Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

ECC Based Authentication System for Performance Improvement in Security of Cloud

[1]Sumita Dey, [2]Dr. S. D.Joshi
[1] M-Tech Student, [2] Professor
[1, 2] Department of Computer Science, Bharati Vidyapeeth Engineering College, Pune, Maharashtra, India

Abstract— Recent years have witnessed the trend of Craning cloud-based services for very large scale distribution, content storage and processing. Security and privacy are among top concerns for the public cloud environments. Here new methodology was clopped for assessing the cryptographic key strength. This methodology needs calculation of true economics cost of key retrieval for the most common cryptographic primitives. Valuable insight provided by resulting points over the time in the selection of cryptographic key sizes. Analysis and recommendation of parameter is an very important task for cryptographers, crucially including key size and thus implying key strength, for cryptographic primitives. Then resulting data extrapolated for the Moore's Law and underlying algorithms by using complexity estimate, more than Moore, Less than Moore in an attempt to assess the longevity of associated keys. In this results in key size recommendations for public-key cryptosystems that over security comparable to popular symmetric cryptosystems; it leads to security estimates in terms of hardware cost or execution time.

Keywords— Cryptography, privacy & security of data in cloud, Key strength, cryptography algorithm, Time and budget model.

I. INRODUCTION

This system provides sufficient protection of the users and their private data against the Internet real-time security threats. This system has been summarized as the pervasive presence around people of a variety of "things" or "objects", like Radio Frequency Identification, mobile phones, sensors, tags, and actuators through which unique addressing scheme, all these things are able to communicate and cooperate with each other and their neighbouring components to reach common aims. The EBD, architecture of the emerging global Internet-based technical providing has as an impact on the privacy and security in global supply chain networks by providing exchange of goods and services of the involved individuals. The internet devices can be used to enable remote health monitoring and emergency notification systems. These devices can range from heart rate and blood pressure monitors to Advance devices are capable of handling specialized implants like either hearing aids or pacemaker. The paper explains about the concept of Small key sizes for authentication process and time constrained key generation. It does not contain any specific key management technique so it would provide us enough space to further decide ECC based key generation algorithms taking into account their lifespan also.

II. RELATED WORKS

In [2] explains the scheme, which is called as energy efficient control which is based on ECC and it is used for WSNs. Author have introduced an easy way to for using ECC, this ECC is a Public key Cryptography Scheme. Author has compared performance of this proposed system with the other access control scheme those are based on PKC and found it better. Another comparison done by author is with SKC based access control scheme was fair performance found by the author. The issue with this system is it requires Key Distribution Center available all the time which is not possible. Because it my denied users to be accessing the WSN nodes.

In [3] here, another three different schemes for WSN have been introduced by the author. These schemes have some better advantages than the current access control schemes as given: a) Resistance to node capture b) DOS and query reply attacks, and c) low expenses in calculation and communication. Here the system introduce by the author is not scalable as compared to the PKC algorithm because this proposed system is based on SKC algorithm. Besides in this system, privilege control was not provided to the user.

In [4] here author have introduce another scheme which is used for WSNs, it is called as Dynamic User Authentication scheme. Here, this new scheme i.e. dynamic user authentication scheme allows users to access any of the sensor node of the WSNs by using any mobile devises like PC's, PDA's, mobile phones etc. The proposed system methodologies allows authorized user to query sensor data at any of the sensor nodes in an ad hoc manner. It requires very simple operation to forcing very little computational load. On the other hand, the proposed system exposed to the possibility of being attacked to the reply and forgery attacks. Changing the password can create a problem to legal users. Sensor nodes allow password to be seen at any point.

In [5] the proposed scheme presents correction to the Wong scheme in [4]. This modification does not only remove weaknesses but also provides more security to it. The introduced system scheme can reduces the percentage of

ejaculation of the password from different nodes of the sensor and this scheme is very strong against forgery attacks and reply. This scheme allows changing or correcting the password to its user if they wish. This scheme has more desirable efficiency than the previous schemes. Mutual authentication does not allowed by this proposed system between the sensor node and user. Also, in this scheme a centralized gateway node needs for password change and registration. Here centralized approach of this system may create some problems to sensor networks; therefore many employed network does not uses base station.

In [6] under a realistic adversary model, author has introduced a distributed user access control. In this sensor would compose and may be conniving. Author introduces ECC based practical and scalable certificate which is based on local authentication. SKC scheme required pre-distribution and PKC deletes the management complicated key. The proposed system is very strong to complicity attacks of user. Besides, the feasibility of introduced system scheme is questionable. According to the author to generate a public key it takes 3.1 second and for conducting local authentication it takes 10.8 second. But in real life many systems in which user need to be authenticate by system itself in millisecond such systems deny these rates.

