IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.7, Special Issue.2, Jan 2019 E-ISSN: 2347-2693

Data Protection Using Elliptic Curve Cryptography

M. Subhashini[1*], P. Srivaramangai[2]

[1,2]Dept of Computer Science, Maruthu pandiyar college of Arts & Science, Thanjavur, India

Corresponding Author: sacsubhal@yahool.com

Available online at: www.ijcseonline.org

Abstract- Cloud computing is a network-based service that provide sharing of resources such as virtual machine, storage, network, software and applications etc. It helps to reduce capital costs since that cloud users only need to rent resources according to their requirements and pay the services they use. It is very flexible since users can access its service in any place through intranet. However, a variety of security concerns such as integrity, availability and privacy act as barriers for cloud users to adopt the cloud service. Among all of these concerns, security of data is key concern holding back cloud adoption for individual or companies. The main purpose of this paper will introduce a method to protect data by using Elliptic Curve cryptography algorithm, how this algorithm works, and using ECC in data security of cloud computing.

Keywords: Cloud Computing, Security, Algorithm, Elliptic Curve, Challenges, Encryption, Decryption

I. INTRODUCTION

Cloud Computing (CC) is one of the most important and hottest deal of attention, both in academia researches and among users, due to its ability for satisfying the computing needs of the users by reducing commercial expenditure bandwidth with computing compounds while increasing scalability and flexibility for computing services, accessing it through an Internet connection from anywhere in the world available Internet network. It was predicted as early as in 1969 by Leonard Kleinrock, one of the chief scientists of the original Advanced Research Projects Agency Network (ARPANET) project which preceded the Internet, who said: "As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of 'computer utilities' which, like present electric and telephone utilities, will service individual homes and offices across the country." This vision of computing utilities based on a service provisioning model anticipated the massive transformation of the entire computing industry in the 21st century whereby computing services will be readily available on demand, like other utility services available in today's society [1]. The National Institute of Standards and Technology (NIST) define cloud computing as 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 [2]. The Cloud Computing model offers the promise of massive cost savings combined with increased IT agility. It is considered critical that government and industry begin adoption of this technology in response to difficult economic constraints. However, cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. Cloud computing is currently being used; however, security, interoperability, and portability are cited as major barriers to broader adoption [3].

1.1 CLOUD CHARACTERISTICS

- **On demand service:** cloud is large resource and service pool that you can get service or resource whenever you need by paying amount that you used.
- **Ubiquitous network access:** cloud provides services everywhere though standard terminal like mobile phones, laptops and personal digital assistants.
- **Easy use:** the most cloud provider's offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.
- **Business model:** cloud is a business model because it is pay per use of service or resource.
- **Location independent resource poling:** the providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand.

1.2 CLOUD COMPUTING SERVICES

Cloud Providers offer services that can be grouped into **three** categories [4]:

- **Software as a Service (SaaS):** In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers'' side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

- **Platform as a Service (Paas):** Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc are some of the popular PaaS examples.
- **Infrastructure as a Service (Iaas):** IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc [5].

1.3 DEPLOYMENT CLOUD MODELS

- **Public cloud:** the cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services.
- **Private cloud:** the cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.
- **Community cloud:** the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.
- **Hybrid cloud:** the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

II. SECURITY ISSUES AND CHALLENGES IN CLOUD

In cloud different types of security issues and challenges are available. Following part is discussed about few security issues, threats and challenges of cloud computing and their mitigation.

- **VM Attacks:** Cloud computing is relied upon VM technology. The Hypervisor, Sphere, VMware are used for Cloud implementation. The cloud developers required to take care of cloud attacks when the implementation is done and also take care by utilizing Intrusion Prevention System (IPS) and Intrusion Detection Systems (IDS) [6]. The IPS and IDS issues can solve by using suitable firewall.
- **Loss of Governance** The Loss Of Governance problem relied upon to losing security and administrative controls in cloud computing. It comprises transferring data to the cloud, it refers to losing control over location, redundancy and file system [7]. Service-level agreement (SLA) may not have guaranteed on cloud provider zone [8]. There is no proper SLA that is standard SLA‘s are not present in the cloud. Thus, the loss of governance problem was found.
- **Lack -In** Lack of security policy process could lead to vendor lock-in problem. This process would require terming the requirements for the cloud providers to certify they are able to assure that data migrated from the legacy provider [9]. But, the cloud user cannot transfer data from one service provider to another service provider. So to overcome this Application Programming Interface (API‘s) should be utilized, this should be identical. So anybody can utilize it on the cloud.
- **Data Loss or Leakage** Data loss or leakage, which means a data loss that occur in any device. Data loss happens when data may be logically or physically detached from the organization or user either unintentionally or intentionally [10].When the confidential information, for example, patient or customer data, design specifications or source code, intellectual property, price lists, trade secrets, budgets and forecasts are leaking out[11]. It is a negative impact on the cloud business environment. By protecting and encrypting the integrity of cloud data at the time transit is needed. Additionally, analysis of data encryption and production at both runtime and design should be done. In [12] introduced a novel Universal Serial Bus (USB) memory bus for moving data safety in a cloud environment [13].
- **Data Integrity and Data Confidentiality:** Data integrity and data confidentiality denote to the belongings that cloud data have not been destroyed or altered in an unauthorized way[14].The data outsourced and stored in the cloud environment because of the users do not have the sufficient physical storage for their data. But validating the exactness of the cloud storage data is a promising subject for cloud storage security. In order to get the cloud data integrity and data confidentiality in a cloud environment, in this survey intakes the concept of existing data integrity and data confidentiality. Different types of data integrity and data confidentiality based cloud security concept was implemented in the cloud storage as follows. Discuss different challenges faced by data encryption and access control mechanisms, in addition to, recent improvements to meet those difficulties of data confidentiality defense in cloud computing.
- **Data Availability and Data Privacy:** As a various security measure, the data privacy and availability in

