IJETCR Open Access

ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 2; Page No. 63-67

Data Security and Privacy Protection with Cryptography in Cloud Computing

Akshita Sharma

M. Tech. Scholar, Department of computer science and Engineering

Jayoti Vidyapeeth Women's University, Jaipur,

Rajasthan (India)

ABSTRACT

It is well known that cloud computing has Many potential advantages and it plays a vital role in Present day to day life. It helps users to maintain their data over the internet by widening its wings in all fields to deliver services. Data security has consistently been a major issue in information technology. Cloud computing has several customers such as ordinary users, and enterprises who have different motivation to move to cloud. In cloud computing environment, data security becomes particularly serious because the data is located in different places even in the entire globe. In cloud architecture, Data security and privacy protection Issues are relevant to both hardware and software. When the Issues of cloud security come up, security threats such as maintenance of data integrity, data safety and data hiding dominate clients concerns. The data communication on the internet or over any network is at risk to the attackers attack. So, in order to secure the data some encryption scheme is used. This paper serve a concise analysis on data security and privacy protection and its issues associated with cloud computing. Then this paper provides cryptographic techniques, Elliptic Curve Cryptography for data encryption/Decryption was used along with Diffie Hellman based on Elliptic Curve mechanism for connection establishment.

Keywords: Cloud Computing, Data security, Privacy Protection, Elliptic curves cryptography.

1. INTRODUCTION:

Cloud Computing is an emanating technology in which enormous data are distributed across different storage servers. The explanation of "cloud computing "from the National Institute of Standards and Technology (NIST) is that cloud computing enables ubiquitous, 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[1].It provides development environment, allocation and reallocation of resources when needed, storage and networking facility virtually. Garter defines cloud computing as "a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies"[2] . The Cloud Computing model NIST defined has three service models (also called SPI model) and four deployment models. The three service models are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS). In SaaS, Software with the related data is deployed by a Cloud Service Provider, and users can use it through the web browsers. In PaaS, a Service Provider facilitates services to the users with a set of software programs that can solve the specific tasks. In IaaS, the Cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities. The four deployment models are: Private cloud, Community Cloud, Public Cloud and Hybrid cloud. In Private cloud, the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. In community Cloud, The Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. In Public Cloud, The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. In Hybrid Cloud, Hybrid Cloud refers to the combination of both public and private cloud.

Cloud computing delivers various advantages to the organizations who decide to adopt it. Cloud computing is the promising development platform of IT industry which provides organizations with an efficient, flexible and cost effective substitutes to host their resources. Regardless of potential benefits, there are several issues which are

Corresponding author: Akshita Sharma

threat to the cloud consumers and that impact the cloud model reliability and passiveness. Cloud Security is the main fear that hinders the implementation of cloud computing model. The popularity of Cloud Computing is largely due to the factuality that various enterprise applications and data are moving into cloud platforms; nevertheless, inadequacy of security is still the key hurdle for cloud implementation [3]. According to a survey from IDCI in 2009, 74% IT managers and CIOs believed that the primary challenge that hinders them from using cloud computing services is cloud computing security issues [4].

2. Issues In Cloud Computing Security

A. cloud computing security

Cloud computing security (sometimes referred to simply as "Cloud Security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies and controls deployed to protect data, applications, and the associated infrastructure of cloud computing [5].

B. Security Issues Associated with the Cloud

Several security issues can affect the cloud security levels, the following are a short list of these [6] [9] [10].

- Privileged user access: Processing sensitive data outside the enterprise faces the risk of logical, physical and personnel control.
- Regularity compliance: Even when the data is held by the providers, the clients have the responsibility of their data security and integrity.
- Recovery: When the cloud server is down, what will happen to the client data? Can it be restored easily? Clients don't prefer to let go their data control to a third party.
- Viability: The availability of the data after faults (provider's faults) or go-broke taking a place in the clients thinking.
- Data segregation: Data from customers share the same environment with other customer's data using encryption is efficient but is it enough.
- Data location: When moving to cloud computing, clients will not know where their data is stored, because the cloud uses distributed storages for hosting the data. Such issue decreases data control by its owner. Is this acceptable by the client?
- Investigative support: Investigating service of the cloud is difficult because multiple customers' logging to their data is spread and collected via a set of data centers/servers.