In [7] Author has implemented ECC based access control on Telos B mote test bed. The security of Elliptic curve cryptography depends on the difficulty of the Elliptic Curve Discrete Logarithm Problem. Author has introduced such an application which indicates that PKC is advantageous to provide security to WSNs for access control. In other way, introduced system i.e. access control scheme is accessible to impersonate attacks. On the other hand, proposed system has very poor performance. According to author it is 80 times more expensive then SKC based access control schemes. The current proposed system act's user authentication in 10.1 seconds, which is not acceptable in practical real life applications.

[8] In this paper the author has compared PKC and SKC based systems for access control in WSNs. And also pair wise key sharing between neighbouring access control and local and remote connections. According to the author, in this paper, the user access control system based on PKC is more auspicious in the form of memory usages, security and message complexity than the SKC based user access control systems. Besides, systems which are based on SKC algorithm are beneficial in the form of computational adaptability.

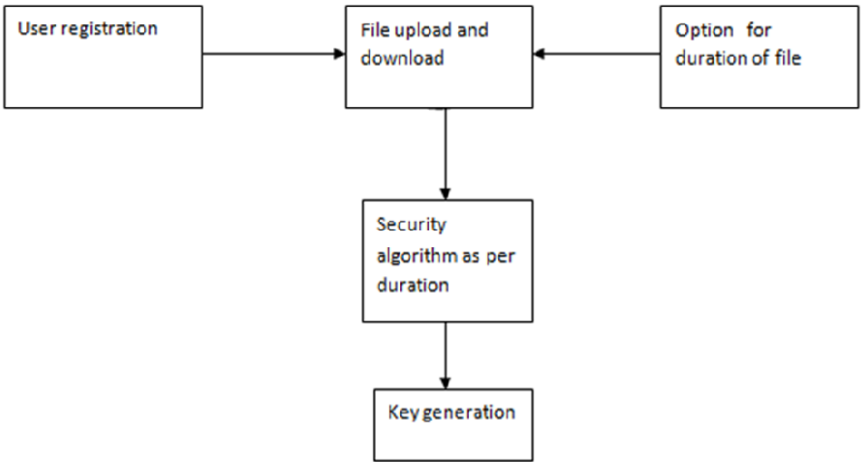
In [9] here in this paper author has implemented ECC based access control protocol which avoids vicious nodes from participating in the WSN at the very beginning. Also, key establishment is also included to help new nodes in establishing shared keys with their neighbours. This implemented protocol obtains better communication and computation work than RSA based algorithm protocol and is very strong against most of the well known attacks in WSNs. The usage PKC is very hot topic for discussion and it seems will be so far while. Unless it is proven, author have used major tool i.e. SKC tool for resource sensor networks.

In [10] here author introduce access control scheme based on ECC. This proposed scheme needs establishments of keys with neighbouring nodes so that it will gives a quick fix to complication of adding a different node to WSN. The main fact about this scheme that it is not secure from reply attacks in the scheme. Also the scheme loss the renewability hash chain that will cause to non-usability of WSN when last key was used in the hash key chain.

III. PROPOSED SYSTEM

The proposed architecture of the system consists of 5 stages. The system is described in detail below. At first stage user needs to register i.e. User registration. Then user can upload and download his important documents in upload and download stage. This is second stage. In third stage user can set time limit to his documents. Then the next stage is algorithm selection which is done by system itself according to the time limit. And last stage is key generation, Deffie-Hellman generates secrete key.

3.1 System divided into five phases:



A. User Registration

User registration is the main module of the EBD. In the EBD, user need to before uploading their files. The database contains all credential of the all users and keeps their data secure by using encryption and decryption algorithm.

B. Upload and Download

Uploading and downloading is another module of the project. After successfully registration, user can upload his important documents on the server of database for the specific time decided by the user. Another thing about downloading module, user can download documents before the expiry date of the document.

C. Expiry date selection

This module is about the main motto of the EBD project. User can set the time for his document. The importance of this module is to set time for user's documents. After the expiration of document user can't download it from his database. For the security purpose of document algorithm gets selected according to the time set in hours by the user.

D. Algorithm Selection

In our project we have AES, DES, SHA-256, and Diffie Hellman algorithm for security of the documents. If we think about AES algorithm, if user selects expiry time >= 40 hours, AES algorithm gets selected by the system. And according to the AES, process of encryption and decryption gets done and provides security to the data. Same process done to DES and Diffie Hellman but the time duration of both is different. DES having time duration <40, >=60 hours and SHA-256 has time duration <60, >=200 hours. In this project, Deffie Hellman algorithm is used for key generation.

