IJCTA, 9(27), 2016, pp. 261-265
ISSN: 0974-5572

The Confidentiality of Security in Cloud Computing Using Proxy Re-Encryption

C. Linda Hepsiba* and J. G. R. Sathiaseelan**

ABSTRACT

A Cloud storage process, consisting of a storage server, gives storage services larger than the Internet. Storing information in a third party's cloud system makes severe anxiety over information privacy but they have a chance to retrieve the data from the cloud. The encryption algorithms are does not provide much confidentiality. General encryption techniques look after information authentication, but also boundary the functionality of the storage space system because a few operations are favored over encrypted data. Constructing a protected storage scheme that wires several functions is difficult when the storage space system is scattered and has no middle ability. In future, entry of proxy re-encryption (RSA is an algorithm used by encrypt and decrypt messages) technique and put together it with a decentralized removal code such that a protected circulated storage system is defined. ECC is used to generate the keys data confidentiality. ECC makes keys via the properties of the elliptic bend equation instead of the conventional functionality. The circulated storage system does not only consider safety and strong storage and recovery, but also lets a user ahead his information in the storage servers to one more user with no retrieving the information back. The major technical participation is that the proxy re-encryption technique supports encryption operations over encrypted text as well as forwarding actions over encryption and encrypted text. Here, the process fully combines encryption, encoding, and forwarding. To examine and use appropriate parameters for the text dispatched to storage servers and the storing servers accessed by a key server. The functionality allows extra flexible alteration between the number of storage servers and strength.

Keywords: Cloud Computing, Security, Confidentiality, Decentralized, Proxy Re-Encryption

1. INTRODUCTION

The Small and Medium Business (SMB) organizations are gradually more realizing that basically by patter into additional obscure they can expand quick contact to best industry applications or severely boost their communications possessions, all at small cost. Gartner defines cloud computing as ''a style of computing anywhere particularly scalable Information Technology are released as service to outside clients using Internet technologies''. Cloud providers at present benefit from a thoughtful occasion in the marketplace. The providers must guarantee that they get the safety aspects right, for they are the ones who will take on the task if belongings go wrong. The cloud offers a number of payback like fast consumption, payment use, Minimum costs, scalability, quick provisioning, quick elasticity, everywhere system access, greater resiliency, hypervisor security against system attacks, low-cost calamity recovery and data storage space solutions, on-demand protection controls, real time finding of system tampering and quick re-constitution of services. while the cloud offers these reward, until several of the difficulties are better understood, many of the main group of actors will be tempted to seize back. These challenges contain, but not narrow to ease of access vulnerabilities, illusions vulnerabilities, web application vulnerabilities such SQL (Structured Query Language) insertion and cross-site scripting, material contact issues, privacy and manage issues arising from

* Research Scholar, Department of Computer Science, Bishop Heber College (Autonomous), Tiruchirappalli, Tamilnadu, India, *Email: hepsi.linda@gmail.com*

** Head, Department of Computer Science, Bishop Heber College (Autonomous), Tiruchirappalli, Tamilnadu, India, *Email: jgrsathiaseelan@gmail.om*

third parties having physical control of data, issues related to identity and documentation organization, issues interconnected to information confirmation, tampering, reliability, privacy, data loss and stealing, issues linked to verification of the respondent machine Though cloud computing is under attack to give well again operation of funds using virtualization techniques and to obtain up a lot of the job load from the client, it is filled with safety risks.

2. RELATED WORK

Cloud computing allows delivering information knowledge power on order. Be it either the hosting of a convinced web request or the outsourcing of a whole server or data center by earnings of virtualization. Applying these techniques however goes along with handing over the final manage of statistics to a third party.

Gampala et al [1] focused on data security in cloud computing using Elliptic Curve Cryptography with Encryption and Digital Signature. Bhavana Sharma [2] explore Elliptic curve cryptography (ECC) technique for secure message non-repudiation of data, integrity, message authentication and data confidentiality, it also delivers several cryptographic algorithms like asymmetric and symmetric algorithms for data storage in cloud. Amounas et al [3] proposed the RSA algorithm and ECC algorithm for data confidentiality. Lo'ai Tawalbeh et al [4] focused on data security, privacy and suggested cryptographic algorithms are increasing the confidentiality level.

