IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 48-53
www.iosrjournals.org

Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography

Asst. Prof. Dr. Salim Ali Abbas[*] AmalAbdulBaqiMaryoosh[*]
[*]*Department Of Computer Science, College Of Education, Al-Mustansiryah University*

Abstract: *Companies tends towards more availability, less cost, managed risk, agility- all of which are providing by cloud computing. The cloud computing is a way to deliver IT services on demand and pay per usage, and it can stores huge amount of data. But until now many companies don't wish to use cloud computing technology due to concerns about data secrecy and protection. This paper aims to provide a secure, effective, and flexible method to improve data storage security in cloud computing. By using IBC the key management complexity will decrease and not need to certificate issued, also the use of ECC provides data confidentiality and use ECDS provides data integrity.*

Keywords: *Cloud computing, Cryptography, Elliptic Curve, Data storage.*

I. Introduction

Cloud computing is a new technology often used virtualized with resources to provide dynamically scalable service via the internet. In the cloud computing, users can access to the resources by using a various devices, such as laptops, PCs, smart phone, etc. to access multiple service such as storage, programs, and application-development platforms, over service that provided by cloud providers via the internet. Through the last years, Cloud computing improved from simple web applications, such as Gmail and Hotmail, into business propositions like SalesForce.com, AmazonEC2, etc [1].

Cloud computing may be supply service for reducing IT costs, business management, and maintenance costs of hardware and software are effective. At the same time, it makes the enterprises able to access to professional IT solutions. Data storage center in cloud computing can be reliable and secure, because the world's most advance data center is helping the users save the data. The users must not concern about virus attack, data loss, and other problems when they used the cloud in correct form[2].

User with cloud computing can use the cloud services anywhere, everywhere, on-demand and based on pay per use principle. Cloudcomputing has two types of models: services models (SaaS, PaaS, and IaaS), and deployment models(Public, Private, Community, and Hybrid cloud). Also the cloud computing is contains five essential characteristics (On-Demand, BroadNetwork Access, Rapid Elasticity, Measured Service,and Resource pooling).There are many companies that provide cloud services such as Amazon, Google, Microsoft,SalesForce.com, etc.

There are many concerns about the data security in cloud computing should be taken into account such as violation of the confidentiality and privacy of customers' data via unauthorized parties [3]. The major concern is if the data secure when it save in cloud?.Therefore, we have dedicated our work to design a new architecture to improve data security in cloud computing by using Identity-Based Cryptography (IBC) and Elliptic Curve Cryptography (ECC) with a Trusted Cloud (TC).

This paper organized as follows: Section 2 displays some works that related to the field of data security in cloud computing. Section 3explain where data storage in cloud computing. Section 4 displays data security lifecycle. Section 5 explain the IBC concept. Section 6review the general concept of ECC. Section 7illustrates the implementation of the proposed system. Section 8shows our work conclusion.

II. Literature Survey

Several works related to our work, which presents the security of data in cloud computing as follow:

In 2009Mohammed Abdelhamid propose techniques to enhance users' privacy based on RSA algorithm.This proposal allowing users to authorize access to their remotely-storeddata [4].

In 2011Syam Kumar P and Subramanian R propose an effective and safe protocol by use ECC and Sobol sequence. This protocol provide integrity and confidentiality of data. Moreover, their system also supports dynamic data operations, which performed by the user on data stored in cloud while maintaining same security assurance [5].

In 2012 Abbas Amini propose system for secure storage in cloud computing. This proposal use RSA algorithm for data integrity, and use AES algorithm to achieve confidentiality of the stored data [6].

In 2012K.Govindaand Dr.E.Sathiyamoorthy propose a manner of secure data storage and identity anonymization in private cloud by use GDS (Group Digital Signature). They use the concept of key exchange

with Diffie-Hellman protocol and strong RSA algorithm for the keys generation in addition to the process of signature, encryption and decryption [7].

