Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 3, September 2018, pp. 1060~1067
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i3.pp1060-1067

Key Escrow with Elliptic Curve Cryptography – Conceptual Framework for Distributed Mobile Networks

B. Sugumar, M. Ramakrishnan
Department of Computer Applications, M.K. University, Madurai, India

Article Info

Article history:

Received May 2, 2018
Revised Jun 21, 2018
Accepted Jul 1, 2016

Keywords:

Cryptography
Distributed Systems
ECC
Key Escrow
Secret Sharing
Segmentation

ABSTRACT

In the large scale distributive environment involving mobile network, metadata server and storage applications, the data access and the security measures are of paramount importance. In parallel application processing, data is distributed across multiple servers and storage location. Ensuring confidentiality and availability of the data to the authorised users at the appropriate time involves high level of encryption algorithms, key management schemes and security algorithms. In this paper, key escrow scheme is implemented with the light weighted symmetric algorithm, elliptic curve cryptography in the distributed environment. Key escrow centre is established along with the metadata server and the encryption keys are segmented and shared among the multiple sub agents using Shamir threshold sharing scheme. The implementation of Key Escrow mechanism with Elliptical Curve Cryptography provides wide range of flexibility and confidentiality in the distributed environment. It also eliminates private secret sub key problem and thereby ensuring better security.

Corresponding Author:

B.Sugumar,
Department of Computer Applications,
M.K. University,
Madurai, India.
Email: sugumarbose89@gmail.com

1. INTRODUCTION

In the progressive data communication environment with mobility of the devices, various cryptographic methodologies like key management and encryption procedures are widely practised while transferring the data and also inside the data storage systems. When insightful and high value data are involved in the data communication process, it is the foremost responsibility of the organizations to comprehend the advantages, concerns, insinuations, and the constraints involved and accordingly employ suitable crypto measures [1].

Depending upon the integration level of the sub systems and the network components involved, the application of crypto procedures in the mobile networks can provide various types of security [2]. For instance, user specific protections are required for files shared within network attached storage where as Intrusion Detection System are required for detection of malicious data across the nodes in the entire network depending upon the level of mitigation.

The two major properties for the data communication are Confidentiality and Secrecy [3]. The availability of information to the authorized parties on demand is called as confidentiality. For a data transfer process involving encryption, method of data process should be deliberated and realized in such a way that no unauthorized party should interfere and determine the secret keys allied with the encryption mechanism and such procedures is termed as secrecy.

1.1 Encryption Procedures

The principal function of encryption procedures is to maintain the confidentiality of the data transmitted or stored. This is achieved by means of encryption algorithms which converts the plain text into the cipher text. The content of the cipher text cannot be found out without the decryption key. But the integrity of the data is susceptible, since the data can be modified by the intruder by predictable efforts even without the availability of the key. So for ensuring the data integrity, it is often essential to exercise additional methods [4]. The confidential awareness based on cryptoanalysis for two factor authentication process is presented by [5]. The comparison of various crypto analyses procedures are discussed. [6]. Basically, there are three categories of cryptographic algorithms. They are as follows:

Hash algorithms, in which hashing functions are used to map data of random or predefined sizes. Symmetric key algorithms, in which the same cryptographic keys are used for encryption of plain text in the transmitter side and decryption of cipher text in the receiver side. The keys may either be identical or some simple transformations involved between transmitter and receiver sides. Asymmetric key algorithms, in which the secret keys are divided into two parts, one public key which is un-trusted and the other one, private key which are kept as secret like symmetric key algorithm.

1.2 Encryption Point

Encryption point is defined as the placement of encryption and decryption mechanism within the data transmission path. Generally it is preferred that the encryption point should be available as close to the source of data. It increases the protection security of the data and also provides nature or characteristics of the data to be factored for security. But when considering the real time factors involved in the data transmission setting, this broad regulation often proves to be not viable [7]. For the selection of suitable encryption points, the following parameters and impacts shall be well thought out for the selection procedures.

