International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.6, March 2016 – www.ijais.org

Data Security for Cloud Computing based on Elliptic Curve Integrated Encryption Scheme (ECIES) and Modified Identity based Cryptography (MIBC)

Salim Ali Abbas, Ph.D
Department of Computer Science, Collage of Education, Al-Mustansiryah University
Iraq, Baghdad

Amal Abdul Baqi Maryoosh
Department of Computer Science, Collage of Education, Al-Mustansiryah University
Iraq, Baghdad

ABSTRACT

Companies tends towards more availability, less cost, managed risk-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 the 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 security in cloud computing. The test results show that the key generation complexity will decrease and not need to certificate issued because the use of MIBC, also the use of ECIES provides data confidentiality and data integrity.

Keywords

Cloud computing, Cryptography, Elliptic Curve, Data security

1. 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. Cloud computing 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, and 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 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 modified Identity-Based Cryptography (MIBC) and Elliptic Curve Integrated Encryption Scheme (ECIES) Algorithm.

This paper organized as follows: Section 2 displays some works that related to the field of data security in cloud computing. Section 3 describes in ECC detail. Section 4 explain the IBC concept. Section 5 defines the architecture of the proposed model. Section 6 illustrates the implementation and result of the proposed system. Section 7 shows our work conclusion.

2. LITERATURE SURVEY

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

In 2011 Suli Wang et al. proposed method for file encryption and decryption system based on RSA algorithm with smaller sizes [4]. In 2012 Abbas Amini proposed system for secure data in cloud computing. This proposal use RSA algorithm for data integrity, and use AES algorithm to achieve confidentiality of the stored data [5]. In 2014 Puneetha and M Dakshayini proposed data security model using ECC algorithm and hash function as digital signature [6]. In 2014 Debajyoti Mukhopadhyay et al. proposed method for securing the data in clouds by implementing key agreement, encryption and signature verification/generation with hyperelliptic curve cryptography [7]. In 2014 Swarnalata Bollavarapu and Bharat Gupta proposed data security system. This system use algorithms like RSA, ECC and RC4 for encryption and decryption techniques [8].

3. 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 [9]. ECC has begun to obtain acceptance of many of the accredited organizations, and many of the security protocols since the beginning of 1990 [10].

3.1 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[*] [11, 12]. The group that has a finite number of elements, it's known as a finite group and the number of elements in 𝔾 is known as the order of 𝔾 [13]. ECC equation:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

3.2 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Assume that E is an elliptic curve over some finite field 𝔽q, 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

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

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 [14].

3.3 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 [12]. Table (1) presents a comparison of the approximate parameter size between strength elliptic curve systems and RSA.

Table 1: Comparative Bit Lengths [14]

ECC (bits)	RSA (bits)	Key Size Ratio
160	1024	1:6
256	2048	1:8
384	7680	1:20
512	15360	1:30

3.4 Elliptic Curve Integrated Encryption Scheme (ECIES)

ECIES is a public key encryption scheme, which considered an enhancement of ElGamal encryption scheme, designed specifically for Elliptic curve groups. ECIES proposed by Abdalla, Bellare, and Rogaway, It has been standardized in ANSI X9.63 and ISO/IEC 15946-3, and is in the IEEE P1363a. This scheme provides safety against adaptive chosen-plaintext and chosen-ciphertext attacks. It provides capabilities for encryption, key exchange and digital signature together. Hence it is called Integrated Encryption Scheme, since it is a hybrid scheme that uses a public key system to transport a session key for use by a symmetric cipher [15].

In ECIES, a Diffie-Hellman shared secret is used to derive two symmetric keys k1 and k2. The key k1 is used to encrypt the plaintext using a symmetric-key cipher, while the key k2 is used to authenticate the resulting ciphertext. ECIES uses the following cryptographic primitives [13]:

1. KDF is a key derivation function that is constructed from a hash function H. If a key of *l* bits is required then KDF(S) is defined to be the concatenation of the hash values H(S,i), where i is a counter that is incremented for each hash function evaluation until *l* bits of hash values have been generated.
2. ENC is the encryption function for a symmetric-key encryption scheme such as the AES, and DEC is the decryption function.
3. MAC is a message authentication code algorithm such as HMAC.

