ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

Cloud data Security using ECC and Searching of Cloud data using KNN Algorithm

R. Sridevi, R. Rahinipriyadharshini

Department of Computer Science, PSG College of Arts & Science, Coimbatore, Tamilnadu, India

Department of Computer Science, PSG College of Arts & Science, Coimbatore, Tamilnadu, India

ABSTRACT: Information security is the process of securing the private information in communication channel. Securing of private data and infrastructures becomes more crucial than ever. As Cloud Computing has become a boon for an IT industry nowadays. It is like a next stage platform in the evolution of Internet. It provides a platform with an enhanced and efficient way to store data in the cloud i.e. server with different range of capabilities and application. It provide an easy way of accessing one's personal file or data and use application without installing it on machines by just having Internet access. Example: Yahoo, Gmail, Amazon etc. are good cloud service providers. So all we need is to have Internet access then we can send mail and can access our account from any part of the world. The server and the email management software is installed on the cloud and managed by service providers. Providing an easy access to work and business still it has a major problem and threat i.e. "DATA SECURITY". Therefore Security, privacy and authentication is highly needed for transmitting data over the cloud. This can be achieved by using the cryptographic algorithms to protect the private information over the cloud. Symmetric and Asymmetric are the two types of algorithms that are used in cryptography for encrypting and decrypting the text. The information which are used on the internet is highly confidential and not for public viewing. So this work focuses on the providing data security in the cloud using Elliptic curve cryptographic algorithm for data protection where data or sensitive information is encrypted before it is launched in the cloud, thus ensuring data confidentiality and security. And also considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Retrieving of all the files having queried keyword will not be affordable in pay as peruse cloud paradigm. In this work with Elliptic curve cryptography we propose the multikeyword search with the highly efficient *k* nearest neighbour technique with coordinate matching, i.e., as many matches as possible to capture the relevance of data documents to the search query.

I. INTRODUCTION TO CRYPTOGRAPHY

Cryptography is the art of protecting information by transforming it into an unreadable format, called cipher text. Cryptography substitutes or transposes letters to create a coded message, traditionally called a cipher, which is used to transform a readable message called plaintext into an unreadable, scrambled, or hidden message called cipher text. Only someone with a decoding key can convert the cipher text back into its original plaintext. The originator of a coded message must share the decoding key in a secure manner with intended recipients who are authorized to know the contents of the coded message. If unauthorized parties can somehow intercept or figure out the decoding key, security is compromised because they can convert the cipher text into plaintext and read the contents of the message. Systems of cryptography also include techniques and mechanisms for verifying that originators of coded messages are authentic as well as ways to ensure that messages have not been altered en route. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. Within the context of any application-to-application communication, there are some specific security requirements including:

- Confidentiality.
- Authentication.
- Integrity.
- Non repudiation.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

A. Symmetric Cryptography

Symmetric key cryptography also referred to as conventional encryption or single key encryption were the receiver and the sender has to agree upon a single secret or shared key. The original message called plaintext and the key; encryption produces unintelligible data, which is about the same length as the plaintext was. Decryption is the reverse of encryption, and uses the same key as encryption. The symmetric encryption scheme has five ingredients.

Figure 1: Symmetric Encryption and Decryption

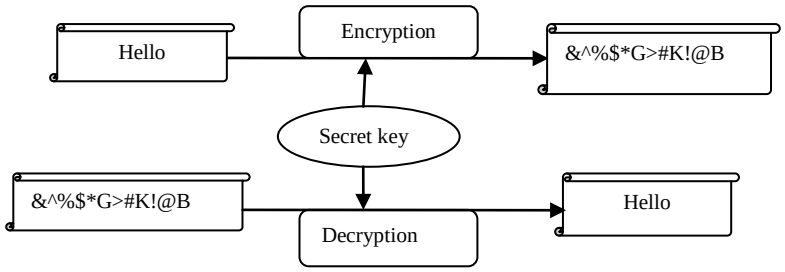

Figure 1**:** shows that the process of encryption and decryption in Symmetric cryptography.