In 2014SwarnalataBollavarapu and Bharat Gupta propose data storage security system in cloud computing. This system use algorithms like RSA, ECC and RC4 for encryption and decryption techniques [8].

III. Data Storage and Date Location

Cloud computing store data in a wide range distributed systems to offer more secure and reliable data storage center. Customers no longer needed to concern on virus attack, data loss, and other problems. The information is managed by the most professional team, and most advanced data center in the world is helping users to save data. Cloud computing requires large amounts data storage, also requires to meet economy, high reliability, and high availability, etc. As a result, cloud's systems need to support large data sets, and process mode of write one time and read many [9].

The security must be taken in mind in a design stage of cloud storage,it must contains redundancy and dynamic data as well as the separation. Data stores in the cloud redundantly by keeping redundant copies of data at many various locations, Redundancy is one of the more essential methodsto protect the security of data storage. While dynamic means that the customer's data usually may be changed.Separation means the time of storing customer's data in the cloud. The customer can access only to own data in order to ensure the independence of the data;data that is changed by the other customers do not affect the current customer [10].

To secure data, firstly, must know where its location, there may be a significant differences between the regulatory policies in various countries. Cloud's user may be implicated in illegal practices without knowing. Some governments suesenterprises which let for specific kinds of data to cross geographical boundaries. Cloud computing customers should treats this problem by understanding the regulatory requirements for every country they will be operating in. Currently, CSPs choice is left to the customer to choose the location of the data center. For example, Amazon provides two locations one in Europe and the other in US [11].

IV. Data security lifecycle

The data security lifecycle is the path which the data going through from the stage of creation to destruction. It consists of the following stages[12, 13]:

a. Create stage: When creating data, it can be manipulation, user's access rightsmay be changed by intruders or incorrectly classified, which leads to loss the control of data. Organizations should be use data tags and classification techniques, like user labeling of data, to reduce the incorrect classification of data.

b. Store stage: The security system of SP is unknown because SPs are third-parties, so data should be protected from manipulation by intruders over network, unauthorized access, and data leak. There should be guarantee that the data, all its copies, and backups, are stored only in geographic locations allowed by Service Level Agreement (SLA).

c. Use and Share stage: Through the use stage, which includes transition among CSP, data processing, and customer, Sensitive data must be secured from that mingle with data of other customers during data traffic in the network. If the data is shared among multiple customers or organizations, the SP must ensures consistency and integrity of data. The SP must also protect all of its cloud service customer from malicious activities carried out by the other customers.

d. Archive stage: As in the storage stage, must protect data from unauthorized access by hackers and malicious customers. In addition to keeping a backup copy of the data and retrieval when needed to prevent data premature destruction or loss. Data which in live production database, the CSP encrypts the data before stored, as for the data that will be archived the cloud customer encrypted it before being sent to CSP to reduce the ability of a malicious CSP or customers from accessing archived data.

e. Destroy stage: The biggest challenges facing the destruction stage is data permanence. Data that were destroyed must be erased, non-refundable, and disposal physically. CSPs Must be uses several techniques to guarantee that the data is completely destroyed, these techniques are disk Erasing, physical data destruction techniques, like crypto-shredding and degaussing.

V. Identity-Based Cryptography (IBC)

IBC is one of the types of public key cryptography, which was initially proposed by Adi Shamir in 1984 to reduce the need for certificate authorities to distribute public key certificate. In IBC use users' identifier information such as phone number, email, IP addresses, or domain name as a public key rather than used digital certificates. Shamir implemented an identity based signature (IBS) by used RSA algorithm to allow users to

verification from digital signatures. Although he tried to implement an identity based encryption (IBE), but he was unable to reach a solution and IBE remained open problem for many years. Until 2001, Franklin, Boneh, and Cocks independently proposed scheme to solve IBE problem by using bilinear pairings and have provable security. IBC allow to any two users to communicate securely, and verification of signatures each other without exchanging any type of keys [14, 15, 16].Figure (1) view IBS and IBE schemes.