Figure 1. Encryption Points – Parameters

As per the network design process, there are chances for various viable encryption points in the entire network. Accordingly, the parameters as shown in Figure 1 can be considered for the selection process. The various possible encryption points and their impacts based on the listed parameters are tabulated in Table 1. Based on the inimitable requirement, data sensitivity, secrecy level and topological structure of the individual organizations, the best encryption point is decided. Various encryption points are at application level, network level, file system level and device level [8]. In the storage environment involving mobile nodes and servers, the selection of encryption points at different levels is shown in Figure 2.

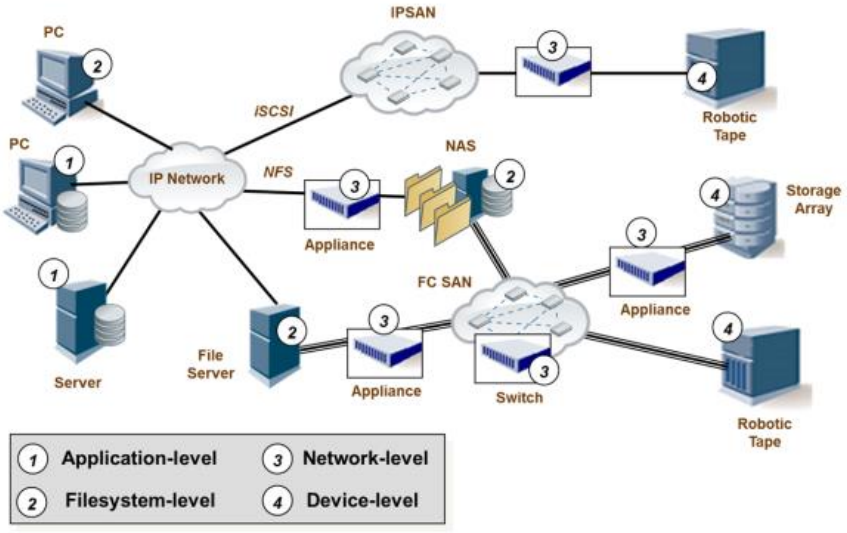

Figure 2. Encryption Point Location Options

Table 1. Parameters Influencing Encryption

IMPACT	APPLICATION	FILESYSTEM	NETWORK	DEVICE
Usability	Low	Low-Moderate	None	None
Availability	Can be significant	Can be significant	Low-Moderate (Redundancy)	Low-Moderate
Infrastructure	Can be significant	Can be significant	Low-Moderate	Low
Performance/ Throughput	Can be severe	Can be significant	Low	Low-Moderate
Scalability	Can be significant	Can be significant	Can be moderate	Minimal
In Motion Confidentiality	Excellent	Low-Moderate (NAS); Excellent (Host)	Low-Moderate	None
Business Continuity/Disaster Recovery	Can be extremely complicated	Can be complicated	Can be extremely complicated	Can be extremely complicated
Proof of Encryption	Can be complicated	Relatively easy	Low-Moderate	Can be complicated
Environmentals	Low-Moderate	Low-Moderate	Can be significant	Low

2. RESEARCH METHOD

2.1. Key Management Schemes

For achieving confidentiality, secrecy and availability of the data, there should be proper key management schemes. Automated key exchange mechanisms are used for the mobility data where as for static data, manual key encryption processes are utilized [9]. In the key management scheme, the life cycle of the keys and the keying procedures are of prime consideration which includes key generation, secure distribution, and activation and deactivation [10]. A simple key life cycle containing three phases, Pre-activation, Active and Disabled states are shown as flow list in Figure 3. Key management scheme involves the deliberation of following prime characteristics,

Availability of Key Materials, i.e. in case of external key management server, there may be times when keys are not accessible by the storage system, so there should be redundant key management server and the key materials need to be available for the encryption and decryption process without break in time.

Secure Transport, i.e. protection of the encryption keys during transmission. Encryption keys are the most sensitive parameter which needs to be transmitted for the successful encryption and decryption processes.

