BIG DATA SECURITY ISSUES BASED ON QUANTUM CRYPTOGRAPHY

Prakruti Chaudhari[1], Prof. Riya Gohil[2]

[1] *Masters of Engineering Computer Engineering, LDRP-ITR, Gandhinagar, Gujarat, India*
[2] *Professor, Computer Engineering, LDRP-ITR, Gandhinagar, Gujarat, India*

ABSTRACT

Security of data one of the main concern in todays trend and nowadays mobile operators increase use on internet day by day so method work on security threats and transmit and receive data so using proposed topology use hybrid cryptosystem with asymmetric key for secure data. Consider parameter security, distribution mechanism, PSNR, SNR, MSR.

Keyword: - *Big data security and privacy; Quantum cryptography; key management; Data center etc.*

1. INTRODUCTION

In this paper we are presenting system where given query and the objective is to enhance the security and privacy with authentication with large authentication server's data with less complexity using ECC and RSA algorithm with quantum cryptography and to reduce complications and increase data security and authentication in mobile data center.

There are many solutions which are available for solving data security in data centers but implementing strong security for which big data (size > 1Terra Byte) being approached to the data center is one of the interesting topics. According to Couch and Robins [1], big data based on digital information has been doubling every 2 years since 2011. Based on the recent research, estimate also suggested that 2.5 zettabytes (2.5 x 1021 bytes) of information handled in 2012. Keeping privacy is another big issue in mobile data center which handles the data using proper management techniques. Goorden et al. [2] explained that Quantum cryptography (QC) supported to generate the authenticated key which provides security through the key management between the authentication server and users involved in the mobile data center. It includes efficient key searching and generating different size of keys with less complexity as big data security issues. Authentication supports privacy through the verifications and validations of entities which are authentication servers and mobile users. Thus, we can control the security and the privacy of big data which may be either sensitive or secret information. Here, proper authentication protocol which reduces the computation complexity when data centers handle the big data may be useful because the complexity prevents from creating the dynamic security solutions. Further, this complexity increases the traffic; delay and storage problems seem to be a quick chance of pilfering the data. This situation needs to be addressed using efficient authentication protocols to control the security and privacy dynamically. There is a trade-off between the complexity and big data security with traffic which is unavoidable during the data handling in the mobile data center.

2. RELATED WORK

This section discussed a literature survey on the use of the feature extraction methods.

Daojing He, Jiajun Bu, Sammy Chan, Chun Chen et al. [3] have made the system to solve the existing problem present a protocol named Handauth to achieve secure and efficient handover authentication and it provides session key establishment. The proposed approach is feasible for real applications. Existing mechanisms for handover authentication mainly focus on designing a secure authentication module, most existing approaches do not support user revocation.

Abdalraouf Hassan, Wesam Batrafi, Khaled Elleithy et al. [4] In this research Utilized the classic features of quantum mechanism, such as superposition and present the underlining mechanisms of quantum cryptography that enhances the security of data transmission with valid results that promise a low error rate that leads to a strong consistent key by raising the constraint of the security concept. The aim of quantum cryptography is to overcome the everlasting problem of unrestricted security in private communication. They designed an efficient algorithm that was developed based on BB84 and B92 techniques.

Alberto Porzio et al. [5] Every time we send personal information over a telecom channel a sophisticate algorithm protect our privacy making our data unintelligible to unauthorized receivers. Quantum cryptology exploits aspects of quantum mechanics, like superposition principle and uncertainty relations. DV protocols where single photon detection with very low efficiency (10%) in the telecom window and reaching high bit-rates. CV systems employ weak coherent light readily attainable in standard lasers. Homodyne detection guarantee efficiencies as high as more than 90% with commercial components.

Kritika Acharya, Manisha Sajwan, Sanjay Bhargava et al. [6] have presented Cryptographic algorithms such as DES,3DES,AES,RSA that are used for securing networks. In this paper to demonstrate the basic differences between the existing encryption techniques in terms of key size, speed, security. The strength of cryptography lies in the choice of the key; longer key resist attack better than shorter keys.