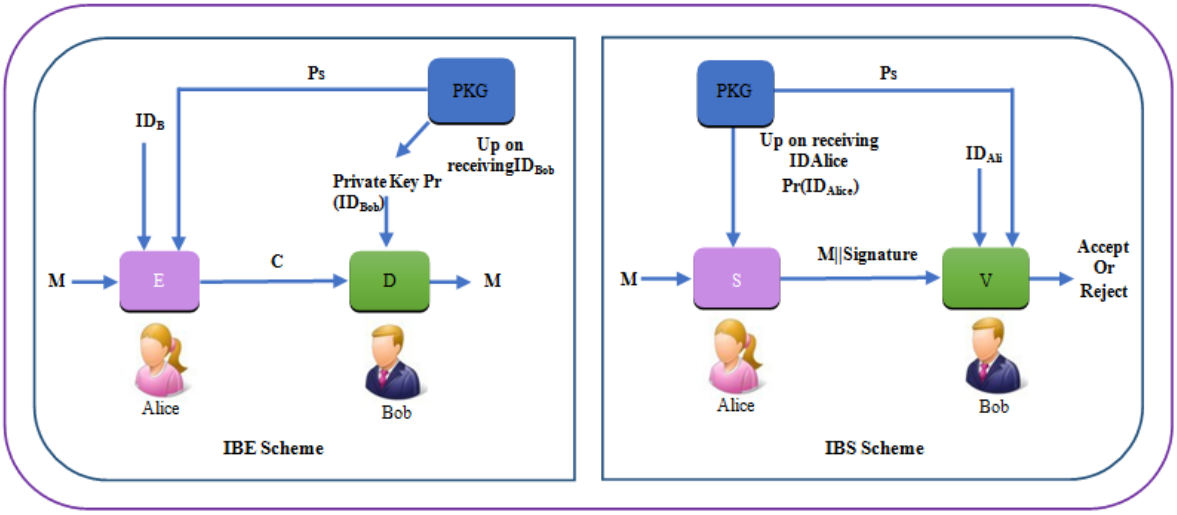

Figure 1: IBE and IBS Schemes

The Identity-basedcryptography systems containthePrivate Key Generator (PKG) that act as a trusted third party, which create a master private key (Mk) and a master public key (Ps), then PKG will publish the master public key and keeps a master private keysecret. Any user can generate his public key by combining a master public key and his identity. The user must connects the PKG with his identity to obtain his private key (Pr). PKG will use the master private key and user's identity to generateuser's private key[17].

VI. Elliptic Curve Cryptosystem

Elliptic curve cryptography (ECC) is one of the public key encryption algorithms which is depend on elliptic curve theory over finite fields. It used to make cryptographic keys smaller, faster, and more efficient. The functions and characteristics of an elliptic curves have been studied in mathematics for 150 years. Their use has been suggested in cryptography for the first time by Neal Koblitz and Victor Miller in 1985, separately [18]. ECC has begun to obtain acceptance of many of the accredited organizations, and many of the security protocols since the beginning of 1990 [19].

6.1 Elliptic Curve Arithmetic

The main attraction of ECC is that it provides an equal level of security, but much smaller key size compared with RSA. We can defined an elliptic curve by equation all its coefficients and variables take values in the set of integers within the range from 0 to p-1, which is performed calculations modulo p. When use an elliptic curve for cryptography, the coefficients and variables are restricted in a finite Abelian group*[20, 21]. The group that has a finite number of elements, it's known as a finite groupand the number of elements in $\mathbb{G}$ is known as the order of $\mathbb{G}$ [22].ECC equation over $\mathbb{F}_{2^m}$is:

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

6.2 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Assume that E is an elliptic curve over some finite field $\mathbb{F}_q$, and P a point of order n on E. ECDLP on E is to find the integer d ∈ [1,n–1], if such an integer exists, so that

$$Q = dP, \text{ where } dP = \underbrace{P + P + \ldots + P}_{d \text{ times}}$$

*We can say about the group ($\mathbb{G}$) is an Abelian group or commutative group if achieved the following condition: $m \cdot n = n \cdot m$ for all m,n in$\mathbb{G}$.

