Privacy-Preserving in Cloud Computing with Security-as-a-Service

Divya Pritam
ME student, University of Mumbai
Department of Computer Engineering
Pillai Institute of Information Technology, New Panvel
Mumbai, Maharashtra
pritamdivya26@gmail.com

Madhumita A Chatterjee
Professor, University of Mumbai
Department of Computer Engineering
Pillai Institute of Information Technology, New Panvel
Mumbai, Maharashtra
mchatterjeee@mes.ac.in

Abstract— Cloud computing is on-demand delivery of data and IT resources in which applications are rapidly provisioned as standardized offerings to users over the web. In the recent years Cloud Computing has grown significantly, it became an important area of research and one of the vital areas in the redevelopment of the infrastructure of information technology. Cloud Computing has been classified into several models based on the type of service provided to customers. Cloud Computing has many benefits, as well as, it has many challenges and concerns such as: security, privacy, data integrity and other problems that make users and organizations fear to dealing with it. The main problem in Cloud Computing is the security of data. The proposed work focuses on secure data transfer by using different combination of mechanisms which not only ensure multi tier authenticities but also maintain the confidentiality of data and integrity of message in terms of authenticity, confidentiality and integrity of data. The proposed system aims to store data in a secure and safe way in order to avoid intrusions and attacks. Also, it will reduce the cost and time to store the encrypted data in the Cloud Computing. In this paper, ECC encryption and decryption algorithm has been proposed to maintain the confidentiality of data in transfer. The same algorithm is implemented in cloud architecture and is compared with the conventional RSA algorithm.

Keywords-*Cloud computing,Data Security,Privacy,Confidentiality,Integrity,Elliptic Curve Cryptography*

*****

I. INTRODUCTION

Cloud computing is the enlargement of different technologies that came together to change a company's way for building an IT infrastructure. The data outsourced on the cloud is regarded as important information to a person with malicious intent. There is so much of personal details as well as sensitive information that the companies store on their computers, and these details are now being transferred to the cloud. This makes it very fussy to explain the security measures taken by the cloud service provider and is fairly essential to take personal precautions to secure our information. Therefore, Data Security and privacy are the two major security concerns for the organizations to adopt cloud services. The organizations are reluctant to store their data outside their own premises because of the exposed security threats. As organizations tend to loose control over data in the cloud environments, they believe that the content stored in the cloud is more prone to security threats. A foolproof security plan must be provided to increase the level of trust between the cloud providers and the cloud consumers. The cloud providers must provide state of the art security solutions to establish the required level of trust. They have to prove scientifically that the data stored in the cloud is secure and only the authenticated and authorized personnel have the ability to access the cloud data.

The authentication mechanism plays a vital role in security enhancement. Authentication mechanism is like an entrance door and will allow only the trusted individuals to enter in the cloud premises. The mechanism should be robust enough to ensure availability by letting the right person in, any time and any place. At the same time, it must ensure confidentiality. Authentication mechanism can be combined with cryptographic techniques to ensure confidentiality of data. Data integrity can also be ensured if only authenticated persons can access the cloud services and proper encryption is done while transferring data. Having the best possible authentication mechanism along with a complete security plan can mitigate most of the security concerns of cloud consumers.

The existing solutions and techniques suffer with certain drawbacks. The major drawback being that the existing solutions focus more on privacy than security and Cloud Service Provider is given more privileges. So, here this solution aims mainly at securing the data and reducing the privileges of Cloud Service Provider.

This paper proceeds as follows. Section II reports related works, highlighting existing privacy-preserving security solution. Section III presents Proposed System which includes the CSP, Data Owner and Data User, emphasizing on securing the data, reducing the privileges of the CSP. Section IV presents the elliptical curve cryptography algorithm for encryption and decryption of data. Finally, section V concludes the paper.

II. RELATED WORK

There are several works which deals with general security issues of cloud computing but there are only few which deals with privacy of user in cloud. The authors Lukas Malina and Jan Hajny [1] presented a unique security solution for privacy-preserving in cloud services. This solution provided anonymous access to users who are registered to cloud services but CSP is given more privileges which is not good regarding the security point of view. Anonymous access phase is successful but focus is on privacy and not on security of data. Hu Shuijing [2] stated the basic problems arising in the cloud while accessing the data and the security related issues and countermeasures to tackle the problem. Issues like Unwanted Access, data segregation, vendor lock in, data romance, etc are covered in this paper. Ali A Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, Deqing Zou[3] presented an efficient scheme for privacy preserving password authentication for cloud computing. A system to prove the authenticated users identity without the need to admit their passwords is stated in this. The idea of using a Data Owner has been implemented in this paper. Here, in this paper privacy has been the main focus and not security of data. F. Amounas and E. H. El Kinani [4] presented a work based on the concept of ECC and provided a new method to secure the output of ECC. V. Gayoso Mart´ınez and L. Hern´andez Encinas [5] facilitated the usage of ECC in Java by analyzing the capabilities and dealing with key generation, key exchange, and digital signatures.