3. PROPOSED SYSTEM

From the surveillance of previous work done in this field, we have integrated different approaches for data security and feature extraction to achieve the higher security in communication between mobile user and mobile data center. The proposed system for big data security is depicted in Fig. 1. In Proposed system there are different stages which are:

a)Load database, b)Normalize data, c)Devide data into chunks, d)Apply distribution mechanism for different user using cryptosystem, e)use key management system, f)decryption of data, g)Store and manage data, h)final output .we are going to apply the RSA and ECC algorithm on cryptosystem.

i. RSA algorithm

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, ie on the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977[7].

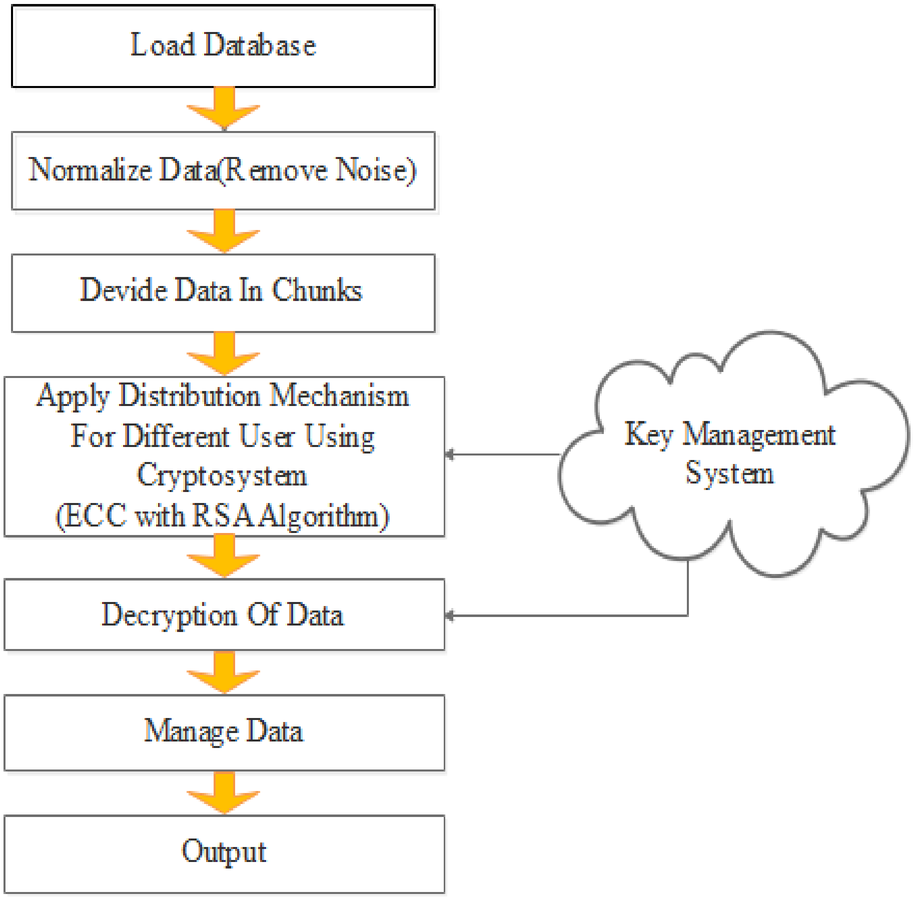
Load Database
Normalize Data(Remove Noise)
Devide Data In Chunks
Apply Distribution Mechanism For Different User Using Cryptosystem (ECC with RSA Algorithm)
Key Management System
Decryption Of Data
Manage Data
Output

Fig1. Proposed system

RSA Key generation encryption and Decryption

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated in the following way

1. Choose two distinct prime numbers p and q.

2. Compute n = p*q.

3. Select the public key (i.e. the encryption key) e such that it is not factor of (p-1) and (q-1)

4. Select the public key (i.e. the decryption key) d such that the following equation is true.

   (d*e) mod (p-1)*(q-1)=1.

