A Secured Cloud System using Hyper Elliptic Curve Cryptography

Mrs. S.Selvi, Dr. R. Ganesan

Abstract — Secure and efficient data storage is needed in the cloud environment in modern era of information technology industry. In the present scenario the cloud verifies the authenticity of the cloud services without the knowledge of user's identity. The cloud provides massive data access directly through the internet. Centralized storage mechanism is followed here for effective accessing of data. Cloud service providers are normally acquires the software and hardware resources and the cloud consumers are avail the services through the internet access in lease basis. Cloud security is enhanced through cryptography technique applied to the cloud security to avoid vulnerability. The intractable computability is achieved in the cloud by using the public key cryptosystem. This paper proposed the approach of applying Hyper elliptic curve cryptography for data protection in the cloud with the small key size. The proposed system has the further advantage of eliminating intruder in cloud computing. Efficacy of the system is to provide the high security of the cloud data.

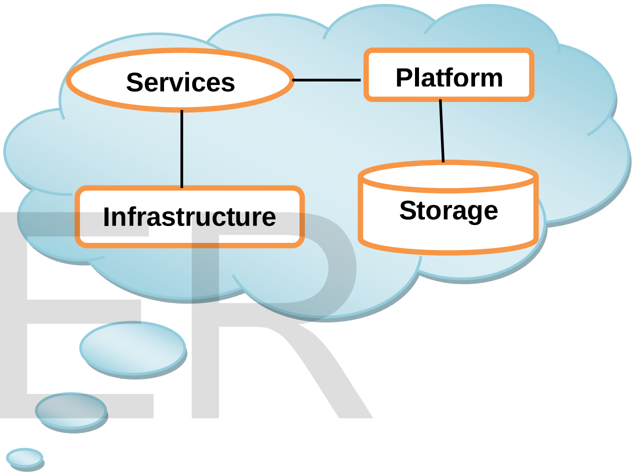
Keywords — Data Storage, Data Security, Encryption, Hyper Elliptic Curve Cryptography.

I. INTRODUCTION

Cloud Computing stands on the concept of virtualization. In other way we can say that virtual computers are the components of cloud. To get better understanding, one should be familiar with the basic concepts of cloud computing. Generally people often think incredible services available in cloud is cloud computing. But in fact cloud computing is fundamental model of separating the whole thing like applications, software and even the infrastructure from the hardware an individual using on. Eg. Google Doc is a traditional web application, Google spreadsheet, Zen, Quick Books and many more. According to the NIST definition 'Cloud computing is a model for enabling 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'. The idea behind making use of cloud computing is storing our own data in a much secured manner as well as in an affordable way.

In case of fatal damages such as system crash, software error or Operating System corrupt, one may lost all essential data and left with nothing in hand. The common technique is one can have entire backup of the system. However that is too expensive and not affordable to everyone to have external hard disk. The alternative way is one can purchase some storage from any of the cloud service providers and can store their data. If the system goes down or OS is crashed then the data is not misplaced as it is protected up in the cloud i.e. server of the service providers. Currently Amazon, Rackspace, Google, Microsoft, VMware, iCloud and Drop Box are the foremost Cloud Service Providers.

The basic cloud computing architecture



The figure shows that the cloud services are provided as a platform and as an Infrastructure. User interactions with the cloud, providing services from the cloud are managed with applications in languages like java, PHP etc. Front ends of web based applications for user interactions are provided with cloud platform. Remote accessing environments are created with Cloud infrastructure. The user requests with the web based application are sent to the database i.e. cloud storage.

ESSENTIAL CHARACTERISTICS:

According to NIST description the cloud characteristics are

Service from the Cloud:

A consumer can requesting services such as email, applications, network as needed automatically without service provider interaction.

Huge network access:

Cloud providers provides services everywhere over the network and accessed through standard mechanisms implemented with the thin or thick client platforms such as mobile phones, laptops and PDAs.

Location independent resource pooling:

Multi-tenant model are used in order to serve numerous consumers with different physical and virtual pooled resources like storage, bandwidth, memory and processing. These resources are allocated to the consumers dynamically released when job is done as the consumer request with higher level of abstraction.

Scalability in cloud:

Service delay at the consumer end happens every so often as the consumers demand is extraordinarily high. Cloud has most significant feature called scalability to overcome such an issue. The resources provided to the consumer can be elastically provisioned and released.

Paid Service:

Service providers charging the consumers as charge-per-use basis as their usage of server. Types of services like storage, processing, bandwidth etc. are leveraged at some level of abstraction as cloud system automatically control and optimize resources. And the monitoring, controlling and reporting of resources usage are done in order to provide transparency for provider as well as for consumer using the service.