Mohamed Al Morsy, John Grundy and Ingo Muller explored the cloud computing security issues from different perspectives , including security issues associated with cloud computing architecture, service delivery models, cloud characteristics and cloud stakeholders [7].

Yampi Chen, Vern Paxton and Randy H. Katz believed that two aspects are to some amount new and necessary to cloud: the complexities of shared trust considerations, and the resultant need for mutual audit facility. They also place out small new opportunities in cloud computing security [8]. According to the SPI service delivery models, deployment models and essential characteristics of cloud, there are security issues in all aspects of the infrastructure including network plane, swarm level and purpose level.

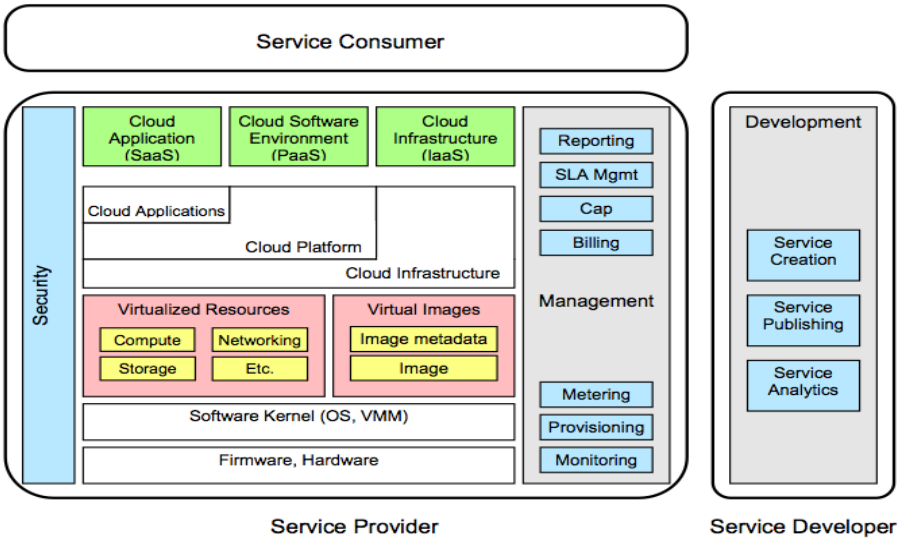

Figure 1: Cloud computing Security Architecture

3. Data Security and Privacy

"Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security." Data stored in the cloud is stored in other places and needs to consider 3 aspects of information security. Confidentiality, Integrity and avail-ability. Common solution for data confidentiality is data Encryption.

Privacy in cloud computing can be defined as "the ability of an entity to control what information it reveals about itself to the Cloud (or to the Cloud SP), and the ability to control who can access that information [11].Numerous existing privacy laws impose the standards for the collection, Maintenance, use, and disclosure of personally identifiable information (PII) that must be satisfied even by Cloud SPs [12]. The major problem regarding privacy in Cloud is how to secure PII from being used by unauthorized users, how to prevent attacks against privacy even when a Cloud SP cannot be trusted, and how to maintain control over the disclosure of private information. Handing sensitive data to another company is a serious concern. Are data held somewhere in the Cloud as secure as data protected in user-controlled computers and networks. Cryptography can be used for the protection of data. Cryptography means hide the existence of information or Make the information secure from intruders. Encryption of data is the process of converting data from normal plaintext to unreadable cipher text. The original plain text message is in simple English language that can be understood by everyone. The codified message by cryptographic techniques is called as cipher text message [13] [14]. There are several authentication and encryption mechanism that are applied for data security in cloud computing and various algorithms such as ECC, RSA, RC4 and El Gamal have been suggested and discussed for Cloud Computing. It was resulted that Elliptic Curve Cryptography is a good approach with smaller size of data for security purposes.

