www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

ECDH algorithm for data storage security in cloud data centers

V.Manimaran[1], A.Renuka[2], M.Santhiya[2], B.Swetha[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College

[2]UG Scholars Department of Computer Science and Engineering, Nandha Engineering College

ABSTRACT

There may be some problem in speed of the application in the service model of cloud computing with massive storage and large users. Using ECDH instead of ECC algorithms, the cloud computing data security scheme is developed. The scheme uses ECDH key exchange mechanism on their personal inputs and protecting the sharing of file in the cloud environment. ECDH algorithm comprises the characteristics of faster speed and lower calculation cost when compared to other security schemes. It supports the mass data and large users on cloud environment.

Keywords: cloud computing; data security; ECC; ECDH

INTRODUCTION

Cloud computing is a network based model that requires to send data over the internet and store it in management system, through various resources in the form of dynamic and elastic shown in figure 1.1. Through network cloud computing provides easy extension and virtualized resources which can be provided quickly and it reduces the management work and interaction with service providers [1].

Under the model of cloud service, most of application software and data information is transferred to the large network data center of cloud computing service provider, management and data information maintenance work of all application programs is also entrusted to cloud computing service providers to complete.

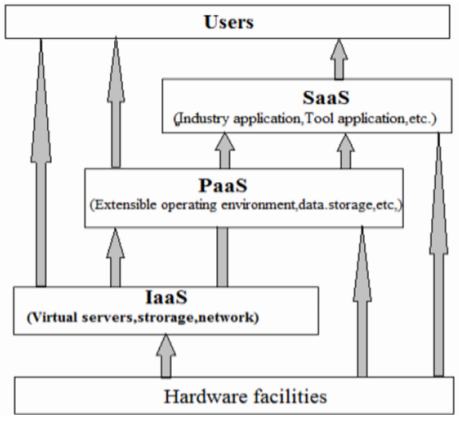

Figure: 1.1 Schematic diagram of cloud computing

Author for correspondence:
Department of Computer Science and Engineering, Nandha Engineering College

Complete statistics processing through the cloud computing center is known as facts gadget. Therefore, the cloud computing center has the duty to make sure facts protection and consumer behavior protection, which is typically, called the "inn model".

Cloud computing provides many security demanding situations and it also have a few risks within the safety of the information sharing which restricts the cloud computing services. The cloud computing additionally has the user comfort in conjunction with this security issues. Confidentiality, integrity and availability of garage facts is the principle awareness on records security trouble, and offers special characteristics as the confidentiality, integrity and availability [2].

THE RISK IN CLOUD COMPUTING

- The information security risk by Cloud service incredibility:
- There are security issues during data use, storage, reuse and delete stage.
- Security risks in virtualization introduced by shared technology gaps:
- All useful parts of the virtualization system have security issues, like virtualization management part, the virtual machine package and virtual machine monitor.
- Data reveal risk brought by Multi-tenancy model:
- Malicious tenants can attack many other tenants and these cloud computing infrastructure via shared resources. As an example, the tenant is in all likelihood to turn out to be the attacker's puppet gadget for defense weaker meat system, shape a denial of carrier vulnerability.
- Risks brought by malicious use of cloud platform in operational security:
- Operational risk is divided into two parts. The attacker can use the interface to invade the cloud environment, organize attacks; weak authentication mechanisms lead to the intruder can easy access the user account and log in virtual machine of the customers.
- If the company does not have adequate legal protections, then it may be liable when there is a data breach at the cloud service let exposes the company data.
- Lack of control risk in cloud computing:
- If you want change the service in future you have complete control over the feature.

RESEARCH BASIS AND STRATEGY

In view of the records protection threats delivered by cloud computing, it's far necessary to set up a mechanism to provide comfortable facts encryption and security protection to prevent records theft. Due to the big traits of facts, the traditional hash integrity verification is no longer applicable, and the conventional encryption era cannot be completely used. The way to efficiently help customers to affirm the cloud facts integrity and retrievable below the situation that users has no reproduction of data, is a key hassle to be solved.

For the time being, statistics security and privacy safety are the maximum involved cloud security problem by means of customers; researchers have recommend records protection. Protection as the primary goal of cloud safety structure. A cloud protection frame of reference together with cloud computing security carrier system and cloud computing protection standards and assessment machine; provide technical help for the cloud user protection [3].