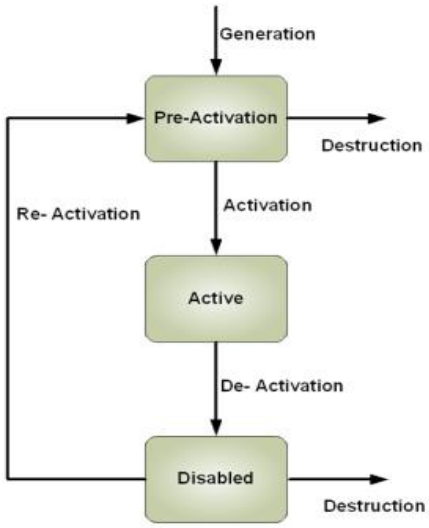

Figure 3. Simple Key Life Cycle

2.2. Key Escrow Concept

Due to the vast growth in the Information and Communication Technology (ICT), lot of computing devices with mobility and heterogeneous applications are deployed in competence of acuity, computing, perception and decision making process by using the network management tools. Transfer of information along with collaboration and dispensation is achieved by secured transmission measures [11, [12]. So for the accomplishment of information processing and communication across wider area, there needs a significant security tool which does not affect the communication efficiency as well as data secrecy [13]. An integrated approach combining random key generation and elliptic curver cryptography is discussed [14].

To overcome the threats faced by the mobile networks, taking apposite methodological safeguard is inevitable. Within the mobile networks, to ensure security of the data communication, it is very much essential to ascertain an effectual key management system.

In the cryptography domain, Secret Segmentation and Sharing (SSS) is the prominent concept gaining much attention. In this mechanism, the secret key is sub divided into multiple sub secret segments and shared among multiple nodes. For recovering the secret key, particular number of nodes from those received sub secrets has to provide their sub secrets and the distribution server will combine these particular number of sub secrets to analyse and retrieve the original information. Secret key segmentation and sharing as developed by [15], [16] based on the threshold algorithms is used in the key escrow based data communication.

2.2.1. Secret Segmentation and Sharing (SSS) by Shamir Threshold Scheme

Shamir Threshold Scheme is based on Lagrange Interpolation Formula (t, n) where t is the threshold limit and n is the number of nodes for which the sub secret segments are shared. The algorithm follows three essential procedures, viz. Initialization, Sub key distribution and Key Recovery.

In the Initialization process, a finite field is defined with the function F(p) where p is the prime number which is greater than number of nodes (p > n). Key distribution is selected by K n distinct non zero elements such that xi is the sub set of F(p). K is assigned to key xi sharers Ni and xi is public.

In Sub Key distribution process, K lets the n sharer (N1, N2 ……. Nn) shared key S is sub set of F(p) and S independently selected t-1 random elements and a is sub set of F(p) and t-1 build a polynomial function defined by f(x) = S+a1x+a2x2+ …….. at-1xt-1, and calculate yi= f(xi) where 1<= i<= n and Ni is assigned to the shared secret as his hierarchical key.

In Key recovery process, the number of sharers n in any group (N1, N2 ……. Nn) to generate their corresponding sub keys which is got when the point t reaches, (x1y1), (x2y2) ….. (x3y3) using Lagrange interpolation scheme. It is used to recover the function f(x) with the system key S = f(0).

2.2.2. Key Escrow with ECC in Distributed Networks

The Key Escrow scheme based on Shamir Threshold Secret key sharing can be implemented in the distributed networks having Elliptical Curve Cryptography encryption [11] [12]. From the algorithm view point, it is easy and space reducing to implement Shamir Threshold sharing. The sub private keys will not

exceed the space allocated for the original key. Also, updating process is simple. As a key calculation process to construct a (t-1) times of the polynomial function, the Computational Complexity will be C(t-1). In distributed networks Key Escrow with ECC is more secure and reliable. The adoption of Elliptical curve cryptography in the finite field with the structure of elliptical curves reduce the size of the key drastically thereby saving the space and also help in faster and secured data transmission.

The conceptual framework of distributed networks with Key Escrow is shown in Figure 4. The Mobile Network with heterogeneous operating systems is connected to the Metadata Server. Metadata Server is connected to the Storage server. Also the Metadata Server is associated by means of Key Escrow procedure through Key Escrow Center (KEC). End users of the distributed network communicate to the mobile network through the Storage Server. The data transmission between the mobile networks and the storage server takes place through direct parallel data exchange, where the data transmission between the metadata server and the storage server occur by means of state synchronization.