III. PROPOSED SYSTEM

The idea is to create a more secure service system i.e. Security as a Service (SECaaS) model which is available through the cloud. The goal of this model is to protect the information systems while allowing the attainment of business objective and preserving the availability, integrity and confidentiality of the information resources. Here, we consider a private cloud. The proposed ECC algorithm works whenever the data transfers from the Data Owner to CSP or from CSP to Data User or from Data Owner to Data User.

A. System Model

The proposed structure consists of the following entities:

- Cloud Service Provider (CSP): CSP offers its customers storage or software services available via a public network or private network.CSP is a company who is partially trusted. Whenever the user accesses the cloud service, the CSP validates the user and issues access attributes to users.
- Data Owner (DO): DO is a cloud client who registers with the CSP.DO outsources data to cloud in encrypted form. DO can anonymously get authenticated to cloud while getting duly authenticated.
- Data User (DU): DU is a cloud client who registers with the CSP. Whenever a DU query for data to the CSP, the CSP provides a list of DO who possesses the data. DU is also anonymous if they follow the rules of the CSP accordingly. Data User can be a Data Owner as well as Data Owner can be a Data User.

B. Security Requirements

The proposed system provides the following security requirements:

- *Confidentiality*: The time period to the CSP for every DU and DO is confidential. The data transmission between DO and the CSP cannot proceed without the initialization key.
- *Integrity:* The data sent to the DU can be modified only with the help of a secret key which would be sent via an e-mail to the DU.
- *Anonymity:* DU and DO identities are hidden if they behave honestly i.e. they stay anonymous while using the cloud services.

C. Phases in the Proposed System

The proposed system consists of the following phases in detail.

- *Registration:* A Data Owner/Data User has to register with the CSP and after successful registration receives an initialization key to access cloud services anonymously. A DO has to register in the cloud first by creating respective accounts and giving necessary details like user name, user id, password, email id and phone number and then upload the data files to the cloud service. If the cloud registration is successful then only it will authenticate the Data Owner and allow for further operation. Every time the Data Owner logs into the cloud, he/she is supposed to undergo the compulsory security questions. A Data Owner/Data User logs into the cloud by their respective email-id and the security answers to the question. If the Data Owner/Data User fails to attempt anyone one of the security questions their access is revoked.
- *Anonymous Communication:* In this phase, anonymous access is given to the duly authenticated users. I^{-th} user U_i anonymously accesses the cloud service. In this phase, the user is authenticated and an initialization key is sent to the user by the CSP.
- *File Selection:* The Data Owners and Data users as a whole can be called as Cloud Clients. The Cloud Clients store large volumes of data for maintenance and computation on the cloud. Cloud Clients can be either individual consumers or commercial organizations; the resources are virtualized by Cloud Service Providers according to the requirements of clients and expose them as storage pools. The Cloud Clients may buy or lease storage capacity from Cloud Service Providers, and store their individual data in these bought or rented spaces for future utilization.
- *Encryption:* The data is encrypted using ECC algorithm before uploading it the cloud by both the Data Owners as well as the Data Users to maintain the secrecy of data.
- *Data Upload:* Data Owner performs the duplicate check with the CSP to confirm if such a file is stored in cloud storage or not before uploading a file. If there is a duplicate file, the Data Owner/Data User can request the CSP to reveal the Owner of the file. If duplicate file does not exist the Data owner can upload the file.
- *Data Download:* If the Data user wants to download a file, he/she should first send request to Data owner. Data owner will decide to share data or not instead of CSP.
- *Decryption:* Data owner will send the decryption key to data user likewise.ECC (Elliptic Curve Cryptography) algorithm is used to decrypt the data.
- *Secure Communication*: Data confidentiality and integrity can be achieved if the user can upload and download data successfully from the CSP in the anonymous phase. We use the ECC algorithm to encrypt and decrypt the transmitted data between the DO, DU and CSP.