An overview of different information protection problem approximately cloud computing. This paper is targeted on presenting safe, reliable cloud computing surroundings to make certain the safety of cloud computing [4].The diverse enterprise migrating to the scope of cloud computing, which specializes in how the employer enterprise safety migrating to the cloud [5]. In view of the safety problems about cloud computing, a few extreme protection chance existing in the associated subject [6].

The protection structure providing sharing and data acquisition, the conspicuous vicinity is setting the permission stage at unique levels [7]. The scheme makes use of RSA set of rules to encrypt huge files and garage date. The system can be used to keep quite a few data base, and the usage of linear technique is damage to the rate of statistics retrieval. Therefore, this gadget is most effective

relevant to the static statistics [8]. A machine to provide security in cloud network. The structure combines Diffie Hellman and AES encryption digital signature set of rules [9].All the above related paintings is focused on cloud computing safety troubles; offer precise mechanisms in a cloud environment to ensure the facts security.

Excellent studies have in common that have to access massive records in a comfy way and the complexity of encryption set of regulations used is unnoticed. In reality, the complexity of encryption set of guidelines right now impacts the charge of facts get right of entry to, specially inside the cloud computing surroundings; it desires to treatment the problem of massive information and the large customer's authentication. Therefore, it desires to find out some answers to achieve green and short manner to get secure records get proper of entry to. From this paper art work we use Elliptical Curve Diffie Hellman set of policies(ECDH) as a Proposed tool try and mastering the patient centric clear up the trouble of evaluate a cause in addition with the resource of several events on their private inputs protected sharing of file sharing. From the customers' factor of view, this architecture has better security and reliability in the cloud services and maintains data integrity simultaneously.

ALGORITHM BASIS

A.Elliptic curve cryptography

ECC algorithm principle

At the middle of 1980s, Ncal Koblitz and Victor Miller independently recommend Elliptic Curve Cryptography. After years of development, ECC has developed right into a mature public-key encryption gadget, had been carried out in more and more fields and come to be a research hotspot in the cryptography [10].

ECC is a form of public key encryption set of rules based on the elliptic curve. It's far a hard and fast of encryption set of rules with maximum encryption intensity within the gift public key encryption set of rules. As compared with conventional public key encryption set of rules, which includes RSA algorithm, ECC set of rules can provide the same security with quick key period. further, ECC also has different blessings and has a terrific attraction within the application of unique subject, inclusive of Wi-Fi devices and the larger server load. The Main advantages of ECC is the following [11-19]

- High safety performance: An encryption algorithm specially relies upon on the safety that it's far primarily based at the intractability of mathematical issues. ECC algorithm ECDLP, there may be no exponential order approach of solving ECDLP. By evaluation, solving ECDLP is plenty greater tough than solving IFP and DLP, therefore, the safety of ECC algorithm obtained guarantee powerfully.
- Small storage space: In well known, the important thing period of ECC is a great deal shorter than RSA and DSA and can provide secure energy identical to longer duration RSA keys. The distance of ECC key occupying may be very constrained; consequently, this feature for resource-constrained utility situations, along with the confined garage capability of a wireless device, has extraordinarily important significance.
- Fast processing speed: Underneath the identical condition of hardware, ECC is relative to other public key set of rules, for example, RSA algorithm, has greater benefits at the complete key processing pace. The characteristic has very sensible significance on accelerating handshake of SSL protocol.
- Low bandwidth requirements: To decrypt the long message, ECC and other encryption set of rules wishes the identical requirement of bandwidth. Whilst decrypt short message, ECC simplest desires a small bandwidth for short key length. The utility regions of public key encryption set of rules greater consciousness on brief message encryption and decryption, which makes ECC has more benefits below the condition of constrained bandwidth compared with different public key encryption set of rules. Elliptic curve refers to the plane curve determined by Weierstrass equation:

  y2 □ a1 xy □ a3 y □ x3 □ a2 x2 □ a4 x □ a6 □□□□

if F is a domain, ai F,i 1,2,...6 ,then(x, y) meeting (1) called the elliptic curve E point

On F domain.

The main basis of elliptic curve encryption and application field is to solve the difficulty of elliptic curve discrete logarithm; this difficulty is mainly reflected in the following:

- For a given arbitrary point c on the curve, Q kP, k F (a) ， it is easier for Q calculation by a given k and P, but more difficult for k calculation by given P and Q ;
- For the unknown a and b ， give X aP,Y bP ， calculating Z abP is difficult.
- Presently there is no formula the same as separate power drawback in finding field to unravel the separate power drawback normally curve .It means, in cryptography will profit of separate power within the finite field to get higher security of coding formula

Security analysis of ECC encryption algorithm

Each public key encryption algorithm guarantees safety via the problem of a complex mathematical hassle operation. Presently, those mathematical troubles can be classified into the three parts: The first is huge integer factorization hassle. The primary ideas of IFP can be honestly summarized two massive high numbers P, q as a public key; whose tough is to decompose these primes in a quick time.