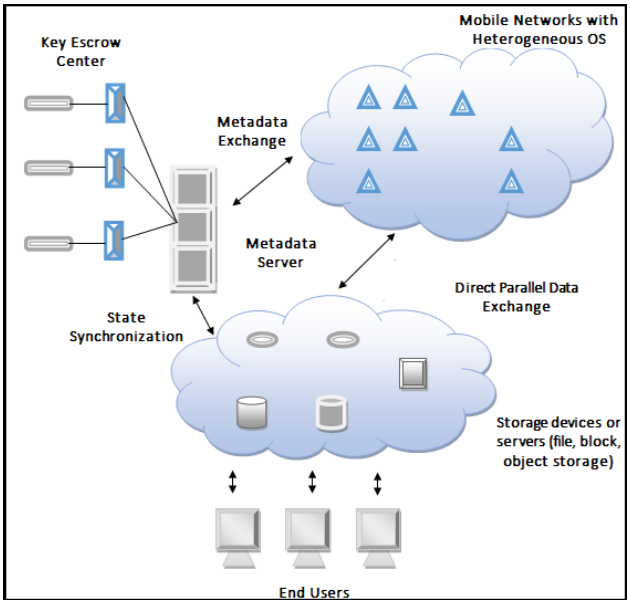

Figure 4. Conceptual Framework of Distributed Networks

By using Shamir threshold scheme for secret sub key sharing, the session key from the metadata server is sub divided into number of parts (n). Considering multi hosting cluster for the Key Escrow Center (KEC), the distribution of the data with the sub keys occurs uniformly. During the recovery process, KEC randomly choose the key elements equal to or greater that threshold (t). Under this scenario, KEC structure is as follows: When the number recovery keys are less than the threshold value, the sub key cannot recover the original key. So the expose of one or fewer keys will not affect the security of the system. So as long as the sub keys exposed is less than the threshold value, the attacker cannot connive to the original key.

2.2.3. Key Escrow with ECC - Solution

Similar scheme is implemented in the actual recovery of the original key by the sub keys. The steps involved in the recovery of original key are as follows:

1) Secret Division
2) Hosting the private secret sub keys
3) Recovering reader's sub key
4) Updating the secret sub key
5) Destruction of secret sub key of KEC

Secret Division occurs in the Initialization phase of the recovery mechanism. Light weighted public key based on ECC is stored in Metadata Server (MS). Before the private key distribution to the reader, it is segmented into sub secret keys in KEC. Following steps are implemented in the secret division process.

1. MS using public key of KEC and encrypt private key of reader and attach the digital signature of MS and send to KEC.

2. KEC receives the information, identify the authenticity of MS, after verifying authentication, it decrypts using the private key waiting to be segmented.
3. Based on Shamir (t,n) threshold, select t-1 random primes in F(p) domain and maintain secrecy.
4. After n times of private sub keys generation, the prime number is destroyed by KEC.
5. Polynomial for key composition generated based on the larger prime number and private secret sub keys are calculated.
6. KEC using public key ECC encryption along with digital signature, private secret sub keys generated.

Hosting the private secret sub keys involves following steps.

1. KEC verifying individual identity
2. After successful authentication, KEC used own private secret sub key, store it and notify the dependent server about the reception of the private secret sub key.
3. In case of failure of authentication, SEC writes error log

Recovering reader's sub key involves following steps.

1. When the MS authenticates the reader, but reader authentication fails, there incorrect results will be posted in MS, so no response. MS will write error log.
2. After investigation, if it is found that reader private key is lost, MS notice KEC and extract threshold amount of private secret sub keys from individual servers.
3. Lagrange polynomial interpolation and reconstruction of polynomial function is created by KEC.
4. For S = F(0), public key of MS encrypt S and send to MS with digital signature.
5. The MS successfully authenticates KEC and public key decrypted to obtain S. Intermediate state server will write S into reader.

Updating of the secret sub key involves following steps.

1. If the private secret sub key of the reader is updated in S, then KEC splits the S into secret segmentation
2. Private secret sub key is divided to identify KEC and public key matching to individual server.
3. Digital Signature of KEC is checked to confirm authentication and on successful verification, the private secret sub key is decrypted to obtain individual values.
4. If authentication fails, retransmission of private secret sub key happens.