B. Asymmetric Cryptography

Public-key cryptography is an asymmetric cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Figure 2: Encryption and Decryption in public cryptographic model

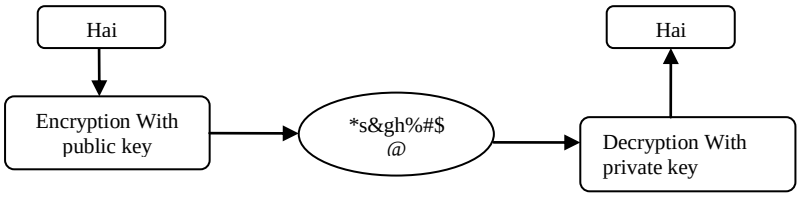

Figure 2**:** shows that the process of encryption and decryption in public cryptographic model

II. RELATED WORK

In "Data Security in Cloud Using Elliptic Curve Cryptography", the authors Puneetha, Dr. M Dakshayini et al discussed that Cloud Computing is a conceptual service based technology which is used by many organizations widely nowadays. As different types of normal data and also secret data are stored in the cloud, the client expects the cloud managing system to protect their data by providing security and maintaining secrecy. Data privacy protection and data retrieval control are the challenging issues to be addressed in cloud computing. Cloud system provides an innovative model for organizations to adopt IT services without upfront investment. Despite the gains achieved from cloud computing, the organizations hesitate in adopting Cloud due to security issues and challenges associated with it. Hence to address these issues, in this paper we propose a proficient data security model using ECC algorithm.

In "Enhancing Security in Cloud Storage using ECC Algorithm", the authors Ravi Gharshi, Suresha, discussed proposed a work towards providing security service such as confidentiality in the cloud services. And this was done by implementing Elliptic Curve Cryptography (ECC) algorithm instead of familiar and generalized RSA for data encryption because of its advantages in terms of smaller key sizes, lower CPU time and less memory usage and for enhancing the security in cloud storage.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

III. CRYPTOGRAPHY IN CLOUD COMPUTING

Information security is the process of securing the private information in communication channel. Securing data is a challenging issue in today's era. With the incredible growth of sensitive information on cloud, cloud security is getting more important than even before. The cloud data and services can be accessed anywhere. With the rapid growth of the cloud users disastrously happen with a growth in malicious activity in the cloud. Due to those malicious activities, every day, new security advisories are published in order to predict the more and more vulnerabilities which are discovered on the cloud for providing the security over the cloud network. This can be achieved by using the cryptographic algorithms to protect the private information over the cloud. Most of the data travel over the internet and it becomes difficult to make data secure.

IV. EXSISTING WORK

Securing the data on the cloud is one of the challenging tasks for the researchers. The different cryptographic algorithms are available to protect the data on the cloud. In the existing work AES symmetric algorithm has been used for encryption and decryption process before sharing or storing the data on the cloud. AES is a block cipher where encryption and decryption process performed on a block of data and the message is broken into block of bits. Block ciphers which operate on blocks of data where message is broken into blocks of bits. And single or Boolean key word search was used.search index has been build based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. A tree-based index structure and various adaption methods for multi-dimensional algorithm were used.

Drawback

- One time transactions where sender and the receiver repeatedly have to change the key at both sides and same Keyword search request is encrypted to different query vector.
- Execution time is slow, it is possible for the cloud server to link the same search request based on the same Similarity scores, and there is a possibility for the cloud server to leak the search pattern.
- Communicating parties must ideally share a different key.

V. PROPOSED WORK

In this paper, we propose an Elliptic curve cryptographic algorithm for data protection where data or sensitive information is encrypted before it is launched in to the cloud, thus ensuring data confidentiality and security. And also we choose the principle of coordinate matching, to identify the similarity between search query and data documents each document is linked with a binary vector as a sub index where each bit represents whether corresponding keyword is contained in the document. We proposed K nearest neighbour algorithm (KNN) to improve document retrieval accuracy by this the cloud server can easily sends back top-k documents that are most relevant to the search query. It reduces the network traffic while searching and avoid getting unwanted data on the cloud. The proposed system works by converting the strings into bits during the encryption process. The given string will be encrypted using Elliptic curve cryptography with the private key. After encryption is applied to the text is in unreadable form called cipher text. This cipher text will be in the form bits using public key encrypted text can be decrypted and finally gets the original text i.e. bits are converted into strings. Experimental result of proposed system provides better result when compare with the existing system.

Advantages

- High security is achieved.
- Secured data transformation is done.
- Valuable data retrieval, instead of returning undifferentiated results.
- Privacy should be achieved with low communication and computation overhead.
- Improves document retrieval accuracy.