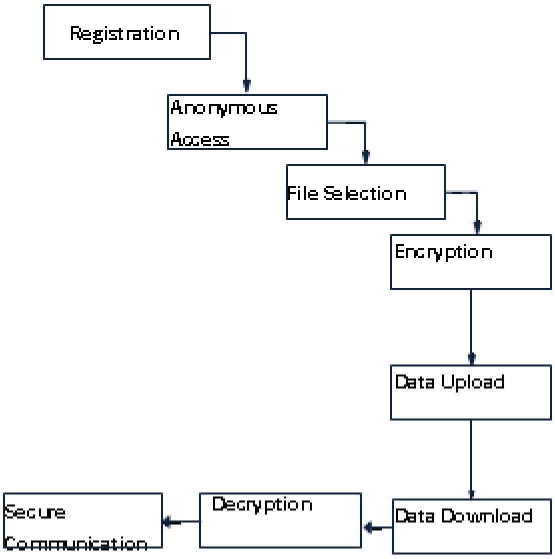

Fig. 1: Flow of Proposed System

Unlike other traditional models, the proposed system aims at reducing the time of data encryption as well as shorter key length for faster execution by making use of ECC algorithm. The proposed system also helps in increasing the protection of data and prevents its violation by the hacker, or even by the Cloud computing service providers themselves.

D. Communication between the Entities

In this section, how the three entities i.e. Data Owner, Data User and CSP communicate with each other is shown in detail:

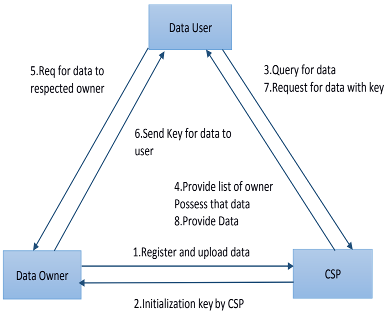
Data User
5.Req for data to respected owner
3.Query for data
7.Request for data with key
6.Send Key for data to user
4.Provide list of owner Possess that data
8.Provide Data
1.Register and upload data
Data Owner
CSP
2.Initialization key by CSP

Fig.2: Communication between Data owner, Data User, CSP

Data Owner registers with the CSP and CSP sends the initialization key to the Data Owner to his registered e-mail id. After successful registration Data Owner uploads the encrypted data to the cloud. The Data User who is a registered user query's for data to the CSP. The CSP then provides a list of Data Owners to the Data User who possesses the requested data. The Data User requests for data from the respected Data Owner. Now, it completely depends on the Data Owner to share the key to the Data User. Once the Data User has received the key, the Data User can download and decrypt the file from the CSP .Here, the privileges of the CSP has been reduced.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

In this section, ECC algorithm for encryption and decryption of data is detailed below using a flow diagram. ECC is an asymmetric key encryption algorithm for public-key cryptography. The equation of an elliptic curve is given as,

$$\mathbf{y^2= x^3+ax+b}$$

Where ***a, b*** are constants and ***x, y*** are variables.

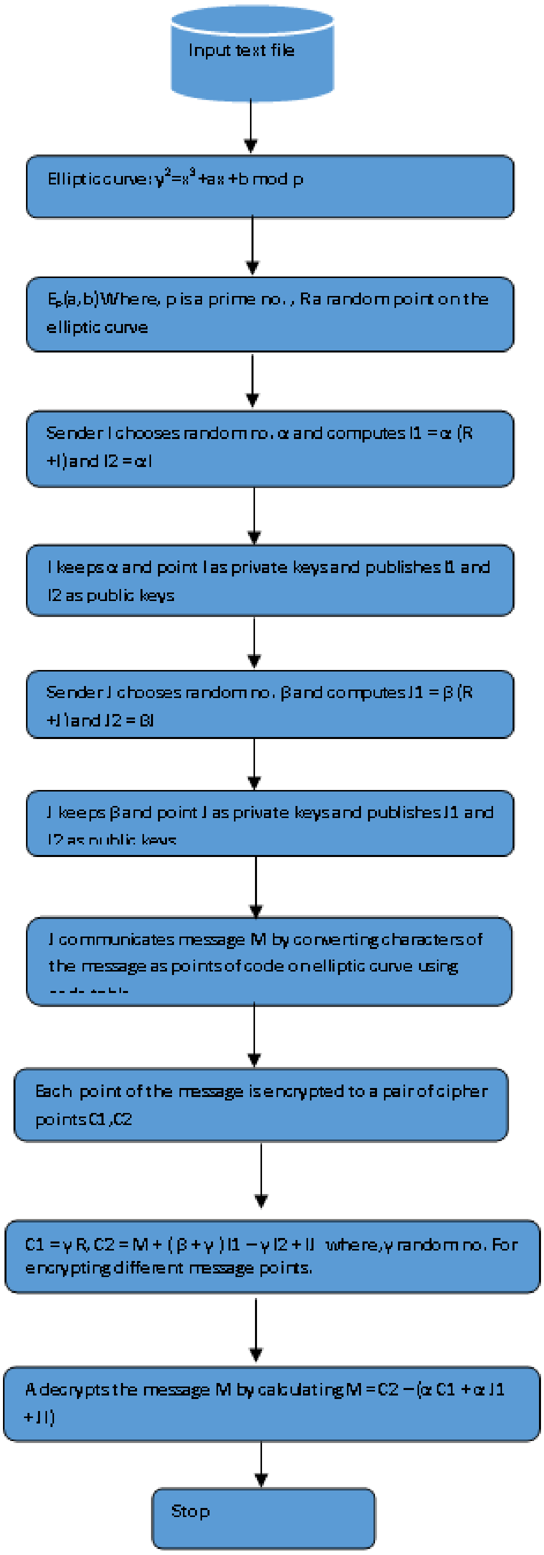
Input text file
Ellipticcurve:y²=x³+ax+b mod p
Eₚ(a,b)Where, p isa prime no., Ra random point on the elliptic curve
Sender I chooses random no. α and computes I1 = α (R +I)and I2 = αI
I keeps α and point I as private keys and publishes I1 and I2 as public keys
Sender J chooses random no. β and computes J1 = β (R +J)and J2 = βJ
J keeps β and point J as private keys and publishes J1 and I2 as public keys
J communicates message M by converting characters of the message as points of code on elliptic curve using
Each point of the message is encrypted to a pair of cipher points C1 ,C2
C1 = γ R, C2 = M + (β + γ) I1 − γ I2 + IJ where,γ random no. For encrypting different message points.
A decrypts the message M by calculating M = C2 − (α C1 + α J1 + J I)
Stop