The discrete logarithm problem (DLP) is does not look like ECDLP, and that ECDLP is considerably more difficult than the DLP. This is due to the lack of known subexponential-time algorithm to solve ECDLP in general [23].

6.3 Security of Elliptic Curve Cryptography

ECC algorithm is one of the most powerful asymmetric algorithms for a particular key length, so that it is attractive especially for security applications where integrated circuit space and computational power is limited, such as PC (personal computer) cards, smart cards, and wireless devices. ECC algorithm security is relies on the difficulty of solving ECDLP. Currently it seems that ECC that be implemented on 160-bit nearly offer the same level of security in the resistance against compared with 1024-bit RSA attacks. That led to improved performance and better storage requirements [21]. Table (1)presents a comparison of the approximate parameter size between strength elliptic curve systems and RSA.

Table 1: Comparative Bit Lengths [23]

Elliptic Curve Cryptosystem (order of base point P)	RSA (length of the modulus n)
106 bit	512 bit
132 bit	768 bit
160 bit	1024 bit
224 bit	2048 bit
384 bit	7680 bit

VII. The Proposed Method

The proposed method contain three parts: Private Key Generator (PKG), Trusted Cloud (TC), and User. The PKG is use to generate users' keys. The user rent infrastructure from TC to save his data. This proposal aims to provide more secure method to secure users' data protection, reduce the complexity of management by using IBC, and providedata confidentiality by using ECC over binary field and data integrity by using Elliptic curve digital signature algorithm (ECDS).The main idea of this proposal is combine the security of IBC and ECC with Trusted Cloud (TC). The use of IBC will significantly decrease the key management complexity and not need to certificate issued. Also the use of TC has many benefits such as decrease the denial of service attack (DOS) on CSPs, this important attraction because TC will save users' data. All these parts increase the strength and resistance of the system. Figure 2 explain the general structure of the proposed system.