II. ISSUES IN CLOUD SECURITY

A guaranteed security service will augment the business performance of the cloud service provider. Security is a crucial service to be offered to the customers, a cloud service provider ought to assure the security. Secure cloud is a consistent source of information. Securing the cloud is a very essential task for security professionals who are responsible 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 monitoring every malicious activity. For the protection purpose, the service provider must provide a support system for the clients in order that each client must be able to recover their data failure in the cloud environment. Hence, the encryption method must be implemented in cloud by the service providers to their clients for reliability and authentication of data. The cloud has to face lot of difficulties while get nearer to Security. The providers must make certain abstraction that the client does not face any problem such as data loss or data theft. A range of problems faced by the cloud computing can be categorized as:

Data protection: Data from one customer must be accurately isolated from that of another; Data has to be kept while “at rest” and must be able to move safely from one location to another. Cloud providers have monitoring systems in place to prevent data leaks or access by third parties.

Authentication and Access Control: The authentication capabilities within all virtual systems by the provider should copy the way other physical systems authenticate. One time password and biometrics should all be implemented in the same approach. Thus all encrypted data should provide authentication technique from one cloud to another. To accomplish this tedious and distinctive technique of authentication, it is desirable that digital signature should be applied in cloud data transfer.

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 the integrity of data to be checked. 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.

Infected Application: Cloud providers make sure that applications available as a service through the cloud are secured by executing, testing and acceptance procedures for outsourced or packaged application code.

Availability: Cloud providers assure clients that they will have standard and predictable access to their data and applications.

III. PROBLEM STATEMENT

The security of consumer’s data is major responsibility of cloud provider. For efficient data security, a proposed mechanism that provides secured data encryption as well as protected shield against data theft. Different researches have focused on the statement that user in general has to access large volumes of data from the cloud in a protected manner. But the complexity of the cryptographic algorithm used, hasn’t been given much importance with security concern. The complexity of the algorithm directly affects the speed of data access in cloud environment. We require some algorithm that will assist in competent, speedy and secured data access.

IV. PROPOSED SYSTEM

A. $a_A \in_R N$ *[choose a prime* (a_A) *at random in N]*

B. $P_A \longleftarrow [a_A] D$

[The form of P_A is (u(x),v(x)) representation which is referred to as Mumford representation]

C. return P_A and a_A

For the random prime number generation in step1, one can apply the probabilistic test of Robbin-Miller (Stallings 2002) or the deterministic test of AKS (Jin 2005). However, various researches have proved that it takes exponential time to determine the given large number is prime or not using AKS algorithm.

Encryption/Decryption Algorithm

In this section, we present the methodology for encryption and decryption. The message 'm' that is to be sent will be encoded as a series of points represented as (u(x),v(x)). The encoded message is referred as Em. For the encryption and decryption process using HECC, we have used ElGamal method to design HEC-ElG Algorithm (HEC-ElGA). Details on ElGamal method can be had from (Avanzi & Lange 2006). The algorithm works as follows: To encrypt and send a message to B, A performs the following steps.

- ***$k \in_R N$ (choose k as a random positive prime number in N)***
- ***$Q \longleftarrow [k]D$ (D is the Divisor of the HEC & The form of Q is (u(x),v(x)))***
- ***$P_k \longleftarrow [k]P_B$ (P_B:(u(x),v(x)) is receiver's(B's) public key)***
- ***$C_m \longleftarrow \{ Q , E_m + P_k \}$ (C_m :(u(x),v(x)) is the Cipher Text to be sent)***

To decrypt Cipher text message, the Decryption algorithm works as follows:
To decrypt the Cipher Text Cm , B extracts the first coordinate 'Q' from the cipher text then multiply with its Private Key (aB) and subtract the result from the second coordinate. This can be written as follows, ALGORITHM for a Hyper-Elliptic Curve Cryptosystem (HECC):
The basis for the Hyper-elliptic curve cryptosystem is the Discrete Logarithm Problem which is described as follows:

"Let Fq be a finite field with q elements. Given 2 divisors, D1 and D2 in the Jacobian, determine m ∊ Z, such that D2=mD1 ."

The following section describes the proposed HECC algorithm which exploits ElGamal technique for key generation process, encryption and decryption process which is named as HEC-ElG Algorithm (HEC-ElGA).