Fig.3: Flow diagram for ECC encryption and decryption

In the public key elliptic curve cryptosystems, let us assume that a sender J wants to send a message M to sender I securely. The two communicating parties I and J communicate the message by using the coded table agreed by I, J and converting the characters of the message as code to the points on the elliptic curve. After encrypting all the characters of the message the parties convert the pair of points of each message point into characters of text using the code table. I, J announce their public key. The parties communicate the cipher text through public channel. I, J keep their private key secret. After receiving the cipher text, I, J convert the cipher text into the points on the elliptic curve and recognizes the points of each character and then decrypts the message.

A. Comparison of ECC and RSA-Based Algorithm

ECC gives equal security as compared to RSA but with the key size much smaller. Using ECC different public key cryptography schemes can get implemented. ECC provides similar security level as other cryptographic schemes but with smaller encryption keys which use fewer memory and CPU resources. The basis of ECC is group theory and field theory and its security is based on elliptic curve discrete logarithm problem.

In Table-1, the key sizes of ECC and equivalent RSA are compared. The table also shows that ECC gives similar level of security as RSA but with smaller key size. Therefore, with the smaller key size, processing power is also less compared to RSA. Hence ECC is favorable for small devices as compare to RSA.

ECC	RSA	Ratio
112	512	1:5
163	1024	1:6
192	1536	1:8
224	2048	1:9
256	3072	1:12
384	7680	1:20

Table 1: Equivalent key size recommended by NIST

V. CONCLUSION

In this paper, Security as a Service model for ensuring privacy preserving in cloud computing is explained .We reviewed the authentication and encryption structure for ensuring the security of data in cloud. The proposed model presents modifications to the current encryption models in Cloud Computing to increase the data security. The proposed model improves integrity of data for registered users and also provides the registered users to be anonymous in the authentication phase for confidentiality of data. The leakage of data by an authorized user is prevented using ECC algorithm. Security is a very crucial part in cloud computing so if proper measures are put in place it would give both the cloud service provider and the cloud user a great relief.

ACKNOWLEDGMENT

I wish to express my deep sense of gratitude to my project guide Dr. Madhumita A Chatterjee for her timely inputs and incalculable guidance to improve my work. I would also like to thank my family for being understanding and supportive throughout. Their help cannot be penned with words.

REFERENCES

[1] Lukas Malina, Jan Hajny, "Efficient Security Solution for Privacy-Preserving Cloud Services", IEEE, 2013.

[2] Hu Shuijing," Data security: The challenges of Cloud Computing",IEEE, 2014.

[3] Ali A Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, Deqing Zou," A Practical Privacy- preserving Password Authentication Scheme for Cloud", IEEE,2012.

[4] F. Amounas and E. H. El Kinani," ECC Encryption and Decryption with a Data Sequence", Applied Mathematical Sciences,2012.

[5] V. Gayoso Mart´ınez and L. Hern´andez Encinas, "Implementing ECC with Java Standard Edition 7", International Journal of Computer Science and Artificial Intelligence,2013.

[6] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan," Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption",IEEE, 2015.

[7] Hong Liu, Huansheng Ning, Qingxu Xiong, Laurence T. Yang," Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE, 2015.

[8] Peter Mell ,Tim Grance, "The National Institute of Standards and Technology (NIST),Information Technology Laboratory definition of Cloud Computing",Version 15,2009.