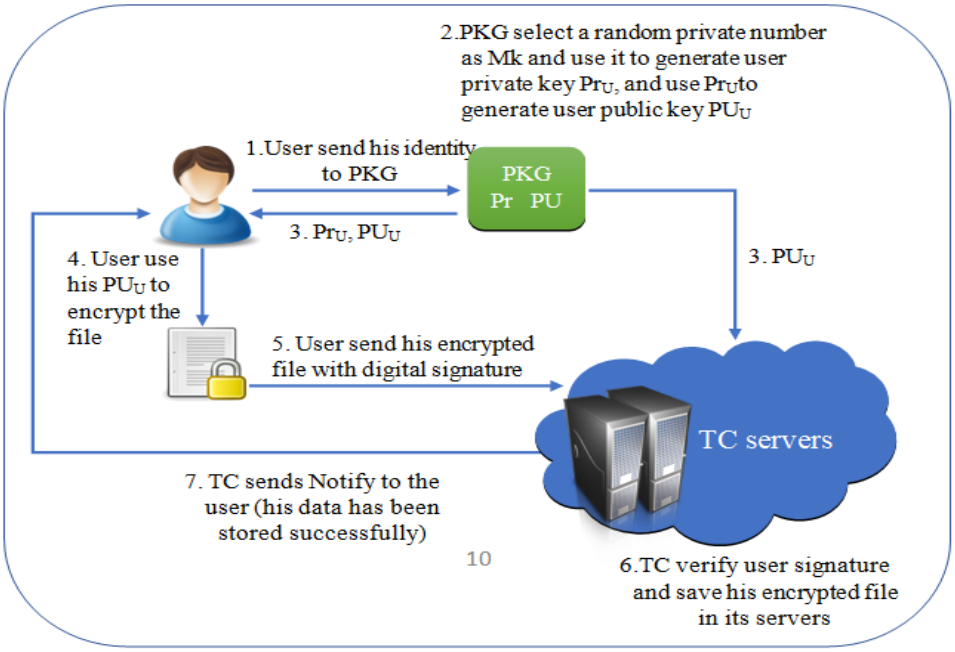

Figure 2: General Structure of Proposed System

The Proposed Algorithm includes the following steps:-

a. Setup: the **PKG** do the following functions:

1. Chooses the curve **E** over $\mathbb{F}_{2^m}$ in the form $y^2 + xy = x^3 + ax^2 + b$ where ***a*** and ***b*** are the curve parameters.

2. Chooses the base point **P** in $E(\mathbb{F}_{2^m})$ whose order **n** should be very large.

3. Selects a random number smaller than the base point **P** order as a private number, this number will be a master private key **Mk**.

b. Extract: when user wants to get his private and public key from **PKG**, he must send his identity ($\mathbf{ID_U}$) to **PKG**. Then the **PKG** will compute the hash value to the identity of user ($\mathbf{ID_U}$) and use it with master private key **Mk** to generate user private key, and use this private key to generate user public key.

$\mathbf{Q_U = H(ID_U)}$

$\mathbf{Pr_U = Mk * Q_U}$

$\mathbf{PU_U = Pr_U * P}$

Then send copy from user private to user, and copy of user public key to user and TC.

c. Encryption: the user can encrypt his file by using the public key to generate his ciphertext as follow:

1. The userencodes his file to points $\mathbf{P_m}$.

2. The user encrypts his file as follows:

a. Selects a random integer number **J**.

b. Calculates the ciphertext$\mathbf{C_m}$ consists of the pair of points

$\mathbf{C_m = \{J*P, P_m + J*PU\}}$

c. The user sends $\mathbf{C_m}$ to TC.

d. Decryption: When user want to retrieve his encrypted file$\mathbf{C_m}$ from TC, he will decrypted the message by computes:

$\mathbf{P_m + J*PU - Pr(J*P)}$

$\mathbf{P_m + J(Pr*P) - Pr(J*P) = P_m}$

Then he decodes $\mathbf{P_m}$to get the original file**m**.

e. Signing and Verifying: The usermust signing the file**m** by using his private key **Pr** as follows:

1. Calculates the hash value to the $\mathbf{e = H(m)}$ message
2. Chooses a random positive integer **J** in interval [1, n-1].
3. Calculates $\mathbf{(x,y) = J*P}$.
4. Calculates $\mathbf{r = x \bmod n}$, if $\mathbf{r = 0}$ go to step 2.
5. Calculates $\mathbf{S = J^{-1}(e + Pr_A * r) \bmod n}$, if $\mathbf{S = 0}$ go to step 2.
6. The file's signature is the pair **(r,S)**.
7. Sends the signature **(r,S)** to TC.

The TC when receive the user's file,it must verify the signature based on the public key $\mathbf{PU_U}$ of user as follows:

1. Calculates $\mathbf{e = H(m)}$
2. Calculates $\mathbf{w = S^{-1} \bmod n}$.
3. Calculates $\mathbf{u1 = e*w \bmod n}$ and $\mathbf{u2 = r*w \bmod n}$.
4. $\mathbf{(x,y) = u1*P + u2*PU_U}$,if $\mathbf{(x,y) = \infty}$then reject the signature,

$\mathbf{v = x \bmod n}$.

