ISSN:0975-9646

Dataset Segmentation for Cloud Computing and Securing Data Using ECC

Vidyanand Ukey, Nitin Mishra

Information Technology Department,
RGPV University

Abstract - **In the cloud, the data is transferred among the server and client. Cloud security is the current discussion in the IT world. This research paper helps in securing the data without affecting the original data and protecting the data from unauthorized entries into the server, the data is secured in server based on users' choice of security method so that data is given high secure priority. In this technique the data are segmented into three different levels according to their data importance ranking, set by data owner. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is 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. The paper will conduct a performance analysis by implementing the Elliptic Curve Cryptography (ECC) in all levels in order to check the performance of model.**

Keywords - **Cloud Computing, Elliptical Curve Cryptography, Encryption, Segmentation.**

I. Introduction

Defining cloud computing becomes a difficult task with many definitions, yet no consensus on single or unique ones. Cloud computing refers to a network of computers, connected through internet, sharing the resources given by cloud providers catering to its user's needs like scalability, usability, resource requirements. The USA National Institute of Standards and Technology(NIST) defines it as follows [1]: "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." Cloud computing allows users to access software applications and computing services. They might be stored off-site at locations rather than at local data centre or the user's computer [4]. Cloud computing caters to users' request for services. There is no need to spend money on purchasing and managing of resources. The three widely referenced cloud computing service models are explained as follows.

1. Software as a Service (SaaS): Also known as Application Service Provider or ASP model. It refers to service that gives users' the efficacy to access services of cloud by running simple software like a browse. Examples: Gmail, Google Groups.

2. Platform as a Service (Paas): This service allows the users' to develop applications and deploy them. Examples: Google App Engine allows developers to create customized apps.

3. Infrastructure as a Service (IaaS): This service allows users' to access the servers' computational and storage infrastructure in a centralized service [2] [3] [6]. Say for an example, we have Amazon Web Services. It allows remote access to Amazon.com's computing services.

In Cloud computing domain, there are set of important policies, which include issues of privacy, anonymity, security, liability and reliability [2]. The most important of these issues is the data security and how cloud providers assures it [2]. Most effective technique to protect our data is its encryption. Different encryption schemes for protection of data have been in use for many decades. Encryption of data is done by converting data from normal plaintext to unreadable cipher text. This tactic, however, doesn't prove to be much effective for cloud systems as this conversion involves huge and very complex mathematical computations.

II. Issues In Cloud Security

A guaranteed security service will enhance the business performance of the cloud service provider. Security is an essential service to be provided to the clients, a cloud service provider should assure. Secure cloud is a reliable source of information. Protecting the cloud is a very important task for security professionals who are in charge of the cloud. Cloud can be protected by protecting the data, making sure data is available for the customers, delivering high performance for the customers, using Intrusion Detection System on cloud and to monitor any malicious activities. For the safety purpose, the provider's must provide a support system for the client's so that every client must be able to recover their own data loss in the cloud environment. Therefore, the encryption technique must be adopted in cloud by the provider's to their client's for integrity and authentication of data. When it comes to Security, cloud has lot of difficulties. The provider's must make sure that the client does not face any problem such as data loss or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user and there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud. The various problems faced by the cloud computing can be classified as:

1. Data protection:

To be considered protected, data from one customer must be properly segregated from that of another; it must be stored securely when "at rest" and it must be able to move securely from one location to another. Cloud providers have systems in place to prevent data leaks or access by third parties. Proper separation of duties should ensure that auditing or monitoring cannot be defeated, even by privileged users at the cloud provider.

2. Authentication:

The authentication of the respondent device or devices like IP spoofing, RIP attacks, ARP poisoning (spoofing), and DNS poisoning are all too common on the Internet. TCP/IP has some “unfixable flaws” such as “trusted machine” status of machines that have been in contact with each other, and tacit assumption that routing tables on routers will not be maliciously altered. One way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged.

3. Data Verification:

Things like tampering, loss and theft, while on a local machine, while in transit, while at rest at the unknown third-party device, or devices, and during remote back-ups. Resource isolation ensures security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache.

4. Infected Application:

Vendor should have the complete access to the server for monitoring and maintenance, thus preventing any malicious user from uploading any infected application onto the cloud which will severely affect the customer. Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures (application-level firewalls) be in place in the production environment.

5. Availability:

Cloud providers assure customers that they will have regular and predictable access to their data and applications.

III. Literature Survey

In 2010, Joshi et al. [1] provide an overview of different data security issues related to cloud computing. This piece of work focuses on ensuring security in cloud computing by providing secured trustworthy cloud environment. Farzad Sabahi [2] explains about the scope of various enterprises migrating to cloud. The author explains how migration to cloud can benefit various enterprises. Cloud computing migration involves considering the gravity of issue of security. In 2011, Ashish Agarwal et al. [3] talk about security issues concerned with cloud computing. This paper has talked about some serious security threats that prevails this field. Ashutosh Kumar et al. [4] focused on providing a secure architectural framework for sharing and data gathering. This cynosure of this work is that the authors have made a permission hierarchy at different levels. The authors have focused on security but with view of use hierarchy. In 2012, M.Venkatesh el al [5] proposes RSASS system for data security. The scheme uses RSA algorithm for encrypting large files and storing the date. The system can be used for storing large databases. But the use of linear methods compromises with the data retrieval speed. Hence, this system is good for static data. Prashant Rewagad et al. [6] propose a system for providing security in cloud network. The architecture uses the combination of digital signature algorithm of Diffie Hellman and AES encryption.

