JES Journal of Engineering Sciences

Vol 11, Issue 5,May/ 2020
ISSN NO: 0377-9254

Secure data storage and access of data in cloud using Elliptic curve cryptography

Dr.G.Madhavi[1], J.Samatha[2]

[1]Assistant Professor, Department of CSE, UCEN JNTUK, Narasaropet, Andhra Pradesh, India

[2]Assistant Professor, Department of CSE, Matrusri Engineering College, Saidabad, Hyderabad, Telangana, India

Abstract:

The undeniably famous cloud computing worldview carries new chances to lessen equipment, upkeep and system costs related with the conventional framework required to offer enormous scope web based administrations or much littler restricted application and capacity arrangements. Nonetheless, with the dynamic versatility, diminished hazard and potential cost investment funds comes lost control that makes new difficulties for embracing cloud based framework. In this paper, we centre around data privacy protection which turns out to be progressively mind boggling with adaptable data sharing among a unique gathering of clients. It requires the mystery of redistributed data and a proficient sharing of decoding keys between various approved clients. For this reason, we, first, proposed another technique depending on the utilization of elliptic curve cryptography, where every customer goes about as a Private Key Generator. That is, he produces his own open components and determines his relating private key utilizing a mystery. Also, made contrasting of proposed diagram and notable security blueprint of RSA. Execution results shows that the proposed work out played out the proposed strategy.

Keywords: Cloud computing, security, RSA, Elliptic curve cryptography

1. Introduction:

In this Era of Technology, Cloud becomes the top most technology used by different industries and organizations due to its services and offerings. The research and analysis market [1] show that the services of cloud will rise day-by-day. The main advantage of the cloud is, it helps to reduce the cost of different services like software, infrastructure and platform cost. Due to this advantage a lot of enterprises started using cloud services for different purposes. It reduces the cost by improving utilization, reducing infrastructure and administration cost and fast services. Cloud Computing is one of the computing techniques which provides highly scalable resources through internet and provide services on demand of users and pay per use basis. Cloud provide different services in which Cloud Storage is one of the most used service. Now-a-days different applications like iCloud, Dropbox, Google Drive are used for storage and it changed the level of storage and improve the way of files stored [2]. Cloud Storage is the key infrastructure to achieve seamless information sharing and service interaction experience from different users, different applications, and different devices around the world using Internet. The use cloud is now-a-days similar to other public services like electricity, water that is available in anywhere and anytime. It provides highly flexible and high-performance service having high capacity and high security which solves the problems of number of users for storage like, low price, safety, high capacity and stability and due to this opted by many individuals and organizations as well.

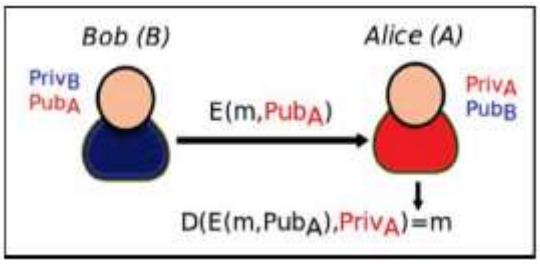

Fig-1: Secure communication between two parties using Elliptic curve cryptography

The services provided by cloud are based on five different attributes named as: Scalability, Elasticity, Multitenancy, self-provisioning of resources and pay as you go. It makes new advances in processors, disk storage, Virtualization innovation, broadband Internet association, and quick, economical servers have joined to make the cloud a more convincing arrangement. So as to give information stockpiling administrations,

distributed storage utilizes programming to interconnect and encourage cooperation between various sorts of capacity gadgets. Contrasted with conventional capacity strategies, distributed storage presents new difficulties in information security, dependability, and the executives. The general cloud architecture contains different network entities in the model [3] and these are (i) Users/Clients, (ii) Cloud Service Provider (CSP) and (iii) Third Party Auditor (TPA). Clients, who have information to be put away in the cloud and depend on the cloud for information calculation, comprise of both individual buyers and associations. A CSP, who has noteworthy assets and skill in structure and overseeing dispersed distributed storage servers, claims and works live Cloud Computing frameworks, TPA is a discretionary substance, who has ability and capacities that clients might not have, is trusted to survey and uncover danger of distributed storage benefits in the interest of the clients upon solicitation. In cloud information storage, a client stores his information through a CSP into different cloud servers, which are running in a concurrent, collaborated and disseminated way. Information excess/redundancy can be utilized with method of eradication remedying code to additionally endure issues or server crash as client's information develops in size and significance. From that point, for application purposes, the client associates with the cloud servers through CSP to get to or recover his information. As clients never again have their information locally, it is of basic significance to guarantee clients that their information is in effect effectively put away and kept up. That is, clients ought to be furnished with security implies so they can make consistent accuracy confirmation of their put away information even without the presence of nearby duplicates. This paper deals with the security mechanism that were used for providing security while storing data on cloud servers and proposed a novel approach for this. The next sections include literature work on security methods that were opted in cloud by different authors, next section deals with proposed elliptic curve based Secure Framework, its implementation on local cloud environment and performance analysis on the basis of time and size.