In order to describe the steps that must be taken in order to encrypt a clear message, we will assume that Alice wants to send a message to Bob. In that scenario, Alice’s ephemeral private and public keys will be represented as PrA and PUA, respectively. Similarly, we will refer to Bob‘s private and public keys as PrB and PUB, respectively. The steps (see Figure.1) that Alice must complete are the following [16]:

1. Alice must create an ephemeral key pair consist of a random secret value Pr_A and the elliptic curve point P ($PU_A = Pr_A \cdot P$). That key pair should be generated pseudorandomly exclusively for the current process.
2. After that Alice will use the Key Agreement function, KA, in order to create a shared secret value, which is the result of the escalar multiplication ($Sk=Pr_A \cdot PU_B$), considering as input values Alice's ephemeral private key Pr_A and Bob's public key PU_B.
3. Then, Alice must take the shared secret value Sk as input data for the Key Derivation Function, KDF. The output of this function is the concatenation of the symmetric encryption key, k1, and the MAC key, k2.
4. With the element k1 and the clear message, m, Alice will use the symmetric encryption algorithm, ENC, in order to produce the encrypted message, C.
5. Taking the encrypted message C, k2, such as a text string previously agreed by both parties, Alice must use the selected MAC function in order to produce a tag.

Finally, Alice will take the temporary public key (PUA), the tag (t), and the encrypted message (C), and will send the cryptogram (PUA||t||C) consisting of those three concatenated elements to Bob.

The following steps illustrate the decryption process that Bob must perform (see Figure.2) [16]:

1. After receiving the cryptogram (PUA||t||C) from Alice, Bob must retrieve the ephemeral public key PUA, the tag t, and the encrypted message C, so he can deal with those elements separately.
2. Using the retrieved ephemeral public key, PUA, and his own private key, PrB, Bob will multiply both elements in order to produce the shared secret value PrB· PUA, as

[*] We can say about the group (𝔾) is an Abelian group or commutative group if achieved the following condition: m · n = n · m for all m, n in 𝔾.

the result of this computation is the same that the product PrA·PUB, which is the core of the Diffie-Hellman protocol.

3. Taking as input the shared secret value Sk, Bob must produce the same encryption and MAC keys by means of the KDF procedure.

4. With the MAC key k2 and the encrypted message C, Bob will first compute the element tag, and then he will compare its value with the tag that he received. If the values are different, Bob must reject the cryptogram due to a failure in MAC verification procedure.