4. 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:

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

Terms that will be used,

E-> Elliptic Curve

P-> Point on the Curve

n-> Maximum limit (This should be a prime number)

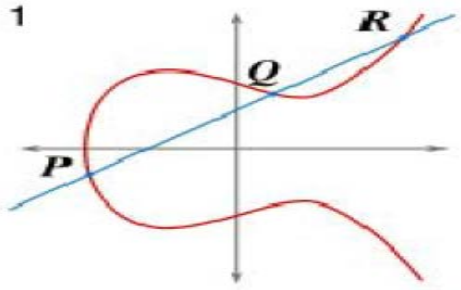

Figure 2: Simple Elliptic Curve

4.1. 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 with 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.

4.2. 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 sending.

4.3. 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.

5. Diffie Hellman Key Exchange Based On Elliptic Curve

Diffie Hellman establishes a shared secret. It can be used for secret communications by exchanging data over a public network [15]. Table 1 illustrates the general idea of the key exchange by using Elliptic curve points instead of a very large number. The key part of the process is that Bob and Alice exchange their secret points in a mix only. Finally, this generates an identical key that is mathematically difficult to reverse for third party that might have been listening in on them.

Table 1: Diffie Hellman based on ECC for key exchange

BOB	ALICE
Common agreement on elliptic curve[1, 18, 19], base point (g) (8, 5) and number of points on the curve (n) [19]	
Select private key [K] [3]	Select private Alice (s) [7]
Generate public key as point on the curve = multiple (g, k) = (15, 18)	Generate public key as a point on the curve. = multiple (g, s) = (18, 4)
Exchange the public keys = multiple (g, s), =(18, 4)	Exchange the public keys = multiple (g, k), (15, 18)
Generate shared secret based on public point and the private key = multiple (g, s*k), =(1,18)	Generate shared secret based on public point and the private key = multiple (g, k*s), = (1, 18)

The client wants to send a message to cloud. The client hashes the message. It generates a message digest in a form of integer. The client concatenates the message with integer digest. This message is encrypted by the client. The encrypted message sends to the cloud. The cloud gets the encrypted message and identifies the client based on the shared key. The cloud decrypts the message. The decrypted message is verified by generating the signature. At that stage, the data is available for insert, delete, modify or update.

The connection establishment used Diffie Hellman key based on Elliptic Curve Cryptography Algorithm. This algorithm used to generate a shared secret key between both of them. The shared secret key is used to provide a secure message authentication and message integrity, along with no repudiation of message and data confidentiality. It occurs during the account creation. It represents one time password. The shared secret key generates each login time. To generate the shared secret key, the cloud and the client must agree on a set of parameters ones. These parameters named the elliptic curve equation, the parameter values of the curve (a, b), the field number (a big prime number q), order of the curve, and a base point named (g).

In each login time, the client generates a private key named ($userID$). This key is used to generate a public client key based on the elliptic curve called ($userpup$), where $userpub$=$userID*g$. On the other side, the cloud generates a private key named ($cloudID$). This key is used to generate a public cloud key named $Cloudpub$, $Cloudpub$=$cloudID$*g.

The client used $cloudpup$ along with his private $userID$ to generate the shared secret key named $Skey$= $userID*.Cloudpub$. At a synchronize time the cloud generates same shared secret key $Skey$= $cloudID*userpub$. This key used to identify and to authenticate the client in the cloud environment. It represents a key for resource accessing on the cloud.

Pseudo code for Diffie Hellman based on elliptic curve in cloud side:

Step 1: common agreements between client and cloud provider.