With the development of hardware operation speed, the development of solving IFP techniques and the improvement of the parallel computing technology, i.e. clear up IFP by tens of hundreds of computer systems synergistically at the equal time.

Shorter duration of RSA keys cannot fulfill the safety necessities more and more. For the same type of encryption set of rules, an extended duration of secret is an awful lot more tough to interrupt than a shorter duration one, with higher safety. So one can make RSA key offer excessive enough safety electricity, researchers must increase the period of RSA keys to boom the issue of decoding IFP. The approach of increasing the length of RSA public key to growth the hardware overhead and gradual operation velocity because the fee makes the application efficiency of RSA set of rules is decrease and lower, this technique has additionally confined the software of RSA algorithm, specially for the hardware environment with limited sources.

The second is the discrete logarithm problem (DLP). The security of typical public key encryption algorithm EI Gama relies on the DLP. The basic ideas of DLP can be described as: Set Q to be a multiplication group in a finite field, and q is a generator of the group, is an arbitrary integer. Assume that Q and q a is known, and how to use mathematical method to get a. If Q is reasonable, when a value is bigger, it is much more difficulty for solving DLP. Now it can be done by the sub-exponential time complexity method to solve DLP.

The third is the elliptic curve discrete logarithm trouble (ECDLP). ECC set of rules is based at the intractability of ECDLP. ECC set of rules has brought on tremendous hobby of password researchers since it became proposed in 1985. Research in recent year’ s display that ECDLP can handiest be solved with the aid of the approach of exponential order time complexity presently. At gift, ECDLP is the simplest one of the issues that cannot discover the approach of exponential order time complexity to resolve the math hassle.

In a word, on the idea of achieving the identical protection level, the important thing period of ECC and other public key encryption set of rules isn't always an order of value; for that reason, ECC set of rules can attain a better protection stage especially through a shorter key length.

ECDH KEY EXCHANGE ALGORITHM

In Key agreement scheme is a brief key cryptographic protocol, that may make both verbal exchange aspects, and more than one member in an open and insecure channel negotiate to set up a consultation used by conversation protocol. Elliptic curve key agreement scheme-Diffie-Hellman version (ECDH) is one of the key settlement scheme typically used in elliptic curve cryptosystem, have been indexed in IEEE1363-2000 and ANSI X9.sixty three. It could save you the passive attack higher.

1976, Whitefield Daffier and Martin Hellman proposed Daffier- Hellman key exchange set of rules based mostly on the problem of computing discrete logarithms over finite subject [20].It maximum critical makes use of modular exponentiation over finite place to generate exchange facts encryption key every communication aspects may want to alternate.

Neal Kibitz and VS Miller used component multiplication operation of elliptic curve over finite area to generate information each communication sides could exchange, known as the ECDH protocol [21.because of use the trouble problem of discrete logarithm solution and calculation, ECDH set of rules has discovered out the session key negotiation characteristic, both communication facets has little data alternate and high security foundation. under the identical safety electricity, in comparison with Diffie- Hellman set of regulations, ECDH protocol calls for smaller key period, quicker computing pace and much less assets consumption [22-26].In this paper, the key settlement process primarily based on the ECDH set of rules is studied, and the consumer get right of entry to key of the cloud facts is generated as follows. pick a point P on the

ECC curve, and a random number d ($1 \le d \le n$ −1), then calculate:

$$Q = d * P \quad (2)$$

Among it, d is the private key, Q is the public key.

The sender encrypts the message records the usage of the general public key of the receiver, and the receiver decrypts the message information using its non-public key.

Firstly, according to the information input by users, establish a group of system parameter (q, F_q, E, P, n) , q Î{ $p, 2^m$ } , p is big prime number, m is the prime number, F_q is the finite field, E is the secure elliptic curve group of F_q , P is the basic point of big prime number n, P Î $E(F_q)$. The sender chooses r_A randomly, calculates:

$Q_A = r_A P$

Among it, 1 £= r_A £ n -1, and then sends Q_A to the receiver; The receiver chooses r_B randomly, calculates:

$Q_B = r_B P$

Among it 1 £= r_B £ n -1, and then sends Q_B to the sender; After the receiver gets Q_B , calculates:

$r_A Q_B = r_A r_B P$

After the sender receives Q_A , calculates:

$r_B Q_A = r_B r_A P$

Then it can be got:

$K_{AB} = K_{BA} = r_A r_B P$. (3)

It is the session key of both communication sides.