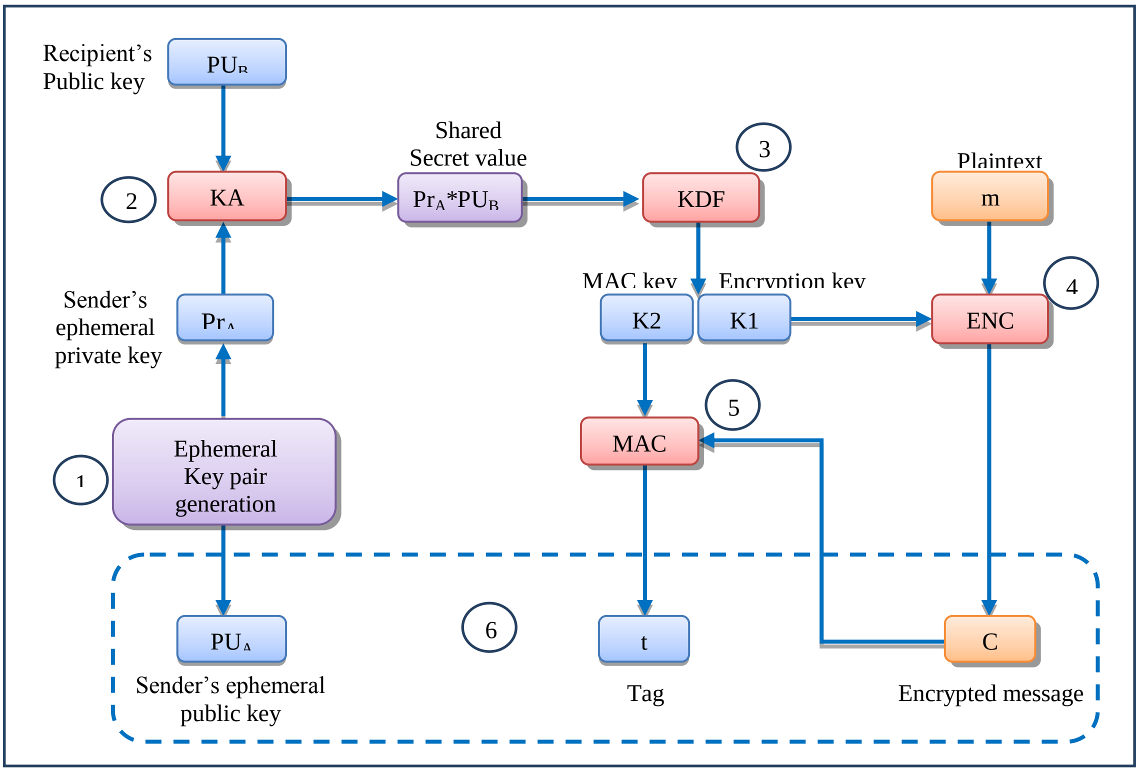

Fig 1: ECIES encryption functional diagram

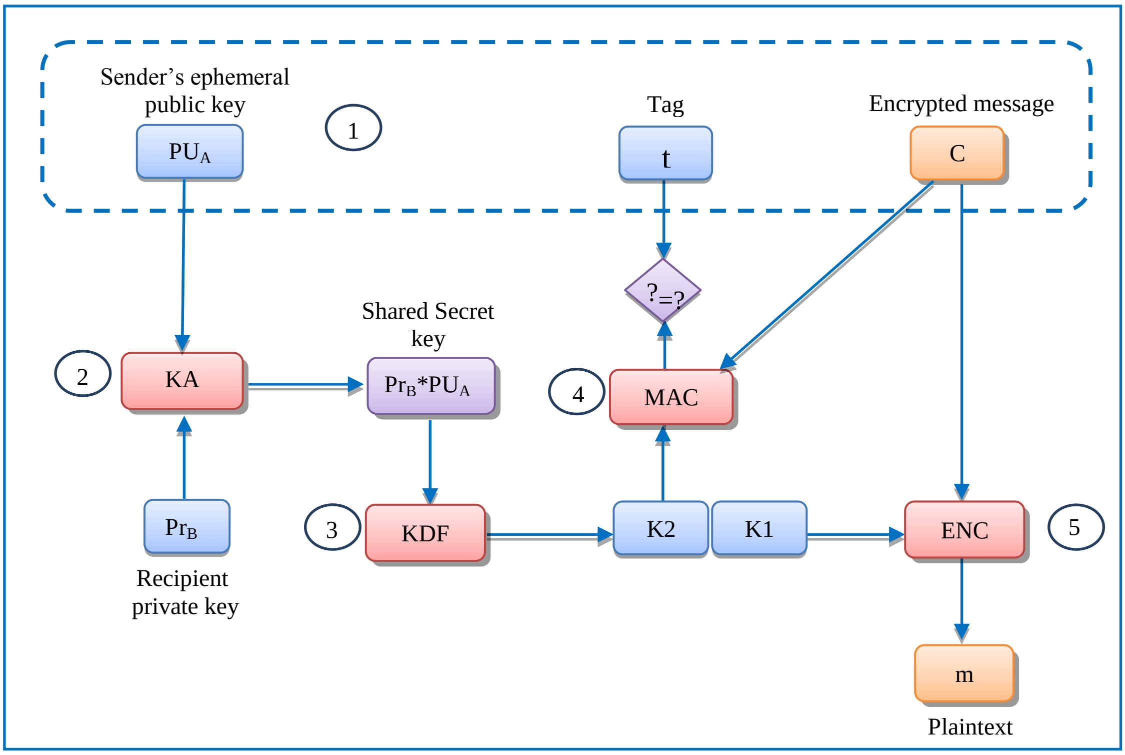

Fig 2: ECIES decryption functional diagram

5. If the tag value generated by Bob is the correct one, then he will continue the process by deciphering the encrypted message C using the symmetric ENC algorithm and k1. At the end of the decryption process, Bob will be able to access the plaintext that Alice intended to send him.

