IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cloud Data double Security Using DES and ECC

Archana Singh Parmar [1],
Monika Sharma [2],

[1] *Assistant Professor, Department of Information Technology, India*
[2] *Assistant Professor, Department of Information Technology, India*

Abstract - *Data security is, protecting data from ill- conceived get to, utilize, intrusion, change, examination, recording or destruction. Cloud computing is a network-based service that provide sharing of resources such as virtual machine, storage, network, software and applications etc. It helps to reduce capital costs since that cloud users only need to rent resources according to their requirements and pay the services they use. It is very flexible since users can access its service in any place through internet. However, a variety of security concerns such as integrity, availability and privacy act as barriers for cloud users to adopt the cloud service. The key issue in effective execution of Cloud Computing is to adequately deal with the security in the cloud applications. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using two cryptographic algorithms back to back to enhance the security in cloud and provide the digital signature as per different perspective of cloud customers.*

Key Words: **Cloud Computing, Elliptical Curve Cryptography, Cryptography 1.**

INTRODUCTION

Cloud computing provides a new way of services by organizing various resources and providing them to users based on their demands. It also plays a crucial role in the next generation mobile networks and services (5G) and Cyber-Physical and Social Computing (CPSC). Cloud computing and capacity arrangements give clients and ventures different qualities to store and process their information in third-party data centers that might be arranged a long way from the user running in remove from over a city to over the world. Cloud computing counts on sharing of resources to attain endurance and economy of scale, similar to a utility (like the electricity grid) over an electricity network. Storing data in the cloud greatly decreases storage load of users and brings them access comfort, thus it has become one of the most important cloud services. Possibilities guarantee that, cloud computing enables organizations to keep away from forthright infrastructure costs (e.g. purchasing servers). Likewise, it engages associations to focus on their core businesses instead of investing energy and supports on computer infrastructure. Cloud computing enables undertakings to get their applications up and running speedier, with enhanced sensibility and less maintenance. Be that as it may, concerns are starting to create about how safe Cloud is? as more data on people and organizations are being put in the cloud. Disregards to all the hype surrounding the cloud, enterprise customers are still unwilling to place their business in the cloud. One of the real concerns which lessens the development of Cloud computing is security and impediment with data security and information protection keep on infecting the market. Cloud information storage augments the danger of data spillage and ill-conceived get to. The architecture of cloud poses certain dangers to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be alert in interpreting the risks of data intrusion in this new environment.[1] The security concerns with respect to cloud computing are end-user data security, network traffic, file systems and host machine security which can be addressed with

the help of cryptography to a considerable level. "Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security.

2. LITERATURE SURVEY

1.Wang, L., Tao, J., & Kunze, M. in their research paper "Scientific cloud computing: Early definition and experience" says that, Computing clouds equips users with services to access hardware, software, and data resource. Some clouds service models are:

i) HaaS: Hardware as a Service

Hardware as a Service was proposed possibly at 2006. As an outgrowth of rapid advances in hardware virtualization, IT automation and usage metering and pricing, users could buy IT hardware - or even an entire data center/computer center- as a pay-as-you-go subscription service. The HaaS could be flexible, scalable and manageable to meet your needs.

ii) SaaS: Software as a Service

Software or application is hosted as a service and provided to customers across the Internet, which excludes the requirement to install and run the application on the customer's local computer. SaaS therefore amends the customer's headache of software maintenance, and decreases the expense of software purchases by on demand pricing.

iii) DaaS: Data as a Service

Data in various formats, from various sources, could be accessed via services to users on the network. Clients could, for instance, control remote information simply like work on local disk or access data semantically on the Internet.

3. Cryptographic Algorithms :

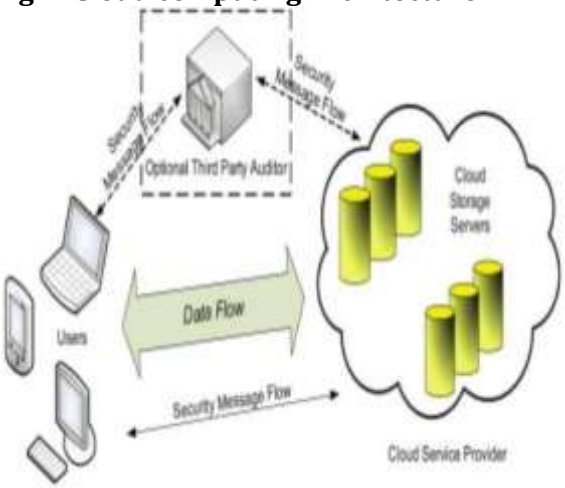
1) Data Encryption Standards (DES)
2) Advanced Encryption Standards (AES)
3) Triple – DES
4) RSA
5) Blowfish
6) ECC

These algorithms can be applied successfully in cloud environment.