VI. ELLIPTIC CURVE CRYPTOGRAPHY IN CLOUD COMPUTING

In this algorithm the file is encrypted by applying Elliptic curve cryptographic algorithm and private key set and public key set for privacy. The given string is converted into bits during the encryption process. Encrypted bits are decrypted with the public key to get the string. In this proposed algorithm security for data transmission is increased. This technique provides high security and confidentiality over data transformation in cloud..Hence ECC is better option than

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

AES, where lot of user connects to cloud based application with small session time like cloud based storage. Offered free of cost while for application like Amazon web service, Google app engine etc each user create sessions of long duration so overall difference will appear to be less. As the growth in computing power happens the requirement of strong key size will also grow. Cloud based application uses lot of thin and dumb client which has very less battery power, they might not be able handle such huge computations. In such scenario elliptic curve based cryptography will come more useful.

Figure 3: General Elliptic curve

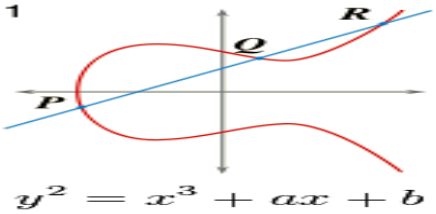

Figure 3: Represents the General Elliptic curve.

In order to improve the efficiency of the search k nearest neighbor is done by descending the tree to find the bucket containing the query point. The search for the knn is limited to the points within that bucket or those contained in the near buckets. Efficient k-nearest neighborhood search requires an efficient data structure which prevents from searching the entire dataset. The basic idea of our new algorithm is value of dmax is decreased keeping step with the ongoing exact evaluation of the object similarity distance for the candidates. At the end of the step by step refinement, dmax reaches the optimal query range Ed and prevents the method from producing more candidates than necessary thus fulfilling the r-optimality criterion.

Figure 4: ECC Key Generation Process

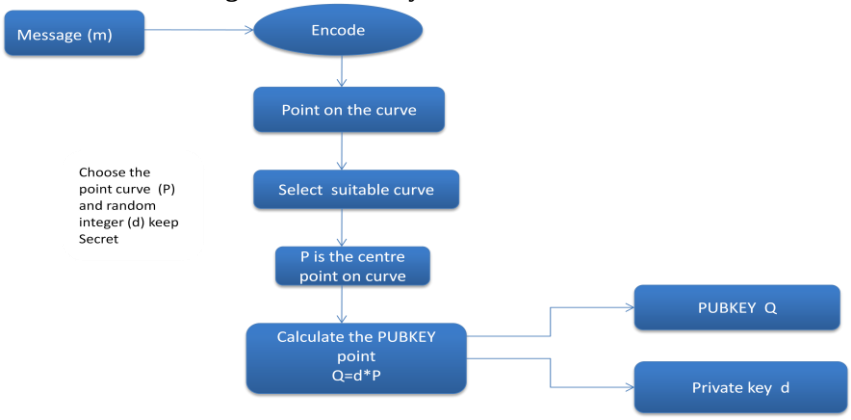

Figure 4: Shows the key generation process of ECC.

Figure 5: ECC Encryption Process

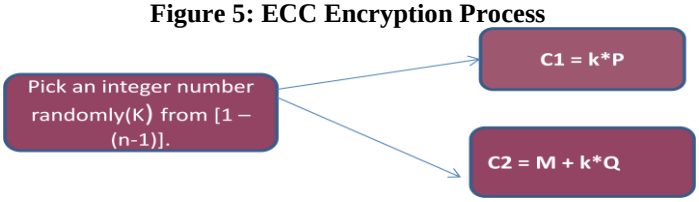

Figure 5: Shows the Encryption Process of ECC

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

Figure 6: ECC Decryption Process

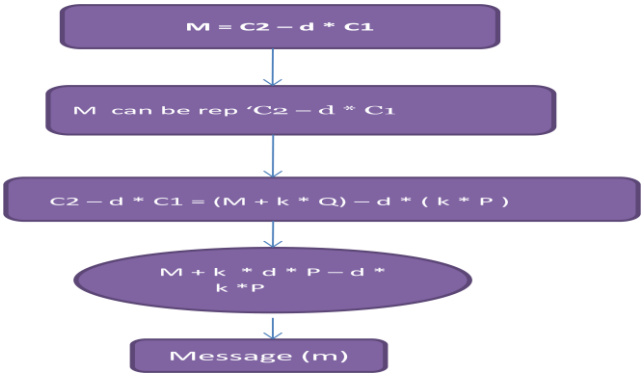

Figure 6: Shows the Decryption Process of ECC

A. Encryption Algorithm

1. Initialize the cipher Cipher. get Instance(algorithm name, provider name).
2. Initialize integrated encryption parameters.
3. Identify cipher with public, private key and specify the mode, parameters for encryption.
4. Choose the file for reading.
5. Encrypted cipher stream created.
6. Encrypt the file.
7. Write the encrypted data into output file.