2. Literature work:

In 2011 Suli Wang et al. proposed technique for document encryption and unscrambling framework dependent on RSA calculation with littler sizes [4]. In 2012 Abbas Amini proposed framework for secure data in cloud computing. This proposition use RSA calculation for data respectability, and use AES calculation to accomplish classification of the put away data [5][25].

In 2014 Puneetha and M Dakshayini proposed data security model utilizing ECC calculation and hash work as advanced mark [6][24]. In 2014 Debajyoti Mukhopadhyay et al. proposed strategy for making sure about the data in clouds by executing key understanding, encryption and mark confirmation/age with hyperelliptic curve cryptography [7][23]. In 2014 Swarnalata Bollavarapu and Bharat Gupta proposed data security framework. This framework use calculations like RSA, ECC and RC4 for encryption and unscrambling strategies [8].

In 2006, Goyal et al. proposed a key-arrangement characteristic based encryption (KP-ABE) conspire [GPea06] that incorporated the entrance strategy with the client private key. That is, figure writings are named with sets of properties and private keys are related with get to structures that control which figure messages a client can decode.

KP-ABE plans guarantee adaptable and fine grained get to control. Actually, data are re-appropriated in a scrambled structure, while various clients are still permitted to unscramble various bits of data per security arrangement. This adequately dispenses with the need to depend on the capacity server for forestalling unapproved data get to. In any case, the burden of KP-ABE is that the entrance strategy is constructed onto one client private key. All things considered, the data proprietor can't pick who can unscramble the data with the exception of picking a lot of qualities which can depict the redistributed data. Furthermore, the sender must believe that the key-backer issues the proper keys to give or deny access to the fitting clients.

In 2007, Bettencourt et al. introduced the primary development of a figure content approach characteristic based encryption (CP-ABE) conspire [BSW07]. In their plan, the client mystery key is related with a lot of qualities, and the figure content is related with an entrance approach over traits. The client can decode the figure content if and just if the characteristic arrangement of his mystery key fulfills the entrance approach determined in the figure content.

[BSW07] is thoughtfully nearer to conventional access control strategies, for example, Role Based Access Control (RBAC). Characteristic based Cryptography (ABC) is alluded to as a creative idea and one of the most alluring approach to oversee and control record partaking in cloud, because of the calculation

properties on traits. Truth be told, customary access control models for the most part expect that remote servers putting away the data are completely trusted by their customers. So that, they are frequently answerable for characterizing and authorizing access control strategies.

Be that as it may, this announcement doesn't for the most part hold in multi-occupant cloud data stockpiling situations, particularly because of the theoretical idea of this plan of action. Thusly, cloud customers are as yet hesitant, while redistributing their data record substance. ABC is considered as a promotive arrangement, to guarantee fine grained get to control to data, which are redistributed on untrusted capacity servers.

To start with, ABC permits looking over encoded data. That is, the figure content is alloted with a lot of enlightening characteristics. In this manner, seeing these qualities as watchwords in such a framework drives a catchphrase put together inquiry with respect to scrambled data. Second, despite the fact that data are redistributed in a scrambled structure, each approved client is permitted to unscramble various bits of enciphered substance, because of the security arrangement remembered for the figure content and a necessary match with the decoding key of this successfully takes out the need to depend on the cloud stockpiling server for forestalling unapproved data get to.

RSA[10] is considered as the primary reality and handy hilter kilter key cryptosystem. It gets true standard for open key cryptography. Its security lies with number factorization issue. For solid security of data huge cryptographic keys (open key and private key) require. Enormous cryptographic keys are regularly viewed as excessively computationally costly for memory imperatives gadgets or little gadgets.

3. Proposed work:

Elliptic Curve Cryptography (ECC) was found in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an elective instrument for actualizing open key cryptography. ECC calculations depend on the logarithmic structure of elliptic curves over limited fields. Elliptic curves (EC) are cubic structures that are characterized over limited fields, for the most part a prime or a double field meant Fp or F2 p , where p and 2 p speak to the request for the field separately. By request, we mean the quantity of components of the limited field.The Proposed Algorithm includes the following steps:-

a. **Setup:** the **EC** do the following functions:

1. Chooses the curve **E** over $\mathbb{F}_{2^m}$ in the form where a and b are the curve parameters.
$y^2 + xy = x^3 + ax^2 + b$

2. Chooses the base point **P** in **E**($\mathbb{F}_{2^m}$) whose order **n** should be very Large.
3. Selects a random number smaller than the base point **P** order as a private number, this number will be a master private key **Mk**.

b. **Extract:** at the point when client needs to get his private and open key from PKG, he should send his personality (IDU) to PKG. At that point the PKG will figure the hash an incentive to the character of client (IDU) and use it with ace private key Mk to produce client private key, and utilize this private key to create client open key.