Three entities involved in the cloud computing are users, cloud service providers and the third-party auditors. Securing the data in cloud service required cryptographic encryptions which isolates the users from accessing others information or workload. The data stored in the cloud server was encrypted and the user access the data from the cloud server will decrypt the data with the key provided for access. The encryption is the process of converting the plain information into a chipper text. The chipper text is an order less or meaningless information which is generated by the encryption algorithm in the certain pattern. Decryption is the process of converting the chipper text into the original plain text. The decryption algorithm reverses the process of encryption to generate the plain text. The main aim of the encryption algorithm is to generate a tough chipper text which should be ordered to decrypt without using the proper decrypt key. The size of the key proportionally toughens the decryption of chipper text without a proper key.

Selecting the encryption algorithm is very important. The quality of the encryption algorithm should be maintained strictly. The algorithm looks promising may be very easy to break. A tougher encryption algorithm to be selected to secure the data from attack.

Fig.1: Cloud computing Architecture



4. Data Security Issues

As many are moving to cloud storages, there are many potential attacks attempted few of them are:

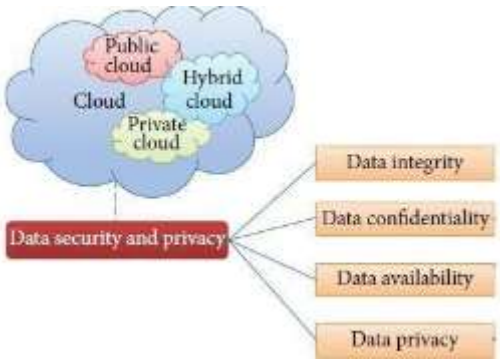
a) Denial of Service(DoS) attacks:

b) Side Channel attacks:
By placing a malicious virtual machine to a target cloud server an attacker can launch a side channels attack.
c) Authentication attacks:
There are many different ways to authenticate users, and methods used are a frequent target of attackers.
d) Man-in-the-middle cryptographic attacks:

e) Inside-job:
Here person, employee or staffs who have the knowledge of system can attack the cloud system.

Security aspects can be classified as data integrity, confidentiality, availability and privacy as show in figure below.

Fig 2: Various security concepts



5. Cloud Computing Entities

Figure 3 shows the cloud computing entities:

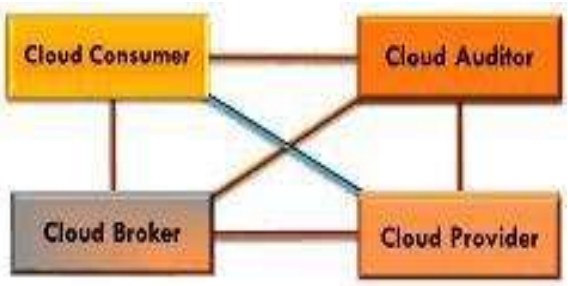


Fig3 : Cloud Computing Entities

i) **Cloud Consumer**: One who uses a cloud provider's resources, from a company to an individual.
ii) **Cloud Auditor:** The goal of Cloud Audit is to provide cloud service providers with a way to make their performance and security data readily available for potential customers.
iii) **Cloud Broker**: the Service brokers concentrate on the negotiation of the relationships between consumers and providers. There are two major roles for brokers: SLA Negotiation and VM Monitor. The SLA Manager takes care that no Service Level Agreement (SLA) is violated and VM Monitor the current stated of virtual machines periodically at specific amount of time[2].
iv) **Cloud Provider**: The Company who makes the cloud available to others. They are in charge of maintenance/ upkeep of the cloud and, of course, making sure it is always available to the cloud user.

6 Proposed system

1) For Encryption of text files:
Upload Text file.
Implementing the DES algorithm of Encryption to generate Cipher text 1.
Implementing the ECC algorithm of Encryption to generate Digital Signature as cipher text2
Store cipher text1 and Cipher Text2 into Database.
2) For Decryption of text files:
Read Cipher Text2 from Database.
Implementing the ECC algorithm of Decryption to decode digital signature cipher text2
Implementing the DES algorithm on cipher1 of Decryption to generate Plain text.
Display Plain Text to User

7 Algorithm of DES and ECC

7.1 Digital Encryption Std :

The Data Encryption Standard (DES) [2] is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64- bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64- bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds [10]. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm as shown in figure