E. Key generation

EBD has one special algorithm for purpose of key generation i.e. Deffie Hellman. System selects algorithm for data encryption and decryption according to the time selected by the user. This algorithm generates one secrete key and gives to the Deffie Hellman algorithm for comprising it. Deffie Hellman comprises the key and generate new key which has small size than the key generated by the either AES or DES algorithm. The main goal of the comprising the key is to provide more security and takes required less space in database.

Following example explains Deffie Hellman in details:

The first step is for A and B to agree on a large prime p and a nonzero integer g modulo p. A and B make the values of p and g public knowledge; For example A and B post something on their webpage, so C knows what they have post too. It should be best for A and B to choose g such that its order in F*p, it is large prime. The next step for A is to pick up a secrete integer a, that she does not inform to anyone about it. In other hand, at the same time B picks up an integer b and keeps it private. B and A uses their secret integers to compute.

$A = g^a \pmod p$ and $B = g^b \pmod p$

A computes this B computes this

They next exchange these computed values, A sends A to B and B sends B to A. Note that C gets to see the values of A and B, since they are sent over the insecure communication channel.

Finally, B and A again use their secret integers to compute

$A' = B^a \pmod p$ and $B' = A^b \pmod p$

A computes this B computes this

The values that they compute, A0 and B0 respectively, are actually the same, since

A 0 ≡ B a ≡ (g b) a ≡ g ab ≡ (g a) b ≡ A b ≡ B 0 (mod p).

These common values are their exchanged keys.

IV. RESULT AND DISCUSSION

This proposed system explains data storage in database and security of the data with the help of different types of algorithm such as AES, DES, and SHA-256.

Result:

Sr. No	Algorithm	Key size
1	AES (32 byte)	WgCTZt1fG3sLEQ=
2	Sha256(32 byte)	VDc61Xn5fhJgJku6p4MVbBJjmZc=
3	DES(8 byte)	Djn1yUuHbXh2yWgCTZt1fG3sLEQ=

V. CONCLUSION

Under the time-and-budget limited adversary model, we will also consider how to choose the size of modulus values as cryptography algorithm under different constraints as duration of file on cloud. The core point of this system having a server firm that can host the services for users connected to it by the network. To summarize, adequate protection was defined as the security offered in 1982 by the DES. It was argued that a system offers adequate protection until a given year if the cost of a successful attack in that year is at least 40M dollar days: a computation that lasts x days on piece of equipment that costs 40=x million dollars to build (for any reasonable x). Given this definition, for the most common cryptographic systems following general key length recommendations can be made.

VI. FUTURE SCOPE

In future we would like to focus on encryption algorithm considering the hardware constraint as hardware and memory required for computation. In future advanced encryption techniques can be used for storing and retrieving data from cloud. Also proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.

REFERENCES

[1] L. Atzori, A. Iera and G. Morabito, The Internet of Things: A survey, Computer Networks, doi:10.1016/j.comnet.2010.05.010, 2010.

[2] R. Sankar, S. Lee, X.H. Le, and I.Butun, ”An energy efficient access control for sensor networks based on elliptic curve cryptography,” Journal of Communications and Networks, 2009.

[3] Y. Shen, J. Ma, and Q. Pei, ”An access control scheme in wireless sensor networks,” in Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on, 2007, pp. 362-367.

[4] K. Wong, Y. Zheng, J. Cao, and S. Wang, ”A dynamic user authentication scheme for wireless sensor networks.” IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2006.

[5] H. Tseng, R. Jan, and W. Yang,”An improved dynamic user authentication scheme for wireless sensor networks.” IEEE Global Communications Conference, 2007.

[6] H. Wang and Q. Li,”Distributed user access control in sensor networks,” Distributed Computing in Sensor Systems, pp. 305-320.

[7] H. Wang, B. Sheng, and Q. Li, ”Elliptic curve cryptography-based access control in sensor networks,” International Journal of Security and Networks, vol. 1, no. 3, pp. 127-137, 2006.

[8] H. Wang, B. Sheng, C. Tan, and Q. Li,”Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control.” The 28th International Conference on distributed Computing Systems, ICDCS’08, 2008, pp. 11-18.

[9] Y. Zhou, Y. Zhang, and Y. Fang,”Access control in wireless sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 3-13, 2007

[10] H.F. Huang, ”A novel access control protocol for secure sensor networks”, Journal of Computer Standards and Interfaces, Elsevier, 2009.