Scheme design

In this article, cloud set of rules identification authentication and data encryption operation plan are realized via using ECDH key alternate and ECC elliptic curve cryptosystem, the execution of the entire scheme consists of 4 steps [2].

Establish connection

When customers login the cloud computing machine for the first time, the machine reminds the person to create consumer account. The preliminary login system makes use of HTTPS and SSL protocols to set up connection.

Create account

Within the login method for the primary time, the system creates bills for users. Users fill within the account information. That info are dispatched to the cloud server, and saved inside the cloud. After account introduction for customers, the server generates user id and private key and public key, and to set up the secure connection between the cloud server and the consumer through the ECDH key change protocol. Person id is the particular identifier of person in a cloud environment and is sent to the user via a security channel, personal key and public key of consumer are used for ECC encryption at the back of.

Identity authentication

As soon as a person opens cloud server home web page, the system would establish a SSL connection routinely. Consumer inputs the consumer identification, and different info as before. The patron makes use of the server public key to encrypt the consumer facts, makes use of the hooked up SSL connection to submit a request to the cloud server. After receiving the request, the cloud server uses the server private key to decrypt the customer information first off, after which tests the legality of the consumer. If the user identification records fits, it'd establish a connection via the protocol, then person effectively logins into the server. The private key

of user and ECC set of rules parameters are dispatched to the consumer for the lower back encryption.

Data Exchange

Information first off, after which tests the legality of the consumer. If the user identification records fits, it'd establish a connection via the protocol, then person effectively logins into the server. The private key of user and ECC set of rules parameters are dispatched to the consumer for the lower back encryption.

ANALYSE THE SECURITY

It is able to be seen that the cozy elliptic curve choice ensures fixing ECDH to be computationally infeasible. Safety of the important thing settlement scheme proposed in the article may be analyzed from the subsequent 4 components.

Verbal exchange protection

The scheme realizes the two-way authentication between A and B; the attacker cannot pretend to be any part of both communication facets, beautify the protection of both conversation side. Assume that the attacker can pretend to be A, for s and kA is unknown, (X1 , X 2) cannot be generated. The public key of B cannot be obtained similar to A with the aid of calculation; additionally the attacker cannot faux to be B, then authentication failure.

Key security

Both communication sides are going on and the premise of two-way authentication before the key agreement, and nA , nB is randomly selected when key agreement, which makes attackers cannot launch future possible session key from a known session, so the key is safe.

Forward security

Due to the difficulty of ECDLP, attackers cannot recover nA ,nB from the transmitted information on channel: GA , GB , (X1 , X 2) , which is still safe.

Prevent replay attack

Because NA, NB is randomly selected, it can guarantee the freshness of information. When key agreement and both communication sides confirmed that the key is obtained in the agreement.

VERIFICATION ON EXPERIMENT

From this paper, key agreement is based on ECDH; comparison scheme is based totally on DH key change. The research popularity of discrete logarithm suggests that after key period of DH is 1024 -bit, it can ensure the medium and long time protection. For comparison, the paper makes key agreement speed tests for ECDH with key length being 96 bit, 122-bit, 160 bit and DH scheme with 512-bit, 768-bit, 1024-bitt respectively. The experimental results are shown in table 1.

Scheme/Key length	CPU Occupation time (ms)	
	Key pair generation	***Shared Key Generation***
DH/512	7.4	7.3
DH/768	16.2	16.0
DH/1024	35.6	35.2
The scheme of the paper/96	1.8	1.9
The scheme of the paper/122	2.0	2.1
The scheme of the paper/166	2.3	2.4

CONCLUSION

The item first analyzes the protection troubles of privations data of customers in cloud computing device, points out that using traditional linear encryption set of policies has the trouble of low performance and sluggish pace inside the big surroundings of cloud computing, this is difficult to put into use within the sensible software. For this, put forward a protection scheme of cloud computing information. This scheme has the advantage of the linear cryptography to set up secure connection within the cloud environment, encryption techniques of index to encrypt statistics, make certain the authenticity of clients and information protection via the four steps. Primarily based on ECDH key alternate set of rules, it is able to provide quicker and better authentication and connection for cloud computing client. Relative to distinctive linear algorithm, the usage of ECC set of rules has developments of decrease calculation cost and faster velocity.