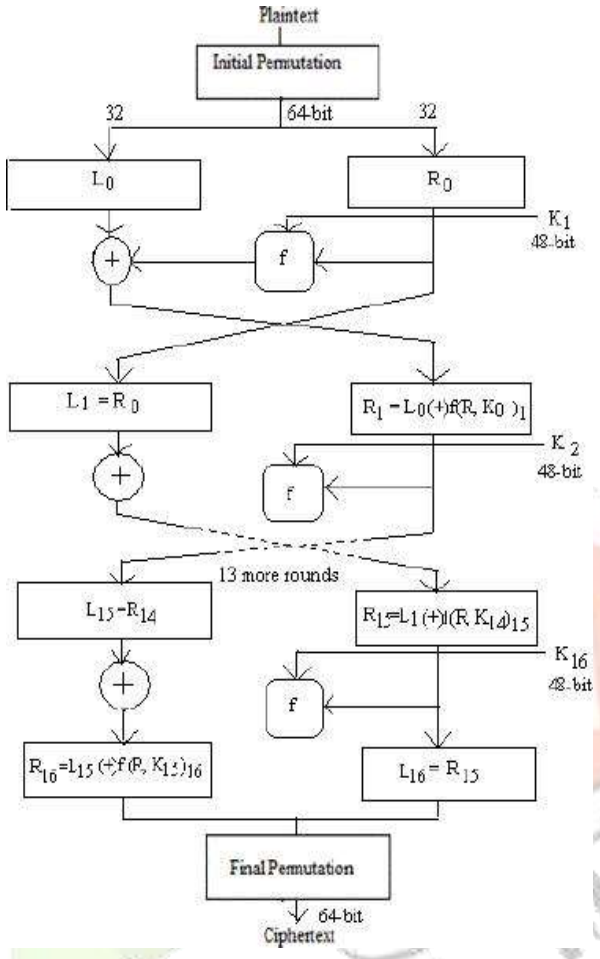


Fig 4: DES cycle

7.2 Elliptical Curve Theory

1. **Algorithms for data security using ECC**

Assume we have two organizations A and B. A and B act as public clouds with data, software and applications. A want to send data to B's cloud securely and data should be authenticated. Here we can use digital signature and encryption to data with ECC in order to send secure data from A to B. Suppose B wants a document from A's cloud, B's user will initialize a request to A's user, A's user select the corresponding document from A's cloud data storage and then apply hash function, it will give message digest. Sign the message digest with his private key by A's software. It is called digital signature. Encrypt digitally signed signature with B's public key using ECC algorithm. Encrypted cipher message will be send to B. B's software decrypt the cipher message to this document with his private key and verify the signature with A's public key.

We assume both A and B agree to some public-known data item:

The elliptic curve equation: $y_2 = x_3 + ax + b$, where $4a_3 + 27b_2 != 0$ The elliptic

group computed from elliptic curve equationA, B taken from the elliptic group

Then we have some algorithms for data security using ECC

Key generation

I.

II.

A selects random integer dA, which is A's private key A generates a public key PA = dA * B

III. B selects a private key dB and generates a public key PB = dB * B

IV. A generates the security key Key = dA * PB

V. B generates the security key Key = dB * PA Signature

Generation

I. For signing a message m by sender of cloud A, using A's private key dA

II. Calculate e = HASH(m), where HASH is a cryptographic hash function, such as SHA-1

III. Select a random integer k from [1, n-1]

IV. Calculate r = x1 (mod n), where (x1, y1) = k * B. If r = 0, go to step III

V. Calculate $s = k^{-1}(e + dA * r) \pmod n$. If s = 0, go to step III

VI. The signature is the pair (r, s)

VII. Finally, send signature (r, s) to B

Encryption algorithm Assume A send an encrypted message to B

I. A takes plaintext message m, and encodes it onto a point, pm, from the elliptic group

II.

III.

IV

A chooses another random integer, k from interval [1, p-1]

The cipher text is a pair of points pc = [(kB), (pm + k * PB)]

Send cipher text pc to B

Decryption algorithm

B will decrypt cipher text pc

I. B computes the product of the first point from pc and its private key dB, which is kB * dB

III. B takes this product and subtracts it from the second point from pc, (pm + k * PB) – kB * dB, since PB = dB * B, so the difference is pm

JJJ. Finally, B decodes pm to get the message m Signature Verification

If B wants to authenticate A's signature, B must have A's public key pA

Verify that r and s are integers in [1, n-1]

Calculate e = HASH(m), where HASH is the same function used in the signature generation