Destruction of private keys involves not once their self destruction but also the destruction of secret sub key saved at KEC. In that case, the original private key cannot be restored. Following steps are involved.

1. MS informs KEC to destroy corresponding private secret sub key. Resultant threshold values to be identified and attachment of digital signature of MS separately sent to KEC.
2. KEC authenticates the identity of MS and on successful authentication, individual private key is decrypted.
3. On querying of the status of individual private secret sub keys, recycling process starts with change in status as "destroy".
4. Process results of KEC get back to MS.

2.3. Solution Analysis

The implementation of Key Escrow mechanism with Elliptical Curve Cryptography provides wide range of flexibility and confidentiality in the distributed environment. In the scheme, the process of key restoration has not happened in a single server. Multiple locations of encryption points such as Metadata Server, Reader and Key Escrow Center with light weighted key encryption process ensures elimination of slow response time and thereby assuring the prevention of attacker activity. The confidentiality of the distributed networks is enhanced by the restoration of the original key by the random threshold number of sub keys which is smaller than the original keys with separate secret segmentation. Optimum range of threshold value can be fixed for faster data encryption and decryption process and also ensuring secrecy.

3. RESULTS AND ANALYSIS

The implementation of the distributed environment involving Mobile Networks with Heterogeneous Operating Systems, Metadata Server, Key Escrow Center, Storage Server and the End Users is simulated in the Java / Netbeans environment. The data communication, file transfer process and the encryption methodology are implemented and the results analyses are compared for Key Escrow with ECC and the other process including Key Escrow with RSA scheme. The simulation metrics Computational cost and Key size are taken for consideration. From the conceptual framework implementation and comparison with different algorithms for distributed mobile networks, the Key Escrow with ECC shows better results in terms of Computational cost and Key size.

Computational cost is defined as the time taken for the computing an encryption process. It is based on the number or rule applications involved in the encryption scheme involved. While assuring the secrecy

measure, computational time involved should be as minimum as possible. Key Escrow with ECC ensures less computation cost as compared to Key Escrow with RSA algorithm. Key size is the vital parameter in the security level of the encryption process. By reducing the size of the key involved, the computational efficiency can be improved. Key Escrow with ECC guarantees better encryption when compared to Key Escrow with RSA with less value of key sizes. The computation cost analysis and the key size reduction analysis are shown in Figure 5 and Figure 6.

