3:* Using the ECC cryptosystem detailed initially a key K is generated and is used to encrypt the incoming data packets. However, quite obviously, the 3 bits that had been inserted at the end in Step 2 will not be encrypted.
- *Step 4:* The encrypted and fragmented data is then stored in its respective allotted cloud servers. Therefore, the last three least significant bits are checked and corresponding to the number they make, are either sent to Cloud Server 1, Cloud Server 2, Cloud Server 3, Cloud Server 4, Cloud Server 5, Cloud Server 6 or Cloud Server 7 for storage. The cloud number (001, 010, etc.) is appended to the end of the string at the time of storing, depending on which cloud it is stored in.

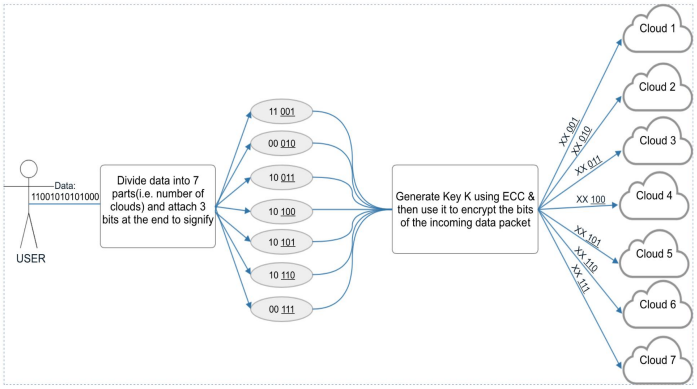

Fig.2 The working of the security scheme when data is stored in the Cloud

The example in Fig. 2 clearly illustrates the working of the algorithm. The security scheme is robust and is able to ensure user's privacy and security. An eavesdropper who even possesses the encryption key will be unable to utilize the user's data as it will be stored in fragments with no clear clue as to in what order it has been stored in. Moreover, the data will be encrypted using ECC to make it secure against other attacks as well.

C. Security Scheme for Accessing Data

The steps for this phase of the security scheme's working are explained below –

- *Step 1:* The data packets are collected from their allotted cloud servers and then all the bits except for the last 3 bits of each data packet are decrypted using the key K that had been generated in the storing-data phase.
- *Step 2:* The decrypted data packets are then combined together in the order signified by their last 3 bits, which were attached in the previous data-storing scenario. The first data packet is put first if its last 3 bits correspond to 001, second place if they correspond to 010, and so on.
- *Step 3:* The last 3 bits signifying the order of collection are then removed and the combined data is provided to the user.

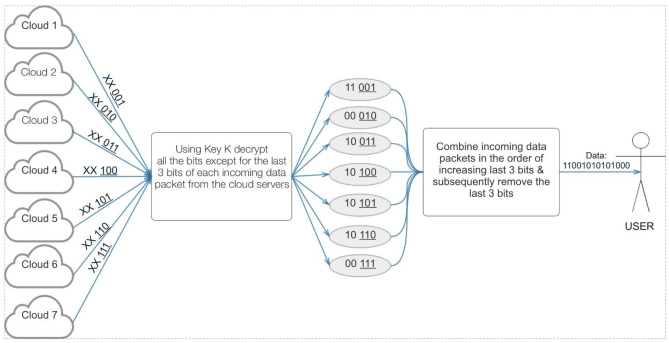

Fig. 3 The working of the scheme when data is accessed from the Cloud

Thus, it can be clearly seen that this phase is just a reversal of the storing-data phase. It can also be seen that the data is secure against eavesdroppers in both the phases as can be seen by the motivating examples in Fig. 2 and Fig. 3.

IV. Results And Analysis

The proposed security algorithm based on ECC, is run alongside RSA. For the same set-up, both ECC and RSA are compared and analyzed in terms of the time taken to encrypt and decrypt the data. It is observed that the proposed scheme outperforms RSA and is much faster in practical implementation.