B. Decryption Algorithm

1. Identifying the cipher with public key and specify the mode and parameters for encryption.
2. Choose the file for reading b
3. Decrypted cipher stream created.
4. Return the decrypted file.

C. KNN Algorithm

1. Initialize searching = index. increm- (F(q), df).
2. Initialize result = new sorted-list (key, object).
3. Initialize dmax = w.
4. While o = searching.getnext and d,(o, q) I d,,, do.
5. If do@, s> s dmax then result.insert (d,(o, q) , o).
6. If result.length 2 k then dmax = result[k].key.
7. Remove all entries from result where key > dmax.

VII. ANALYSIS OF RESULT

Table 1 Performance of AES and ECC algorithm.

Factors (Time in seconds)	AES	ECC
Key generation	0.08	0.03
Encryption	0.15	0.07
Decryption	0.06	0.02

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

Figure 7: Comparison chart of AES and ECC Algorithm

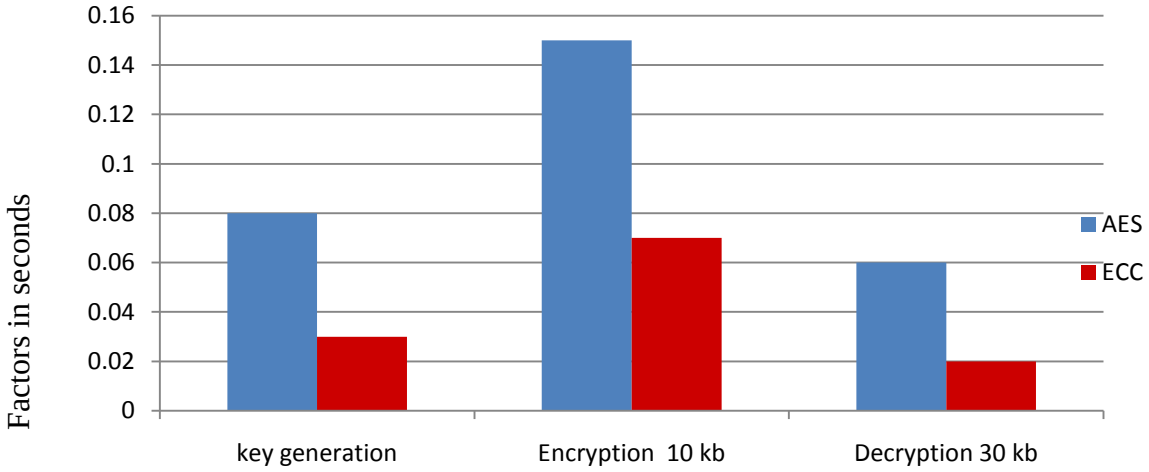

Figure 7: Comparison chart has been generate based on the performance of AES and ECC Algorithm

VIII. CONCLUSION

The present work proposes file encryption in cloud environment. Where the cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments, to address these concerns, transforming the data in cloud through ECC algorithm makes it more secure. Files can be uploaded in encrypted form and using the concept of keys file can be downloaded. Here, Security is based on the difficulty of computing discrete logarithm in a finite field, in which one encryption key, known as the private key, is kept secret, while another, known as a public key, is freely distributed. Public key cryptography is computationally more expensive than private key encryption, which employs a single, shared encryption key. Authentication, security, confidentiality, reliability can be easily achieved by implementing the elliptic curve cryptography in the cloud computing. We also used multikeyword search for searching the documents from the cloud.to meet the effective data retrieval need, instead of returning undifferentiated results data users to find the most relevant information quickly, rather than burdensomely sorting through every match in the content collection. We need to invest more effort and money to make elliptic curve cryptography more implementable and easier to understand.