Kui Ren [16], proposed the publicly auditable cloud data storage which is able to help the cloud economy become fully established. This auditing service helps the data owners’ to maintain their data effectively that is present in the cloud storage. The proposed system accounts the users regarding the usage of their data by both the user himself and the TPA. Services for the legacy users is made available, who may not only access but also modify the data in the cloud. Farzad Sabahi [2], proposed a system that deals with the problem of ensuring the integrity of data storage in cloud with the help of a Third Party Auditor. Data integrity is achieved through the public auditing that is carried out on the users data by the Third Party Auditor. Block tag authentication is made to handle the data from the cloud storage efficiently. For the data that is stored in the cloud database, there is need for remote data integrity check which assurers the cloud users with a sense of security regarding their data. The third party audit ting has to be made available in such a way that no additional burden is introduced to the cloud users. A single Third Party Auditor is capable of handling multiple auditing tasks, which is achieved with the bilinear aggregate signature technique. Aderemi A. Atayero [17], proposed an auditing system which is carried out in such a way that the Third Party Auditor does its job without demanding the copy of user’s data. Also the Third Party Auditor is not capable of deriving the user’s data while performing the auditing task. To verify the correctness of the cloud data on demand from the cloud users the Third Party Auditor is used, who without retrieving a copy of the whole data or introducing additional online burden to the cloud users performs the auditing.

IV. Problem Statement

The security of data of the user is prime responsibility of cloud provider. So, for efficient data security we need a mechanism that provides secure data encryption as well as secure shield against data theft. The related works mentioned above have focused on cloud security issues. They have provided different mechanisms for data security in cloud environment. Different researches have focused on the fact that user generally has to access large volumes of data from the cloud in a secured manner. But the complexity of the cryptographic algorithm used, hasn’t been given much importance. The complexity of the algorithm directly affects the speed of data access. We need some algorithm that will help in efficient and speedy secured data access.

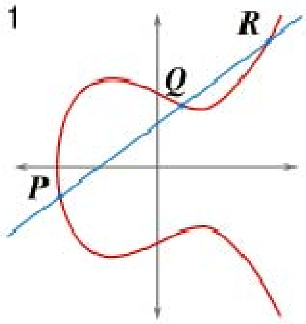
V. Elliptic Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,
E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)



$$y^2 = x^3 + ax + b$$

Fig 3

The fig 3 shows simple elliptic curve.

5.1 Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver’s public key and the receiver will decrypt its private key.

Now, we have to select a number‘d’ within the range of ‘n’.

Using the following equation we can generate the public key

$$Q = d * P$$

d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve.

‘Q’ is the public key and‘d’ is the private key.

5.2 Encryption

Let ‘m’ be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details.

Consider *‘m’* has the point *‘M’* on the curve *‘E’*. Randomly select ‘k’ from [1 - (n-1)].

Two cipher texts will be generated let it be C1 and C2.

$$C1 = k*P$$

$$C2 = M + k*Q$$

C1 and C2 will be send.

5.3 Decryption

We have to get back the message ‘m’ that was send to us,

$$M = C2 – d * C1$$

M is the original message that we have send.

VI. PROPOSED SYSTEM

In this proposed scheme the data are segmented into three different levels according to their data importance ranking set by data owner. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is 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. The paper will conduct a performance analysis by implementing the Elliptic Curve Cryptography (ECC) in all levels in order to check the performance of model.

VII. CONCLUSION

In this study different security issues research papers were studied briefly. In both larger and smaller scale organizations they are using cloud computing environment because of large advantage of cloud computing. The cloud computing has different security issues in threats in user view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. The bond between service providers and users is necessary for providing better cloud security.

Several attempts had been made at providing a secured environment for activities in the Cloud. Elliptic Curve Cryptography (ECC) provides solutions for a secured Cloud environment with improved performance in cloud computing and resource usage. This makes it attractive for secure cloud applications. ECC had provided a robust and secured model for the development and deployment of secured application in the Cloud. This work would promote confidence in both large and small scale organization in Cloud investment.

REFERENCES

[1] Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.

[2] Farzad Sabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[3] Ashish Agarwal, Aparna Agarwal. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946].

[4] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG), CSI Sixth International Conference, Sept. 2012

[5] M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. Recent Trends In Information Technology (ICRTIT), 2012 International Conference, April 2012.

[6] Prashant Rewagad, Yogita Pawar in. 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.

[7] Hai Yan, Zhijie Jerry Shi. Software Implementations of Elliptic Curve Cryptography. Information Technology: New Generations, Third International Conference, April 2006.

[8] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 1976.

[9] Ravi Gharshi, Suresha. Enhancing Security in Cloud Storage using ECC Algorithm. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 7, July 2013.

[10] H. Modares, M. T. Shahgoli, H. Keshavarz, A. Moravejosharieh, R. Salleh. Make a Secure Connection Using Elliptic Curve Digital Signature. International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 ISSN 2229-5518 IJSER © 2012.

[11] Aqeel Khalique Kuldip Singh Sandeep Sood. Implementation of Elliptic Curve Digital Signature Algorithm. International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010

[12] Alfred Menezes, Minghua Qu, Doug Stinson, Yongge Wang. Evaluation of Security Level of Cryptography: ECDSA Signature Scheme. Certicom Research. January 15, 2001.

[13] W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003.

[14] Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.

[15] Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO 85

[16] Kuyoro S. O, Ibikunle.F and Awodele O, Challenges and Security Issues in Cloud Computing *International Journal of Computer Networks, Vol. 3, No. 5*, pp. 247-255, 2011

[17] Aderemi A. Atayero, Oluwaseyi Feyisetan , Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption, *Journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 10*, October 2011