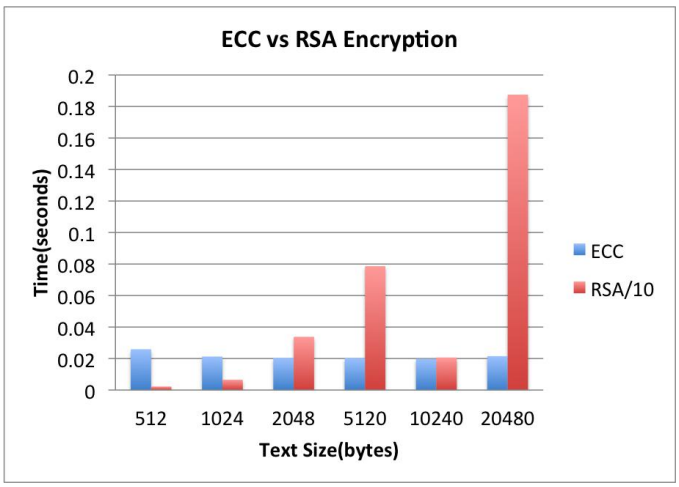

Fig.4

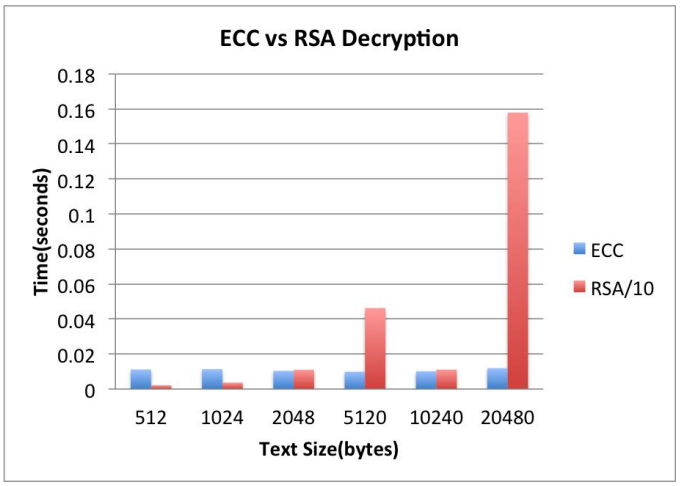

Fig.5

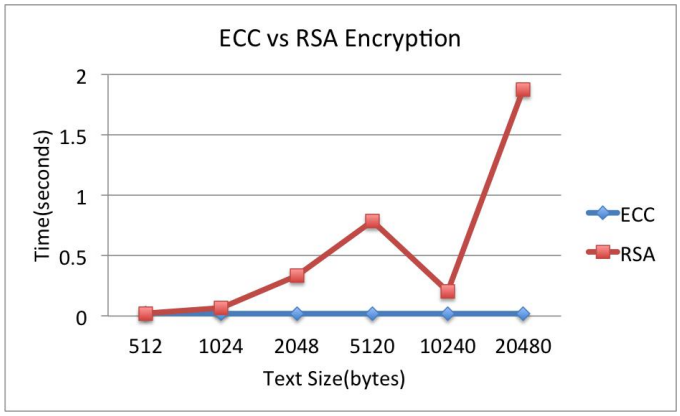

Fig.6

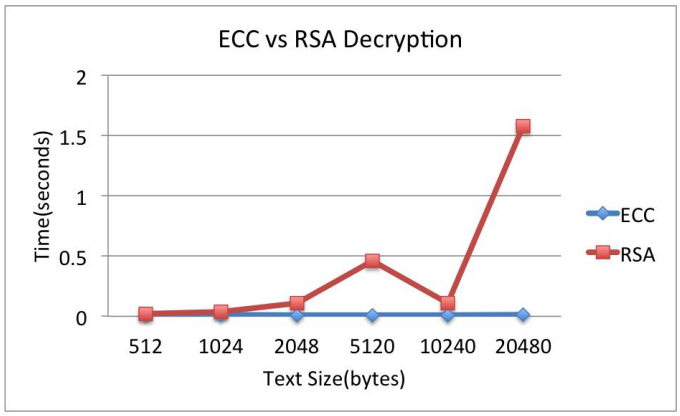

Fig.7

The results obtained are plotted as shown in Fig. 4 - Fig. 7. First, the time taken to encrypt the incoming data packets (in seconds) is plotted while increasing the size of the data. For variations in data sizes ranging from 512 Bytes to 20480 Bytes, encryption times are plotted for both the proposed scheme and RSA. The proposed ECC based scheme is much faster than RSA for encryption. This can be seen in Fig. 4 where the proposed ECC scheme's encryption time along with RSA's

encryption time (divided by 10) is plotted. This is done because as bytes are increased, RSA takes more time than ECC and eventually scales up by a magnitude of more than 10. The original values can be observed for ECC and RSA for encryption in Fig. 6. For decryption, in Fig 5, it is observable that the proposed scheme is again in fact lightweight compared to RSA. It takes significantly lesser time to decrypt the data as it is based on ECC. Here too, the magnitude of RSA has been scaled down by a factor of 10 since it takes so much more time than ECC. The actual magnitudes without scaling for decryption can be seen in Fig. 7. Thus, the proposed ECC based scheme is able to secure the user's private data effectively. It is an ideal choice for a security mechanism against eavesdroppers in Cloud storage services.

V. Conclusion

In this paper, a novel scheme for securing the Cloud against eavesdroppers has been proposed. The algorithm for the scheme, which is based on ECC, has been shown to be lightweight and effective. Moreover, it is able to effectively counter eavesdropping attacks as it fragments the data and then pseudo-randomly allots the different data packets to seven different cloud servers. ECC is used to generate the encryption key to secure the data against external threats as well. The scheme is shown to outperform RSA in terms of expediency in encryption and decryption times. It is faster than the RSA algorithm for both encryption and decryption by at least a factor of 10 in magnitude. At the same time it is excellent for alluding eavesdroppers. Thus, it is ideal for utilization in Cloud storage services, where users and their storage data are continuously increasing.

References

[1] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst. 24 (1) (2013) 131–143.

[2] Y. Li, W. Dai, Z. Ming, M. Qiu, Privacy protection for preventing data over collection in smart city, IEEE Trans. Comput. 65 (5) (2016) 1339–1350.

[3] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inf. Sci. 258 (2014) 355–370.

[4] M. Mozaffari-Kermani, A. Reyhani-Masoleh, A lightweight high-performance fault detection scheme for the advanced encryption standard using composite fields, IEEE Trans. Very Large Scale Integr. Syst. 19 (1) (2011) 85–91.

[5] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, H. Zhao, Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Gener. Comput. Syst. (2016) 1.

[6] S. Liu, Q. Qu, L. Chen, L. Ni, SMC: A practical schema for privacy-preserved data sharing over distributed data streams, IEEE Trans. Big Data 1 (2) (2015) 68–81.

[7] Tirthani, Ganesan: Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. Web: https://eprint.iacr.org/

[8] D. Mukhopadhyay, A. Shirwadkar, P. Gaikar and T. Agrawal, "Securing the Data in Clouds with Hyperelliptic Curve Cryptography," 2014 International Conference on Information Technology, Bhubaneswar, 2014, pp. 201-205.

[9] P. Rewagad and Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 437-439.

[10] M. Venkatesh, M. R. Sumalatha and C. SelvaKumar, "Improving public auditability, data possession in data storage security for cloud computing," 2012 International Conference on Recent Trends in Information Technology, Chennai, Tamil Nadu, 2012, pp. 463-467.