4. 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 [17, 18, 19]. Figure (3) views IBS and IBE schemes.

The Identity-based cryptography systems contain the Private 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 key secret. 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 generate user’s private key [20].

IBC scheme has some disadvantages. Bob receives his private key from PKG which computes his private key as a function of its master secret and Bob’s identity. This requires Bob to authenticate himself to the PKG, and requires a secure channel through which the PKG may send Bob his private key. Bob’s PKG must publish parameters that embed its master secret key, and Alice must obtain these parameters before sending an encrypted message to Bob. Also the main disadvantage of IBC scheme is key escrow where the PKG knows (can compute) the private keys of all the users. If it detected, the security of communications can be questioned. This means that the users should trust the PKG that their keys will not be made available to others.

The proposed system uses some the main advantages of IBC. Its eliminate the need to certificates, reduce the complexity by depend on a trusted authority (PKG) to generate the parameters of the system and master secret key, and not need to keys revocation because the keys are expire after the end of the session. As well as the proposed system overcomes the disadvantages of IBC where gets rid from the problem of key escrow where the user generates the keys with the help of a trusted authority, and the proposed system use SSL as secure channel to get the parameters of the system and master key. The proposed system prefer the use of ECC algorithm instead bilinear pairing to provide more security and to reduce the complexity, because the bilinear pairing computation is hard understanding for the most programmers and needs to generate three group and many extra parameters. But the proposed system provides high level of security with less complexity.