III. Calculate w = (s – 1) % n

IV. Calculate u1 = e*w % n and u2 = r*w % n

V. Calculate (x1,y1) = u1 * B + u2 * PA

VI. The signature is valid if x1 = r % n, otherwise invalid

9. Advantages of ECC Algorithm

Many cryptographic algorithms are introduced to perform asymmetric key generation for encryption and decryption process. In that RSS algorithm is a widely used method for cryptographic function. But the RSS algorithm needs more powerful processors and the memory unit. To overcome these limitations ECC based algorithm is developed to provide the tighter encryption technique which challenges the hackers technologies. In 2010 the researchers in cryptosystem concluded that the keys with longer size would provide maximum security over the attack, but the theory is no longer succeed. Lengthening of key size results to the undesirable effects on encryption. In the case of RSA algorithm doubling the size of the key decreased the performance of the algorithm. The advantage of the ECC algorithm based on the key size is analysed to better than the RSS algorithm. Table 1 shows the performance of the RSS and the ECC algorithm based on the key size.

Key Size of ECC	The key size of RSS	The ratio of the key size
160	1024	1:6
224	2048	1:9
256	3072	1:12
384	7680	1:20
512	15360	1:30

Table 1 : Comparison od ECC and RSA

Table 1 clearly shows that the performance of the ECC algorithm is higher than the RSS algorithm even in smaller key size. Increasing the key size of ECC increases the performance of it, but the RSS needs to increase more than double the value of it to match the performance of the ECC algorithm. Moreover, the speed of generating the key is 1000 time faster than the RSA algorithm.

10. Application of ECC algorithm in Cloud

ECC algorithm undergoes the four-step procedure to provide security in cloud architecture. The four steps include Connection generation, account creation, authentication and data exchange. Two initial steps were undergone for the first time connection. Connection generation and account creation were performed by the user to generate a cloud application interface. HTTPS and SSL protocols are used to generate communication with the cloud systems. The third process is authentication. The authentication is performed by applying the connection ID which is generated during the account creation process. And the ECC algorithm plays at the data exchange process. The Data was encrypted and shared with the cloud storage, and the user who downloads the data from the cloud should decrypt the downloaded data with the appropriate private key. The sender encrypts the data with the public key, and the user decrypts it using the private key. The data in the middle (in cloud storage) is in the form of chipper data. This provides the security in handling cloud storage or virtualisation.

11. Conclusion:

Cloud Computing can become more secure using cryptographic algorithms. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms.
But the existing cryptographic algorithms are single level encryption algorithms. Cyber criminals can easily cracked single level encryption. Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage.

As our proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data by confirming the Digital Signature . Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using single level encryption.

12. REFERENCES

1. [1]S. Subashini, V. Kavitha -Anna University Tirunelveli, India," A survey on security issues in service delivery models of cloud computing"ELSEVIER- Journal of Network and Computer Applications Volume 34, Issue 1, January 2011,
2. Jashanpreet Pal Kaur, Rajbhupinder kaur, Yadavindra College of Engineering, Talwandi Sabo, Bathinda Punjab, "Security Issues and Use of Cryptography in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014, ISSN: 2277 128X.
3. Wang, L., Tao, J., & Kunze, M. (2008). "Scientific cloud computing: Early definition and experience". Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, Austin, TX, 825–830.
4. Reservoir Project [URL]. http://www-03.ibm.com/ press/us/en/pressrelease/23448.wss/, access on June 2008.
5. Amazon Elastic Compute Cloud [URL]. http://aws. amazon. com/ ec2, access on Nov. 2007.
6. IBM Blue Cloud project [URL]. http://www- 3.ibm.com/press /us/en/pressrelease/22613.wss/, access on June 2008.
7. Nimbus Project [URL].http://workspace.globus.org/ clouds/nimbus.html/,access on June 2008.
8. Status Project [URL]. http://www.acis.ufl.edu/vws/, access on June 2008.
9. OpenNEbula Project [URL].http://www.opennebula.org /, access on Apr.2008.
10. G. Devi , M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.
11. Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.
12. Wayne Jansen ,Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication,NIST SP - 800- 144 ,80 pp., 2011.
13. G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud Computing: IT asa Service," IT Professional, vol. 11, pp. 10-13, Mar./Apr.2009.
14. Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2, pp.831-835, October 2012.

15. Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, pp.1922-1926, Jul-Aug 2013.
16. Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , "Cloud Computing System Based on Trusted Computing Platform", International Conference on Intelligent Computation Technology and Automation, Volume 1, pp.942-945, 2010.
17. Pearson, S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702, 2010.
18. Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, "Cloud Computing: A Perspective Study", New Generation Computing- Advances of Distributed Information Processing, Volume 28, pp.137-146, 2010.
19. Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume 169, pp.103-112, 2011.
20. Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal, pp.179-183, 2012.