cloud storage signifies to that the data are usable and accessible when authorized users needs them from any security machine at any time in the cloud. In an earlier stage of cloud computing, cloud data availability was more concern because the lack of reliable infrastructure and mature [15]. Different types of data availability and data privacy based cloud security concept was implemented in the cloud storage as follows. Discuss different challenges faced by data encryption and access control mechanisms based on data availability and data privacy, in addition to, recent improvements to meet those difficulties of data availability and data privacy defense in cloud computing.

III. ECC ALGORITHM

Elliptical curve cryptography (ECC) [16] 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. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. The properties and functions of elliptic curves have been studied in mathematics for 150 years. Their use within cryptography was first proposed in 1985, (separately) by Neal Koblitz from the University of Washington, and Victor Miller at IBM. An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes [17]. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse.

ALGORITHM FOR ECC

There has to be some information that is publicly known to all the users, thus making it the public key cryptography. The publicly known entities are:-

1. From the equation of the elliptic curve, we need to know:-
   - The values of the constants a and b.
   - The value of m, where elliptic curve is de_ned over GF(2^m).
2. The group of the elliptic curve.
3. A base point B, i.e. any point on the curve E that belongs to the group taken as a base.

The algorithms for different parts of ECC are:-

a. Key Generation Algorithm

- Randomly select an integer Apriv. It acts as the private key for A.
- Then generate Apub such that Apub = Apriv * B, where Apub is the public key for A.
- Randomly select an integer Bpriv. It acts as the private key for B.
- Then generate Bpub such that Bpub = Bpriv * B, where Bpub is the public key for B.
- Finally, A generates key, Ka = Apriv * Bpub
- B generates key, Kb = Bpriv * Apub

b. Signature Generation Algorithm

- Calculation of message digest with a HASH function, preferable SHA-1, where e is the message digest, m is the message such that e = HASHfun(m)
- Generate a random integer rand between 1 and n-1.
- The first of the signature, sign1 is calculated from sign1 = x mod n where x is the product of B with rand i.e. x = xcod(rand * B) where xcod is a function to get the x co-ordinate.
- But if sign1 is 0, then redo the previous step.
- The second part of the signature, sign2 is calculated from the equation sign2 = rand -1(e + (Apriv*sign1)(mod n)
- But if sing2 is 0, then re-generate r and follow the procedure again.
- The signature generated is a pair (sign1,sign2).

c. Signature Validation Algorithm

- Check if sign1 and sign2 lie between the range of 1 and n-1. If not, the signature is not valid.
- Calculate the message digest from the received message with the same hash func- tion, e = HASHfun(m).
- Calculate var1, where var1 = sign2 1(mod n)
- Calculate var2, such that var2 = (e*var1) modn
- Calculate var3, such that var3 = (sign1*var1) modn
- We then calculate X, such that X = (var2*B) + (var3*Apub)
- If sign1(mod n) is equal to xcod(X), then signature is verified.

d. Encryption Algorithm

- The plain text M is mapped onto the elliptic curve at a point P.
- Generate a random integer rand between 1 and n-1.
- The cipher text is then encoded as a pair C, where C = [(rand * B),(P + (rand * Bpub)]

e. Decryption Algorithm

- Get x, where x = xcod(C).
- Calculate prod, where prod = Bpriv * x

- Calculate (P + (rand * Bpub)) prod), this gives the mapped point P
- Then un-map P to the plain text M

In today's world ECC algorithm is used in case of key exchanges by certificate authority (CA) to share the public key certificates with end users. Elliptic Curve Cryptography is a secure and more efficient encryption algorithm than RSA as it uses smaller key sizes for same level of security as compared to RSA. For e. g. a 256-bit ECC public key provides comparable security to a 3072-bit RSA public key. The aim of this work is providing an insight into the use of ECC algorithm for data encryption before uploading the documents on to the cloud. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography [18]. Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths [19]. Every participant in the public key cryptography will have a pair of keys, a public key and private key, used for encryption and decryption operations. Public key is distributed to all the participants where as private key is known to a particular participant only.