Acknowledgement

The authors would love to acknowledge the many beneficial recommendations of the reviewers and the members on earlier variations of this paper. We also thank the authors of the references.

REFERENCES

[1]. Mell P and Grance T. The NIST Definition of Cloud Computing[R/OL]. http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, 2010-02-11.

[2]. Tirthani N, Ganesan R. Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Crypto graphy[J/OL]. IACR Cryptology ePrint Archive, 2014: 49.

[3]. FENG DengGuo, ZHANG Min, ZHANG Yan, et al., Study on Cloud Computing Security, Journal of Software, 2011, 22(1):71-83.

[4]. Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security and Privacy, 2010, 8(6):24-31.

[5]. Farzad Sabahi. Cloud Computing Security Threats and Responses[C]//Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference,Xi'an, 2011, 27-29.

[6]. Ashish Agarwal, Aparna Agarwal. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946], 2011:257-259.

[7]. Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment// Software Engineering (CONSEG), CSI Sixth International Conference, Indore,2012:1-8

[8]. M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing//Recent Trends In Information Technology (ICRTIT), 2012 International Conference, Chennai,Tamil Nadu,2012:463-467.

[9]. Prashant Rewagad, Yogita Pawar in. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing// 2013 International Conference on Communication Systems and Network Technologies,Gwalior,2013:437-439.

[10]. HONG-Li,DU Yaozong.ECC-based key agreement and mutual authentication scheme.Computer Engineering and Design,2007,28(13):3076-3078.

[11].] Koblitz A H, Koblitz N, Menezes A.Elliptic curve cryptography : The serpentinecourse ofa paradigm shift.Journal of Number Theory,2011,131(5):781-814.

[12]. Gupta V,Gupta S,Chang S.Performance analysis of elliptic curve cryptography for SSL//Proceedings of the 1st ACM workshop on Wirelesssecurity,ACM,Atlanta,2002:87- 94.

[13]. Yang J H,Chang C C.An ID-based remote mutual authentication with keyagreement scheme for mobile devices on elliptic curve cryptosystem.Computers&security,2009,28(3):138- 143.

[14]. Mohammadi S,Abedi S.ECC-based biometric signature:A new approach in electronic banking securit//2008 International Symposium on Electronic Commerce and Security,IEEE,2008:763-766.
[15]. Ko W T,Chiou S Y,Lu E H.An improvement of privacy-preserving ECC-based grouping proof for RFID//Cross Strait Quad-Regional Radio Science and Wireless Technology Conference(CSQRWC), IEEE,2011:1062-1064.
[16]. Du X,Guizani M,Xiao Y,et a1.Transactions papers a routing-driven Elliptic Curve Cryptography based key management scheme for Heterogeneous Sensor Networks[J].IEEE Transactions on Wireless Communications,2009,8(3):1223-1229.
[17]. Liu A,Ning P.TinyECC:A configurable library for elliptic curve cryptographyin wireless sensor networks//Intemational Conference on Information Processing in Sensor Networks, IEEE,2008:245-256.
[18]. Galbraith S D,Lin X,Scott M.Endomorphisms for faster elliptic curve cryptography on a large class of curves[J].Journal of cryptology,2011,24(3):446-469.
[19]. Diffie W,Hellman M.New Direction in Cryptography. IEEE Transaction on Information Theory,1976,6(22):644-654.
[20]. Lee W,Lee J.Design and Implementation of Secure E-mail system Using Elliptic Curve Cryptosystem. Future Generation Computer Systems, 2004, 20(2): 315-326.
[21]. HONG Li, DU Yao-zong, ECC-based key agreement and mutual authentication scheme, Computer Engineering and Design, 2007,28(13): 3076-3078.
[22]. Zhineng Liu, Yanli Zhao, Hui Fan, Selection of Security Curve in Elliptic Curves cryptosystem Based on ECC, Journal of Huaihai Institute of Technology, 17(1), 2008 :25-28.
[23]. Huifang Hou, Yunxia Wang, Provable Secure Authentication Protocol Based on CPK and Improved ECDH Algorithm, Computer Science, ,38(9): 2011, 55-58.
[24]. LI Guan-peng, TIAN Zhen-chuan, ZHU Gui-liang , Database Encryption System Based on ECDH and Rijndael, Computer Engineering, ,39(4) : 2013, 173-179.
[25]. Shengjin Li, Hongchang Zhang, Dawei Zhou, An Authenticated Key Agreement Protocol Based on ECDH, China Information Security, 9(7), 2011, :71-7