Q_U = H (IDU) Pr_U = Mk*Q_U PU_U = Pr_U*P

Then send copy from user private to user, and copy of user public key to user and TC.

c. **Encryption:** the user can encrypt his file by using the public key to generate his cipher text as follow:

1. The user encodes his file to points P_m.
2. The user encrypts his file as follows:

a. Selects a random integer number **J**.
b. Calculates the ciphertext C_m consists of the pair of points
C_m = {J*P, P_m + J*PU}
c. The user sends C_m to TC.

d. **Decryption:** When user want to retrieve his encrypted file C_m from TC, he will decrypted the message by computes:
P_m + J*PU – Pr(J*P)
P_m + J(Pr*P) – Pr(J*P) = P_m

Then he decodes P_m to get the original file **m**.

e. **Signing and Verifying:** The user must signing the file **m** by using his private key **Pr** as follows:
1. Calculate the hash value to the e=H(m) message
2. Chooses a random positive integer J in interval [1,n-1];
3. Calculate (x,y)=J*P
4. Calculate r= xmod n, if r=0 go to step-2
5. Calculate S=Inv(J)(e+Pr_a*r) mod n, if S=0 go to step-2
6. The file signature is the pair (r,S)
7. Send the signature (r,S) to TC

The TC when receive the user's file,it must verify the signature based on the public key **PU**$_U$ of user as follows:

1. Calculate e=H(m)
2. Calculate w= S^{-1} mod n
3. Calculate u1= e*w mod n and u2= r*w mod n
4. (x,y)= u1*p+ u2*PU, if (x,y)= infinite reject the signature

if v= x mod n and v=r

5. if then the signature is valid other vise invalid

4. Experiment results:

This paper implements ECC and RSA with sample data inputs of 8 bits, 64 bits, 256 bits using random private keys based on recommendation of NIST[1], [13]. The experiments are done on JAVA platform and used Intel Pentium dual-core processor (1.60 GHz, 533 MHz, 1 MB L2 cache) with 2GB DDR2 RAM under Ms-Windows platform. The efficiency of ECC over RSA.