5. For encryption calculate the cipher text CT from the plane text PT as follows

   $CT=PT^{e} \bmod n$

6. Send CT as the cipher text to the receiver.

7. For decryption, calculate the plane text PT from the cipher text CT as follows.

   CT^{d} mod n

ii. Elliptic Curve Cryptography Algorithm

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005. The algorithm was approved by NIST in 2006. Let E be an elliptic curve over finite field F_p . Let p be a point on $E(F_p)$ and suppose that P has prime order n. then the cyclic subgroup $E(F_p)$ generated P is $<P>=\{ \infty,P, 2P, 3P, 4P...........(n-1)P\}$.The prime P , the equation of the Elliptic curve E, and the point P and its order n are the public domain parameter. A private key is an integer d that is selected uniformly at random from the range [1,(n-1)] and the corresponding public key is Q=d*P [8], [9].

Key pair generation

Input Elliptic curve domain parameter (p,E,P,n)

Output Public key Q and private key d.

1. Select d =R[1,(n-1)]

2. Compute Q=d*P.

3. Return (Q,d)

The first task is to encode the plane text message m to be sent as an x-y point P_m. It is the point P_m that will be encrypted as cipher text and subsequently decrypted. To encrypt and send a message P_m to B, A Chosses a random positive intger k and produces the the cipher text $C_m =\{K*P, P_m + k*Q\}$, where Q is B's public key. The sender transmits the point C1=k*P and $C2=P_m+K*q$ to the recipent. To decrypt the cipher text, B multiplies by the first point in the pair by B's secret key and subtract the result from the second point as $P_m+k*q-d(k*P)=P_m+k(d*P)-d(kP)=P_m$..

Elliptic Curve Encryption

Input : Elliptic curve domain parameter (p,E,P,n), public key Q, plane text m

Output : Cipher text C_m

1. Represent the plane text m as a point

   P_m in E (F_p).

2. Select k [1,(n-1)].

3. Compute C1=k*p

4. Compute $C2=P_m+K*q$.

5. Return (C1,C2).

Elliptical Curve Decryption

Input : Elliptic curve domain parameter (p,E,P,n), private key d, Cipher text C_p.

Output : Plane Text m.

1. Compute P_m=C2-d*C1
2. Compute (P_m).

4. CONCLUSION

Nowadays mobile operators increase use on internet day by day so using proposed method work on security threats and transmit and receive data so using proposed topology use hybrid cryptosystem with asymmetric key for secure data. we will try to solve problems using parameter security, noise ratio, distribution mechanism PSNR, SNR, MSR using different algorithms to propose a new approach for achieving higher security between mobile user and mobile data center.

5. REFERENCES

[1]. Couch N and Robins B, Big Data for Defence and Security, report, Royal United Services Institute (RUSI), 2013; pp. 2 -36M.
[2]. Goorden S A, Horstmann M, Mosk A P, Škori B, and Pinkse P W H, "Quantum-Secure Authentication Of A Physical Unclonable Key", Optica, Vol. 1, No. 6 / December 2014
[3]. He D, Jiajun Bu, Sammy Chan and Chun Chen. Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks. IEEE Transactions on Computers, VOL. 62, NO. 3, MARCH 2013.
[4]. http://ieeexplore.ieee.org/document/7494155/
[5]. http://ieeexplore.ieee.org/document/6843831/
[6]. http://www.ijcat.com/archives/volume3/issue2/ijcatr03021009.pdf
[7]. William Stalling, "Cryptography and Network Security Principal and Practice", Third Edition, Pearson 2006. Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill Education Private Limited, Seventh Edition 2009.

[8]. Vivak Kapoor, Vivak Sonny Abraham, Ramesh Singh, "Elliptic Curve Cryptography", ACM Ubiquity Volume 9, Issuse 20, May 2008 .

[9]. P. K. Shau, Dr. R. K. Chhotray, Dr. Gunamani Jena, Dr. S Pattnaik, "An Implementation of Elliptic Curve Cryptography", International Journal of Engineering Research and Technology(IJERT) ISNN: 2278-0181, Vol 2 Issue 1, January 2013.