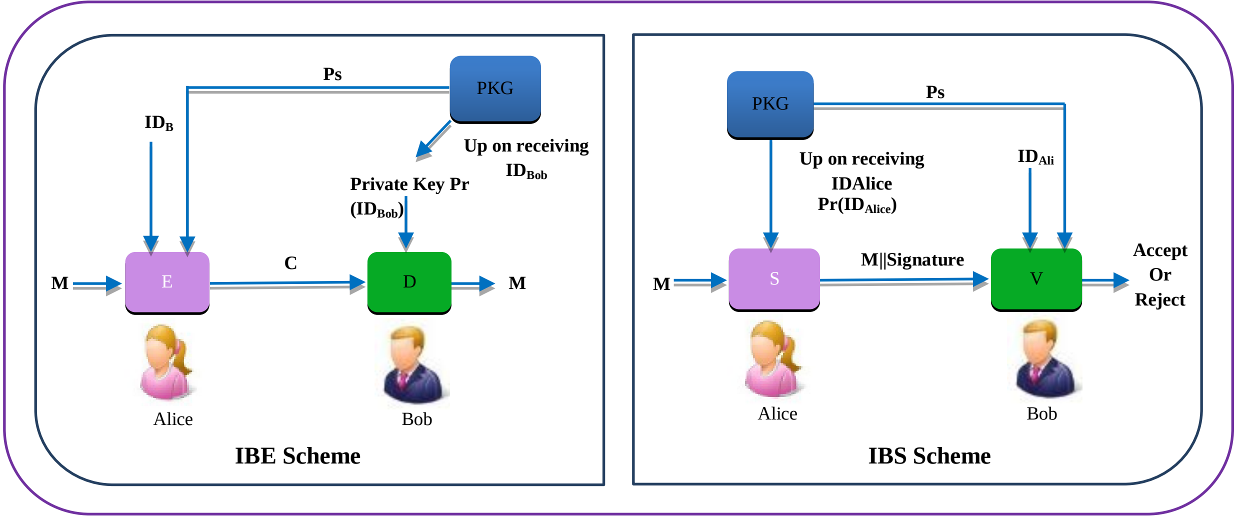

Fig 3: IBE and IBS Schemes

5. THE PROPOSED SCHEME

The proposed scheme contains three parts: Trusted Authority (TA), Trusted Cloud (TC), and User. The TA responsible for generate the essential parameters in the system. This parameters are the base point (P), the field ($\mathbb{F}_p$), the prime number (p), the order (n), the curve (E), and the curve’s parameters (a,b). As well as it is generates a random private number as a master private key (Mk) and keeps it secret. The user sends his request to TA to get the parameters of system and Mk to generate his private and public keys. After the user get the request he will compute the hash value (H) to the user’s identity[*] (ID_U) and generate the private key (Pr_U) by multiplying the Mk with H(ID_U), and then use this private key (Pr_U) to generate the public key (PU_U) by use elliptic curve discrete logarithm problem. This proposal is aimed to provide more secure method to secure users’ data protection, reduce

[*] User’s identity must be unique and can be any attribute such as phone number, email address, etc.

the complexity of key generation by using modified Identity Based Cryptography (MIBC), and provide data confidentiality and integrity by using Elliptic Curve Integrated Encryption Scheme (ECIES). The main idea of this proposal is combine the security of MIBC and ECIES with Trusted Cloud (TC). The use of MIBC will significantly decrease the key generation 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 (4) show general structure of the proposed scheme.

1. Encryption Algorithm

Step1: Key Agreement: compute the shared secret key by use ECDH Sk = Pr_A* $PU_{B.}$

Step2: Use key derivation function (KDF) to derive a symmetric encryption key (k_1) and MAK key (k_2), (k_1,k_2)= KDF (x_{Sk},PU_A), where x_{Sk} is the x-coordinate of Sk.

Step3: Encrypt the plaintext m by use AES 256: C = ENC_{k1} (m).

Step4: Compute the tag encrypted data: t= MAC_{k2} (C).

Step5: Return (PU_A||C||t).

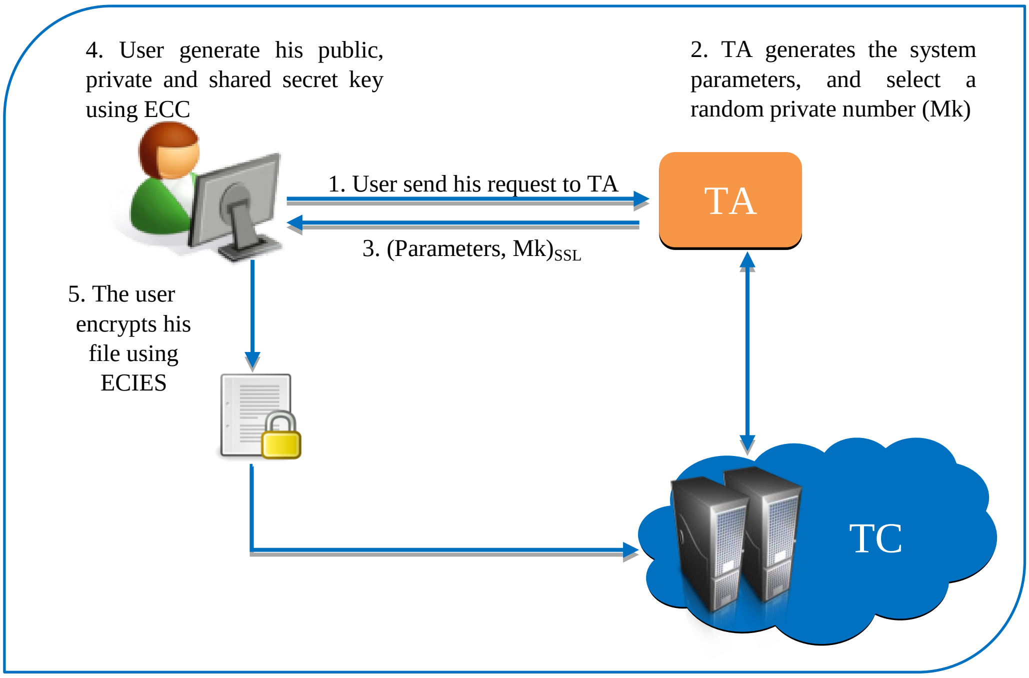
4. User generate his public, private and shared secret key using ECC
2. TA generates the system parameters, and select a random private number (Mk)
1. User send his request to TA
TA
3. (Parameters, Mk)SSL
5. The user encrypts his file using ECIES
TC