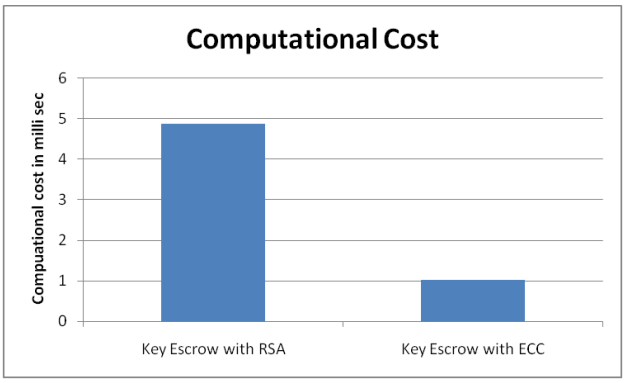

Figure 5. Computational Cost

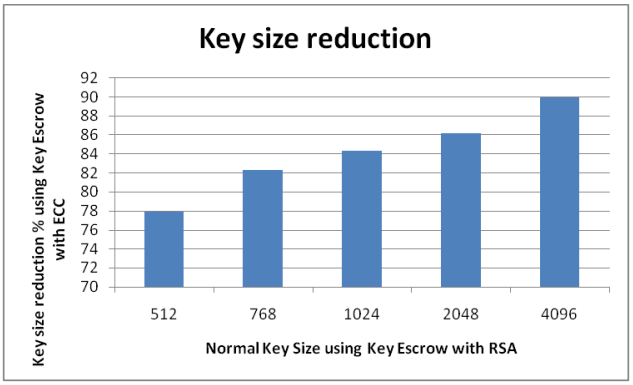

Figure 6. Key Size Reduction

4. CONCLUSION

With the reputation of the distributed and heterogeneous network involving mobile networks, metadata server and large storage server systems, much attention has to be paid for the security of the system. This paper concentrated on the implementation of Key Escrow scheme with the light weighted characteristics of Elliptic Curve Cryptography in the distributed environment. This has effectively eliminated private secret sub key problem on the distributed networks. From the conceptual framework implementation and comparison with different algorithms for distributed mobile networks, the Key Escrow with ECC shows better results in terms of Computational cost and Key size. The implementation of heterogeneous proto cols and devices in the cloud or Internet of Things (IoT) environment might invite future challenges in future for which the improvisation of dynamic key management schemes along with Escrow could provide the optimal solution for the challenges.

REFERENCES

[1] Canetti, Ran, and Hugo Krawczyk. "Analysis of key-exchange protocols and their use for building secure channels". *Advances in Cryptology—EUROCRYPT 2001*, pp. 453-474, 2001.

[2] Mahalingam, P., N. Jayaprakash, and S. Karthikeyan. "Enhanced Data Security Framework for Storage Area Networks". *In Environmental and Computer Science, 2009. ICECS'09. Second International Conference on IEEE*, pp. 105-110, 2009.

[3] Storage Networking Industry Association (SNIA) Technical White Paper. "Storage Security: Encryption and Key Management". August 26, 2015.
[4] Bu, Yingyi, Bill Howe, Magdalena Balazinska, and Michael D. Ernst. "HaLoop: Efficient iterative data processing on large clusters". *Proceedings of the VLDB Endowment*, Vol. 3, no. 1-2, pp. 285-296, 2010.
[5] Choi, Younsung. "Cryptanalysis on Privacy-aware two-factor Authentication Protocol for Wireless Sensor Networks". *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, Vol. 8, no. 2, pp. 296-301, 2017.
[6] Singh, Pooja, and R. K. Chauhan. "A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN." *International Journal of Electrical and Computer Engineering (IJECE)* Vol. 7, no. 4, pp. 2232, 2017.
[7] Eisler, Mike. "LIPKEY-a low infrastructure public key mechanism using SPKM." (2000).
[8] Gibson, Garth A., David F. Nagle, Khalil Amiri, Jeff Butler, Fay W. Chang, Howard Gobioff, Charles Hardin, Erik Riedel, David Rochberg, and Jim Zelenka. "A cost-effective, high-bandwidth storage architecture". *In ACM SIGOPS operating systems review*, vol. 32, no. 5, pp. 92-103. ACM, 1998.
[9] Barker, Elaine, Miles Smid, Dennis Branstad, and Santosh Chokhani. "A framework for designing cryptographic key management systems". *NIST Special Publication*, Vol. 800, pp. 130, 2013.
[10] Leung, Andrew W., and Ethan L. Miller. "Scalable security for large, high performance storage systems". *In Proceedings of the second ACM workshop on Storage security and survivability*, pp. 29-40. ACM, 2006.
[11] Cao, Zhenfu. "A threshold key escrow scheme based on public key cryptosystem". *Science in China Series E: Technological Sciences*, Vol. 44, no. 4, pp. 441-448, 2001.
[12] Cao, Zhenfu. "A threshold key escrow scheme based on public key cryptosystem". *Science in China Series E: Technological Sciences*, Vol. 44, no. 4, pp. 441-448, 2001.
[13] Li, Quandong, and Yanhui Zhou. "Security decision analysis based on A. Shamir's (t, n) threshold secret sharing scheme". *In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on IEEE*, pp. 2065-2068., 2012.
[14] Gayathri, P., Syed Umar, G. Sridevi, N. Bashwanth, and Royyuru Srikanth. "Hybrid Cryptography for Random-key Generation based on ECC Algorithm". *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7, no. 3, pp. 1293-1298, 2017.
[15] Shamir, Adi. "How to share a secret". *Communications of the ACM*, Vol. 22, no. 11, pp. 612-613, 1979.
[16] Pang, Liao-Jun, and Yu-Min Wang. "A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing". *Applied Mathematics and Computation*, Vol. 167, no. 2, pp. 840-848, 2005.