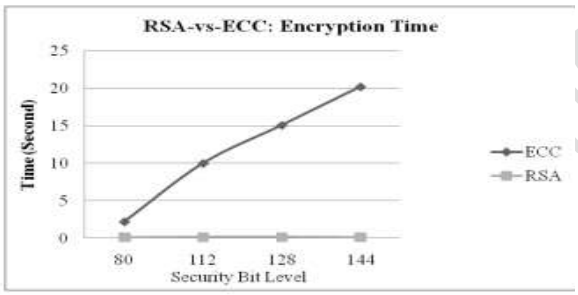

Fig-2: Encryption time with 64-bit key

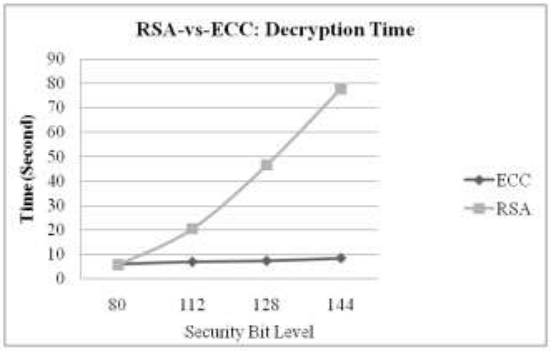

Fig-3: Decryption time with 64-bit key

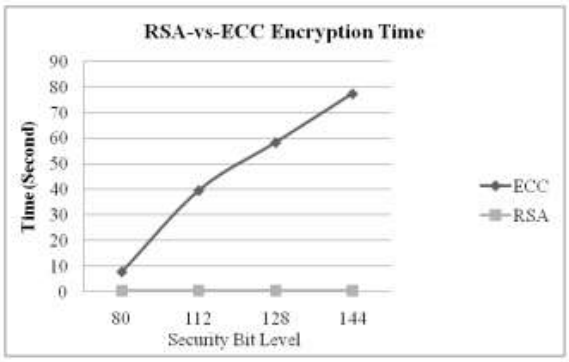

Fig-4: Encryption time with 256-bit key

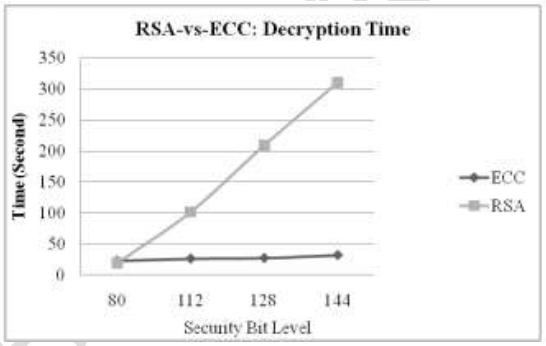

Fig-5: Decryption time with 256-bit key

5. Conclusion:

This paper propose a more flexible and effective scheme to address data storage security problems in cloud computing. Security of the data is very important while being transmitted from one user to cloud server, from cloud server to user or system. Security of data is provided by cryptographic technique. Symmetric-key cryptography is very good in providing security to the message but suffers with key distribution problem. In order to mitigate the key distribution problem and providing confidentiality and integrity of message, asymmetric-key cryptography was pioneered by Diffie-Hellmen[14]. This pa per analyses security strength of ECC and RSA over 2 sample input data of 64 bits, 256 bits with random keys based on NIST recommendation. This work demonstrates that ECC outperforms in terms of operational efficiency and security over RSA.

References:

[1] Jeffrey Voas and Jia Zhang. 2009. Cloud Computing: New Wine or Just a New Bottle?. Published by the IEEE Computer Society.
[2] Sameeh A. Jassim. 2013. Mediated IBC-Based Management System of Identity and Access in Cloud Computing. MSc thesis. College of Computer, University of Anbar.
[3] Salim A. Abbas and Amal A. Maryoosh. 2015. Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography. IOSR Journal of Computer Engineering, Volume 17, Issue 4, Ver. I.
[4] Suli Wang and Ganlai Liu. 2011. File encryption and decryption system based on RSA algorithm. International Conference Computational and Information Sciences (ICCIS).
[5] Abbas Amini. 2012. Secure Storage in Cloud Computing. MSc thesis. Department of Informatics and Mathematical Modelling (IMM), the Technical University of Denmark.
[6] Puneetha C. and M. Dakshayini. 2014. Data Security in Cloud Using Elliptic Curve Cryptography. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5.
[7] Debajyoti Mukhopadhyay et al, 2014. Securing the Data in Clouds with Hyperelliptic Curve Cryptography. Available at: http://arxiv.org/ftp/arxiv/papers/1411/1411.6771.pdf.
[8] Swarnalata Bollavarapu and Bharat Gupta. 2014. Data Security in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3
[9]. Sugang Ma, "A Review on Cloud Computing Development", JOURNAL OF NETWORKS, VOL. 7, NO. 2, FEBRUARY 2012.
[10]. SajjadHashemi, "DATA STORAGE SECURITY CHALLENGES IN CLOUD COMPUTING", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.
[11]. Victor Delgado, MSc thesis, "Exploring the limits of cloud computing", KungligaTekniskaHögskolan (KTH) Stockholm, Sweden, October 4, 2010.
[12]. UttamThakore, "Survey of Security Issues in Cloud Computing", College of Engineering, University of Florida, Available at: http://www.cise.ufl.edu/~sgchen/papers/Survey%20of%20Security%20Issues%20in%20Cloud%20Computing.pdf, Accessed Date: 14 January 2015.
[13]. Albert Caballero and et al, "Open Data Center Alliance:Data Security Framework Rev 1.0",Open Data Center Alliance, Inc. ALL RIGHTS RESERVED, 2013.
[14]. Marc Joye and Gregory Neven, "Identity Based cryptography", IOS Press, 2009.
[15]. JoonsangBaek et al, "A Survey of Identity-Based Cryptography", Australian Unix Users Group Annual Conference, 2004.
[16]. DivyaNalla and K.C.Reddy, "Signcryption scheme for Identity-based Cryptosystems", Mathematics of Computation, 2003.
[17]. Liang Yan, ChunmingRong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography", Springer-Verlag Berlin Heidelberg, 2009.
[18]. Ravi Gharshi and Suresha, "Enhancing Security in Cloud Storage using ECC Algorithm", International Journal of Science and Research (IJSR), Volume 2 Issue 7, July 2013.
[19]. Chester Rebeiro, M.Sc.thesis, "Architecture Explorations for Elliptic Curve Cryptography on FPGAS", Department of Computer Science and Engineering, Indian Institute of Technology, Madras, February 2009.
[20]. William Stallings, "Cryptography and Network Security",principles and practice 5th edition,Pearson Education, Inc., 2011.
[21]. Ali MakkiSagheer, MSc thesis, "Enhancement of Elliptic Curve Cryptography Methods",Computer Science, University of Technology, 2004.
[22]. Darrel Hankerson, Alfred Menezes and Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, 2004.
[23]. MajidKhabbazian, MSc thesis, "Software Elliptic Curve Cryptography",Department of Electrical and Computer Engineering, University of Victoria, 2004