$\mathbf{v = r}$ otherwise calculates

5. If then the signature is valid otherwise invalid.

VIII. Conclusions and Future Research Directions:

This paper propose a more flexible and effective scheme to address data storage security problemsin cloud computing. The use of IBC provide key management and not need to certificate issued, and ECC led to protect data security and confidentiality before it stores in cloud servers, also the use of ECDS provide data integrity. Future researches might consider in future such as use the hierarchal identity-based cryptography (HIBC) instead of IBC and compare the result with this proposal.

References

[1]. Jeffrey Voas and Jia Zhang, "Cloud Computing: New Wine or Just a New Bottle?", Published by the IEEE Computer Society, 2009.
[2]. Sameeh A. Jassim, MSc thesis, "Mediated IBC-Based Management System of Identity and Access in Cloud Computing", College of Computer, University of Anbar, 2013.
[3]. SameeraAbdulrahmanAlmulla and Chan YeobYeun, "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), Presented at 2nd IEEE International Conference, 30 march 2010.
[4]. Mohamed Abdelhamid, PhD thesis, "Privacy-preserving Personal Information Management", School of Computer Science, McGill University, Montreal, August 2009.
[5]. Syam Kumar P and Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
[6]. Abbas Amini, MSc thesis, "Secure Storage in Cloud Computing", Department of Informatics and Mathematical Modelling (IMM), the Technical University of Denmark, May 2012.
[7]. K.Govinda and Dr.E.Sathiyamoorthy, "Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud", Published by Elsevier Ltd., Procedia Technology, April, 2012.
[8]. SwarnalataBollavarapu and Bharat Gupta, "Data Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.
[9]. Sugang Ma, "A Review on Cloud Computing Development", JOURNAL OF NETWORKS, VOL. 7, NO. 2, FEBRUARY 2012.
[10]. SajjadHashemi, "DATA STORAGE SECURITY CHALLENGES IN CLOUD COMPUTING", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.
[11]. Victor Delgado, MSc thesis, "Exploring the limits of cloud computing", KungligaTekniskaHögskolan (KTH) Stockholm, Sweden, October 4, 2010.
[12]. UttamThakore, "Survey of Security Issues in Cloud Computing", College of Engineering, University of Florida, Available at: http://www.cise.ufl.edu/~sgchen/papers/Survey%20of%20Security%20Issues%20in%20Cloud%20Computing.pdf, Accessed Date: 14 January 2015.
[13]. Albert Caballero and et al, "Open Data Center Alliance:Data Security Framework Rev 1.0",Open Data Center Alliance, Inc. ALL RIGHTS RESERVED, 2013.
[14]. Marc Joye and Gregory Neven, "Identity Based cryptography", IOS Press, 2009.
[15]. JoonsangBaek et al, "A Survey of Identity-Based Cryptography", Australian Unix Users Group Annual Conference, 2004.
[16]. DivyaNalla and K.C.Reddy, "Signcryption scheme for Identity-based Cryptosystems", Mathematics of Computation, 2003.
[17]. Liang Yan, ChunmingRong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography", Springer-Verlag Berlin Heidelberg, 2009.
[18]. Ravi Gharshi and Suresha, "Enhancing Security in Cloud Storage using ECC Algorithm", International Journal of Science and Research (IJSR), Volume 2 Issue 7, July 2013.
[19]. Chester Rebeiro, M.Sc.thesis, "Architecture Explorations for Elliptic Curve Cryptography on FPGAS", Department of Computer Science and Engineering, Indian Institute of Technology, Madras, February 2009.
[20]. William Stallings, "Cryptography and Network Security",principles and practice 5th edition,Pearson Education, Inc., 2011.
[21]. Ali MakkiSagheer, MSc thesis, "Enhancement of Elliptic Curve Cryptography Methods",Computer Science, University of Technology, 2004.
[22]. Darrel Hankerson, Alfred Menezes and Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, 2004.
[23]. MajidKhabbazian, MSc thesis, "Software Elliptic Curve Cryptography",Department of Electrical and Computer Engineering, University of Victoria, 2004.