Fig 4: General Structure of the Proposed Scheme

The Proposed Algorithms

2. Keys Generation Algorithm

Step 1: Setup: the TA do following functions:

1. Chooses a prime number p that has the prime order n, and a finite filed $\mathbb{F}_p$.
2. Chooses the curve E over $\mathbb{F}_p$ in the form $y^2 mod\ p = x^3 + ax + b\ mod\ p$ where a and b are the curve parameters.
3. Chooses the base point P in E($\mathbb{F}_p$) whose order n should be very large.
4. Selects a random number smaller than the order of base point P as a private number, this number will be a master private key Mk.
5. Send (p, n, $\mathbb{F}_p$, E, P, Mk) to user across SSL protocol.

Step 2: Extract: when Alice wants to generate her private and public key, she must compute the hash value to her identity (ID_U). Then use the hash value with master private key Mk to generate her private key, and use this private key to generate her public key.

Q_A = H (ID_A)

Pr_A = Mk*Q_A

PU_A = Pr_A*P

3. Decryption Algorithm

Step1: Compute the shared secret key by use ECDH Sk = Pr_B* PU_A.

Step2: Use key derivation function (KDF) to derive a symmetric encryption key (k_1) and MAK key (k_2), (k_1,k_2)= KDF (x_{Sk},PU_A), where x_{Sk} is the x-coordinate of Sk.

Step3: Verify from the authentication of tag encrypted message: t' = MAC_{k2} (C).

Step4: Decrypt the Ciphertext m = DEC_{k1} (C).

6. THE PROPOSED SCHEME IMPLEMENTATION RESULTS

The proposed scheme must be consuming less execution time to be accepted by the users. The PC that used to implement this scheme has a processor Intel core i7 CPU 2.20 GH and 4 GB RAM.