IX. FUTURE ENHANCEMENT

Security is not a new issue and now it is recognized as one of the most complex problems like confidentiality, integrity, authentication, authorization. Proposed algorithm is designed to solve those problems. When compared to the existing algorithm the proposed Elliptic curve cryptographic algorithm provides solution for securing the information in cloud environment with improved and high performance in computing power as well as battery usage and can been implement in the applications of cloud computing. Future work will focuses on implementing of some other newly developed cryptographic algorithm for securing the data with tool.

REFERENCES

[1] Rashmi Nigoti, ManojJhuria, Dr.Shailendra Singh, A Survey of Cryptographic Algorithms for Cloud Computing, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), Madhya Pradesh,2010.
[2] K.S.Suresh, Prof K.V.Prasad, Security Issues and Security Algorithms in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Hyderabad, 10, October 2012 .
[3] Dr. L. Arockiam, S. Monikandan, Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
[4] Teng, P. Y., Huang, S. I., ―Multilevel Data Encryption & Decryption System and Method Thereof‖, Industrial Technology Research Institute, 2009.
[5] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader, Mohly Mohamed Hadhoud, Evalution the Performance of Symmetric Encryption Algorithms‖, international journal of network security vol.10,No.3,pp,216-222,May 2010.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829-837, April, 2011.
[7] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50-55, 2009.
[8] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, pp. 693-701, 2012.
[9] Veerraju Gampala. Data security in cloud computing with elliptic curve cryptography. International Journal of Soft Computing and Engineering (IJSCE), 2, 2012.
[10] Amit Sangroya. Towards analyzing data security risks in cloud computing environments. JULY/AUGUST 2010.
[11] Ashutosh Saxena Sravan Kumar R. Data integrity proofs in cloud storage. 2011.
[12] Vanya Diwan et al., "Cloud Security Solutions: Comparison among Various Cryptographic Algorithms" International journal of advanced research in computer science and software engineering (IJARCSSE), April 2014.
[13] Hashizume et al.,"An analysis of security issues for cloud computing", Journal of Internet Services and Applications (jisa), April2013.
[14] Rashmi, "A Survey of Cryptographic Algorithms for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Science (IJETCAS), May 2013.
[15] Hashizume et al.,"An analysis of security issues for cloud computing", Journal of Internet Services and Applications" (JISA), April 2013.
[16] Rashmi, "A Survey of Cryptographic Algorithms for Cloud Computing, International Journal of Emerging Technologies in Computational and Applied Science" (IJETCAS), May 2013.
[17] Abhishek Mohta et al, Ravi Kant Sahu and LK Awasthi, "Robust Data Security for Cloud while using Third Party Auditor" in International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE),Volume No. 2, Issue 2,Feb 2012.
[18] Dripto Chatterjee, et al "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" in International Conference on Communication Systems and Network Technologies (CSNT), June 2011.
[19] Douglas Selent, "Advanced encryption standard" Rivier academic journal, volume 6, number 2, 2010.
[20] Maulik P. Chaudhari and Sanjay R. Patel, "A Survey on Cryptography Algorithms", International Journal of Advanced Research in computer science and management studies (IJARCSMS),March 2014.
[21] Vishwa gupta et al., " Advance cryptography algorithm for improving data security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.
[22] AL.Jeeva et al., "Comparative Analysis of Performance Efficiency and Security Measures Of Some Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Volume. 2, Issue 3, May-Jun 2012.
[23] Mandeep Kaur et al., "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Volume. 2, 10 October 2012.
[24] Dhanraj, Nandini.C, and Mohd Tajuddin"An Enhanced Approch for Secret Key Algorithm baata Encryption Standard", International Journal of Research And Review in Computer Science, August 2011.
[25] Nadeem.A, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.
[26] Sridevi.R, Rahinipriyadharshini.R et al., "Secured transmission of data in cloud environment using Elliptic curve cryptographic algorithm" International Journal of Innovative Research In Computer and Communication Engineering (IJIRCCE), Vol. 3, Issue 8, August 2015.
[27] Sridevi.R,Rahinipriyadharshini.R et al., " A comparative study on the performance and the security of RSA and ECC algorithm" UGC sponsored National Conference On Advanced Networking and Applications (NCANA), 27th March 2015.
[28] Manikandan.G, Rajendran.P et al., "A Modified Cryptosystem Scheme for Enhancing Data Security", Journal of theoretical and Advanced Information Technology(JTAIT), Jan 2012, Conference on, vol., no.,pp.1-6, 23-27 May 2010.
[29] Chase, Melissa, et al., Sherman Chow. "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", ACM Conference on Computer and Communications Security 2009.