Algorithm for Public Key & Private Key generation

Input: The public parameters are hyper elliptic curve C, prime p and divisor D

Output: The Public key PA and Private key aA

HECC FOR GENUS 2 OVER PRIME FIELD FP (LENGTH OF PRIME IS 100)	
HECC Equation	C: v^2=u^5+7943193u^4+6521255u^3+1065528u^2+3279922u+3728927 Prime: 4112543547855339322343814790708185367671872426434747235319998473455582535888229747778325047393413053 Time (Milliseconds) taken for curve generation : 15.0
Divisor Generation	D:div (u^2+224572136585796451 61u+62960708771725664757, 65279057408798633572u+32004384923913711271) To create Divisor, it took 0.28114057028514255 Seconds
Key Gen	Public key A pkA: div (u^2+35289916585119035066u+61878544074138355074, 30345388419907903671u+48504897385056260640) User A SecKey and PubKey generated in 0.054527263631815905 Seconds Public Key B div (u^2+49122133097793891 26u+50571352708141814388, 59945850494684002755u+82670314232420817874) User B SecKey and PubKey generated in 0.04702351175587794 Seconds Q value div (u^2+42232173388387593518u+4929632337156016505, 40106992517673620469u+23099672970375134358) Pk value div (u^2+17951814325890873471u+26643639829660501424, 62786586170825441317u+89070843160260 26841) Receiver rD div (u^2+17951814325890873471u+26643639829660501424, 62786586170825441317u+8907084316026026841)

$$E_m + kP_B - a_B (Q) = E_m + k P_B - a_B (kD) = E_m + k P_B - k(a_B D) = Em + k P_B - k P_B = Em$$

In the above process, 'A' has masked the message Em by adding kPB to it. The 'A' know the value of k, so even though PB is a public key, nobody can remove the mask kPB. For an attacker to remove message, the attacker would have to compute k from the given D and [k]D i.e. Q, which is assumed very hard.

V. CONCLUSIONS

This study focuses on different security issues in cloud computing environment. Nowadays utmost of the organizations are using cloud computing because of huge benefits of the cloud computing. The cloud computing has different security issues in threats in consumer view, one can say that lack of security is the only worth stating drawbacks of cloud computing. The acquaintance between service providers and consumers is essential for providing better cloud security. A number of attempts had been made at providing a secured environment for activities in the Cloud. Hyper Elliptic Curve Cryptography (HECC) provides solutions for a secured Cloud environment with enhanced performance in cloud computing and resource utilization. HECC has provided a robust and secured model for the development and deployment of the secured application in the Cloud. This work would promote the confidence in both large and small scale organization in Cloud investment.

Authors:

[1] *Assistant Professor,Department of Computer Science, PSG college of arts and science,Bharathiar University, India*
selvisellapppan75@gmail.com

[2]*Associate Professor,School of Computing Science and Engineering,VIT, India*
rganrao@gmail.com

VI. REFERENCES

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

[2] FarzadSabahi. Cloud Computing Security Threats and Responses.Communication Software and Networks (ICCSN), 2011 IEEE 3rdInternational Conference.

[3] AshishAgarwal, AparnaAgarwal. The Security Risks Associatedwith Cloud Computing. International Journal of ComputerApplications in Engineering Sciences [VOL I, SPECIAL ISSUE ONCNS, JULY 2011] [ISSN: 2231-4946].

[4] Ashutosh Kumar Dubey, Animesh Kumar Dubey, MayankNamdev,Shiv Shakti Shrivastava. Cloud-User Security Based on RSA andMD5 Algorithm for Resource Attestation and Sharing in JavaEnvironment. Software Engineering (CONSEG), CSI SixthInternational Conference, Sept. 2012

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

[6] PrashantRewagad, YogitaPawar in. Use of Digital Signature withDiffie Hellman Key Exchange and AES Encryption Algorithm toEnhance Data Security in Cloud Computing. 2013 InternationalConference on Communication Systems and Network Technologies.

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

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

[9] Ravi Gharshi, Suresha. Enhancing Security in Cloud Storage usingECC 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 DigitalSignature. International Journal of Scientific & EngineeringResearch Volume 3, Issue 9, September-2012 ISSN 2229-5518IJSER © 2012.

[11] AqeelKhaliqueKuldip Singh SandeepSood. Implementation ofElliptic Curve Digital Signature Algorithm. International Journal ofComputer Applications (0975 – 8887) Volume 2 – No.2, May 2010

[12] Alfred Menezes, MinghuaQu, Doug Stinson, Yongge Wang.Evaluation of Security Level of Cryptography: ECDSA SignatureScheme. Certicom Research. January 15, 2001.

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

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

[15] Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO85

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

[17] Aderemi A. Atayero, OluwaseyiFeyisetan , Security Issues in CloudComputing: The Potentials of Homomorphic Encryption, Journal ofEmerging Trends in Computing and Information Sciences, Vol. 2, No.10, October 2011