IV. CONCLUSION

Cloud Computing provides a platform with an enhanced and efficient way to store data in the cloud. The functioning of Cloud Computing is significantly distressed by issues such as that of data security, integrity, theft, loss and presence of infected applications. These issues are the major disadvantages to the consumer to move their data to the cloud. This paper studied a model using Elliptic Curve Cryptography to enable more efficient data security in the cloud computing. Here, Security is based on the difficulty of computing discrete logarithm in a finite field. ECC forms of public key cryptography, in which one decryption key, known as the private key, is kept secret, while another, known as a public key, is freely distributed. Public key cryptography is computationally more expensive than private key encryption, which employs a single, shared encryption key. By using the ECC algorithm, Cloud computing can achieve high level of security more than the security attain by the IT enterprises their own hardware and software.

REFERENCES

[1]. L. Kleinrock, "A Vision for the Internet", ST Journal of Research, 2(1):4-5, Nov, 2005.

[2]. Mell, Peter, and Timothy Grance, "The NIST definition of cloud computing (draft)," NIST special publication vol.800, 2011.pp 145.

[3]. P. Siani. "Privacy, security and trust in cloud computing." Privacy and Security for Cloud Computing. Springer London, 2013. pp3-42.

[4]. H.Jian, Z. . "Analysis and Application of Consumer Features with Cloud Computing and Data Mining Technology." In Intelligent Computation Technology and Automation, 7th International Conference ICICTA, Oct 2014 ,pp. 84-87.

[5]. B. Rajiv R and M.Nitin."Cloud Computing A CRM Service Based On Separateencryption And Decryption Using Blowfish Algorithm." computing, vol.1, pp. 11.

[6]. Aye Aye Thu, "Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment",International Journal of Computer Applications,Vol. 67– No.4, 2013.

[7]. VinayakShukla,ShobhitSrivastava, Nidheesh Sharma, "Cloud Computing: Security Issues and Solutions",International Journal of Emerging Trends & Technology in Computer Science,Vol.3, Issue 5, 2014. [10]Mitchell Cochran,Paul D. Witman, "Governance And Service Level Agreement Issues In A Cloud Computing Environment",Journal of Information Technology Management, Vol. XXII, Number 2, 2011.

[8]. Grispos, G., Glisson, W.B., and Storer, T., "Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization", 21st European Conference on Information Systems, 5-8, 2013.

[9]. BijayalaxmiPurohit,PawanPrakash Singh, "Data leakage analysis on cloud computing",International Journal of Engineering Research and Applications,Vol. 3, Issue 3, 2013.

[10]. V. Shobana, M. Shanmugasundaram, "Data Leakage Detection Using Cloud Computing",International Journal of Emerging Technology and Advanced Engineering, Vol.3, Special Issue 1, 2013.

[11]. Manas M N, Nagalakshmi C K, Shobha G, "Cloud Computing Security Issues And Methods to Overcome",International Journal of Advanced Research in Computer and Communication Engineering,Vol. 3, Issue 4, 2014.

[12]. Tomoyoshi Takebayashi, Hiroshi Tsuda, TakayukiHasebe, RyusukeMasuoka, "Data Loss Prevention Technologies", FUJITSU Sci. Tech, vol.46, No.1, PP 47-55, 2010.

[13]. Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 2000, Available at http://www.secg.org/download/aid-385/sec1_final.pdf

[14]. Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, Available at http://www.secg.org/download/aid-386/sec2_final.pdf

[15]. Darrel Hankerson, Alfred Menezes and Scott Vanstone, Guide to Elliptic Curve Cryptography, Springer (2004).

[16]. Lawrence C. Washington, Elliptic Curves Number Theory and Cryptography, Taylor & Francis Group, Second Edition (2008).

[17]. Jorko Teeriaho, Cyclic Group Cryptography with Elliptic Curves, Brasov, May (2011).

[18]. S.Maria Celestin Vigila and K. Muneeswaran, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography, International Conference on Advanced Computing, IEEE, pp. 82–85, December (2009).

[19]. D. Sravana Kumar, Ch. Suneetha and A. Chandrasekhar, Encryption of Data Using Elliptic Curve Over Finite Fields, International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, January (2012).

Authors Profile

Dr.P.Srivaramangai received her Ph.D Degree from Mother Teresa University, Kodaikanal in the year 2012. She received her M.Phil Degree from Manonmaniam University, Tirunelveli in the year 2003. She received his M.C.A Degree from Bharathidasan University, Trichy in the year 1996. She is working as Associate-Professor, PG and Research Department of Computer Science, Marudupandiyar College of Arts & Science, Thanjavur, Tamilnadu, India. She has above 30 years of experience in academic field. She published 25 papers in National & International journals so far. Her areas of interest include Computer Networks, Internet of Thing, Grid Computing, Cloud Computing and Mobile Computing.

Ms M.Subashini is pursuing her Ph.D from Marudupandiyar College Thanjavur, affiliated to Bharathidasan University in part time and she is working as an Asst.Prof in the Dept. Of computer Sciecne at Srimad Andavan College of Arts and Science, Srirangam , Trichy. Her areas of Research and interest includes Data Mining, Data science, Big Data, Predictive Analytics, cryptography, Network security etc.. She has presented and publisher more than five papers in various Ntional and Internal Journals.