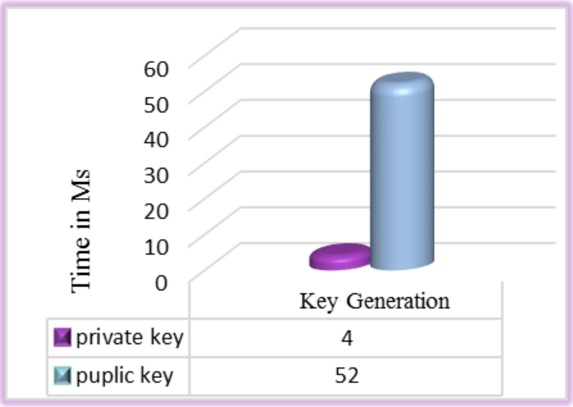

Fig5: The Execution Time for Private and Public Key Generation

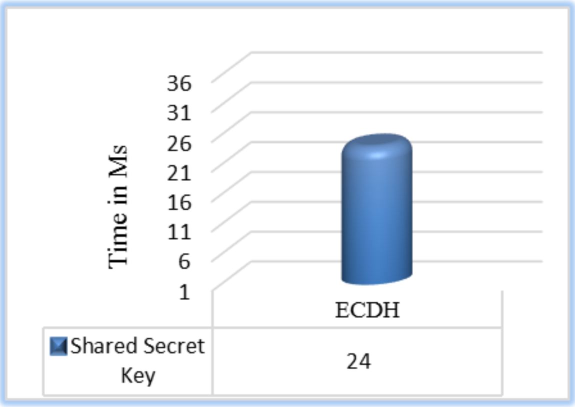

Fig 6: The Execution Time for Shared Secret Key Generation

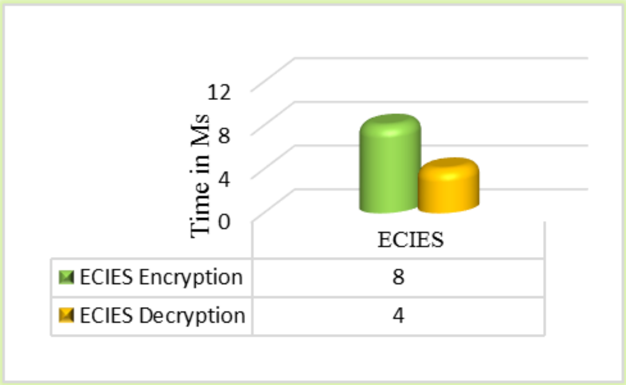

Fig 7: The Execution Time for Shared Secret Key Generation

7. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

This paper propose a more flexible and effective scheme to address data storage security problems in cloud computing. The use of MIBC reduce the complexity of key generation and eliminate the need to certificate issued, and ECIES provide data confidentiality and integrity. Future researches might consider in future such as use the hierarchical identity-based cryptography (HIBC) instead of MIBC and compare the result with this proposal.

8. REFERENCES

[1] Jeffrey Voas and Jia Zhang. 2009. Cloud Computing: New Wine or Just a New Bottle?. Published by the IEEE Computer Society.

[2] Sameeh A. Jassim. 2013. Mediated IBC-Based Management System of Identity and Access in Cloud Computing. MSc thesis. College of Computer, University of Anbar.

[3] Salim A. Abbas and Amal A. Maryoosh. 2015. Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography. IOSR Journal of Computer Engineering, Volume 17, Issue 4, Ver. I.

[4] Suli Wang and Ganlai Liu. 2011. File encryption and decryption system based on RSA algorithm. International Conference Computational and Information Sciences (ICCIS).

[5] Abbas Amini. 2012. Secure Storage in Cloud Computing. MSc thesis. Department of Informatics and Mathematical Modelling (IMM), the Technical University of Denmark.

[6] Puneetha C. and M. Dakshayini. 2014. Data Security in Cloud Using Elliptic Curve Cryptography. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5.

[7] Debajyoti Mukhopadhyay et al, 2014. Securing the Data in Clouds with Hyperelliptic Curve Cryptography. Available at: http://arxiv.org/ftp/arxiv/papers/1411/1411.6771.pdf.

[8] Swarnalata Bollavarapu and Bharat Gupta. 2014. Data Security in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3.

[9] Ravi Gharshi and Suresha. 2013. Enhancing Security in Cloud Storage using ECC Algorithm. International Journal of Science and Research (IJSR), Volume 2 Issue 7.

[10] Chester Rebeiro. 2009. Architecture Explorations for Elliptic Curve Cryptography on FPGAS. M.Sc. thesis. Department of Computer Science and Engineering, Indian Institute of Technology, Madras.

[11] William Stallings. 2011. Cryptography and Network Security principles and practice. 5th edition. Pearson Education, Inc.

[12] Ali Makki Sagheer. 2004. Enhancement of Elliptic Curve Cryptography Methods. MSc thesis. Computer Science, University of Technology.

[13] Darrel Hankerson, Alfred Menezes and Scott Vanstone, 2004. Guide to Elliptic Curve Cryptography. Springer-Verlag New York.

[14] Majid Khabbazian. 2004. Software Elliptic Curve Cryptography. MSc thesis. Department of Electrical and Computer Engineering, University of Victoria.

[15] Manali Dubal and Aaradhana Deshmukh. 2013. Achieving Authentication and Integrity using Elliptic Curve Cryptography Architecture. International Journal of Computer Applications, Volume 69– No.24.

[16] V. Gayoso Martínez, L. Hernández Encinas and C. Sánchez Ávila. 2010. A Survey of the Elliptic Curve Integrated Encryption Scheme. JOURNAL OF COMPUTER SCIENCE AND ENGINEERING, VOLUME 2, ISSUE 2.

[17] Marc Joye and Gregory Neven. 2009. Identity Based cryptography. IOS Press.

[18] Joonsang Baek et al. 2004. A Survey of Identity-Based Cryptography. Australian Unix Users Group Annual Conference.

[19] Divya Nalla and K.C.Reddy. 2003. Signcryption scheme for Identity-based Cryptosystems. Mathematics of Computation.

[20] Liang Yan, Chunming Rong, and Gansen Zhao. 2009. Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. Springer-Verlag Berlin Heidelberg.