(Elliptic curve, base point named g, a big prime number named q and finally the order of the curve named N)

Step 2 **In cloud side:** Generate a private key named $\boldsymbol{cloudID}$ as an integer. Where 0 < $\boldsymbol{cloudID}$ < N, Compute $\boldsymbol{Cloudpub}$ = $\boldsymbol{cloudID*g}$

In client side:

Generate a private key named as an integer where 0< $\boldsymbol{userID}$ <N

Compute $\boldsymbol{userpub}$= $\boldsymbol{userID*g}$

Step 3: Exchange public key between cloud and client.

Step 4: Generate shared key for both client and cloud.

$\boldsymbol{Skey}$= ==$\boldsymbol{cloudID*\ userpub}$

6. Conclusion and Future Scope

In this paper, we explored the cloud computing environment and tried to discuss security and privacy concerns related to cloud computing. The challenges in privacy protection are sharing data while protecting personal information. Cloud Computing has enormous prospects, but the security threats embedded in Cloud Computing approach are directly proportional to its offered advantages. Security of the Cloud relies on trusted computing and cryptography. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. A service provider needs to ensure that applications are safe from all possible attacks. Various techniques have been used for the data security and privacy protection but separation of sensitive data and access control is a serious concern. We used encryption for data security.

In our proposed work, only the authorized user can access the data. Data security is provided by ECC with the secure connection establishment by Diffie- Hellman key exchange based on ECC. Data security can be very good assured by use of linear cryptographic algorithms put large amount of data in cloud resents a hindrance to the idea. Cryptography based on ECC provided robust and secured model for cloud applications. In future, it can use different key size along with elliptic curve with different parameters. Different encryption algorithm can be used.

7. REFERENCES:

1. P.Mell and T. Grance, "The nist definition of cloud computing," National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009.
2. Gartner. Predicts 2014: Cloud Computing Affects All Aspects of IT Technical report. http://www.gartner. com / technology/ topics/cloud-computing.jsp
3. Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, "Securing Cloud computing Environment against DDoS Attacks", IEEE, , pp. 1-5,2011.
4. Sun Cloud Architecture Introduction White Paper (in Chinese).http://developers.sun.com.cn/blog/function al ca /resource/sun_353cloudc omputing_chinese. pdf.
5. Cloud computing security, http://en.wikipedia.org/ wiki/ Cloud_computing_security.
6. Rani, A. M. G., & Marimuthu, A. (2012). A Study on Cloud Security Issues and challenges. Int.J.Computer Technology & Applications, Vol. 3(1), pp. 344-347.
7. Mohamed Al Morsy, John Grundy, Ingo Müller, "An Analysis of The Cloud Computing Security Problem," in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.
8. Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About Cloud Computing Security?"Technical Report No. UCB/EECS-2010-5.http://www.eecs. berk-eley. edu /Pubs /TechRpts/2010/EECS-2010-5.html
9. Kumar, S., & Goudar, R. H. (2012). Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication, Vol. 1(4), pp. 356-360.
10. Chandrahasan, R. K., Priya, S. S., & Arockiam, L., (2012). Research Challenges and Security Issues in Cloud Computing. International Journal of Computational Intelligence and Information Security, Vol. 3(3), pp. 42-48.
11. P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Ben Othmane, L. Lilien, and M. Linderman, "A User-Centric Approach for Privacy and Identity Management in Cloud Computing," Proc. 29th IEEE Intl. Symp. on Reliable Distributed Systems (SRDS), New Delhi , India, Nov. 2010.
12. R. Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," World Privacy Forum, Feb. 2009. Online at: http://www.worldprivacy forum.org/pdf/WPF_Cloud_Privacy _Report.pdf
13. William Stalling, A Handbook on "Cryptography and network Security" by Pearson Education, 2009
14. A. Jaber, M. Fadlili, "The Use of Cryptography in Cloud environment", IEEE International Conference and Computing and Engineering, December 2013.
15. Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-3, July 2012