Alowolodu et al [5] has study to concentrate on Elliptic curve cryptography algorithm is used to create more efficient, smaller and faster cryptographic keys for progress of secure deployment and secured data or information in cloud. Peng Yong et al [6] deliver cryptographic methodologies such as identity-based encryption, XML encryption, broadcast encryption, attribute-based encryption, group signature, group encryption, searchable encryption and search authenticator, which are expended for data security in cloud. Dimitrios et al [7] provide solution for data confidentiality, integrity and authentication in cryptographic algorithms for cloud storage. Koorosh Goodarzi et al [8] focused on modern and classical cryptography algorithms for retaining confidentiality, integrity and availability in cloud data storage. Neha Mishra [9] concentrated on different types of cryptographic algorithms and data security threats for confidential data. Chandu et al [10] focused on RSA algorithm for data integrity in cloud data storage.

3. PROPOSED WORK

The enhanced conclusion of this paper is RSA and ECC perception. RSA is an algorithm used by current computers to encrypt and decrypt mail. It is an asymmetric cryptographic algorithm. Asymmetric algorithms that there are two different keys, this is also called community key cryptography; since one of them can be given to each individual the other key should be kept confidential. Elliptic curve cryptography (ECC) is a draw near to public key cryptography base on the algebraic structure of elliptic curves.

3.1. System setup

The algorithm SetUp(1) generates the arrangement parameters. A customer uses KeyGen to create his community and secret key pair and Share KeyGen to divide his secret key to a set of m key servers with a threshold t, where k < = t < = m. User's adjacent deliverances to the third constituent for key conversion.

3.2. Data storage

When user A desires to hoard a memo of k blocks m1, m2,. . .;mk with the identifier ID, he computes the uniqueness voucher and performs the encryption algorithm Enc k blocks to get k original cipher texts C1, C2, . . . ; Ck. An original cipher text is indicated by a foremost bit b ¼ 0. User A sends each code text Ci to v erratically selected storage servers. A storage server receives a set of novel symbols texts with the same self from A. When a cipher text Ci is not acknowledged, the storage server inserts Ci to the set. The singular format of is a mark for the absence of Ci. The storage attendant performs Encode on the set of k cipher texts and provisions the encoded result (code word symbol) Encryption. Encoding is main part in the data storeroom.

3.3. Data forwarding

User A requires forwarding a memo to a new user B. He requests the first constituent a1 of his furtive key. If A does not hold a1, he queries key servers for key shares. When at least t key servers respond, A recovers the first section a1 of the secret key SK_A via the Key Recover algorithm. Let the identifier of the meaning be ID. User A computes the re-encryption key $RK^{ID}_{A->B}$ via the Re KeyGen algorithm and steadily sends the re encryption key to each storeroom server. By using $RK^{ID}_{A->B}$ a storage server re-encrypts the unique password symbol C0with the identifier ID into a re-encrypted code word symbol C'' via the ReEnc Þ algorithm such that C'' is decrypt clever by using B's secret key. A re-encrypted code word sign is indicated by the foremost bit b ¼ 1. Let the public key PK_B of user B be (g^{b1}; h^{b2}).

3.4. Data retrieval

There are two cases for the data recovery stage. The first container is that a user A retrieves his own communication. When user A needs to recover the significance with the identifier ID, informs all key servers with the identity token A key server first retrieves unique key cryptogram from user A arbitrarily chosen storeroom servers and then performs partial decryption split Dec on each retrieved unique password character C0. The result of partial decryption is called a partially decrypted code word symbol. The key server sends the somewhat decrypted code word symbols and the coefficients to user A. After customer A collect replies from at least t key servers and at smallest quantity k of them are originally from distinct storage servers, executes unite on the t somewhat decrypted code word symbols to recover the blocks m1; m2; . . .; mk. The next case is that a user B retrieves a communication forwarded to him. User B informs all key servers directly. The gathering and combining parts are equal as the first case except that key servers retrieve re-encrypted code word symbols and perform fractional decryption Share-Decrypted on re-encrypted code word symbols.

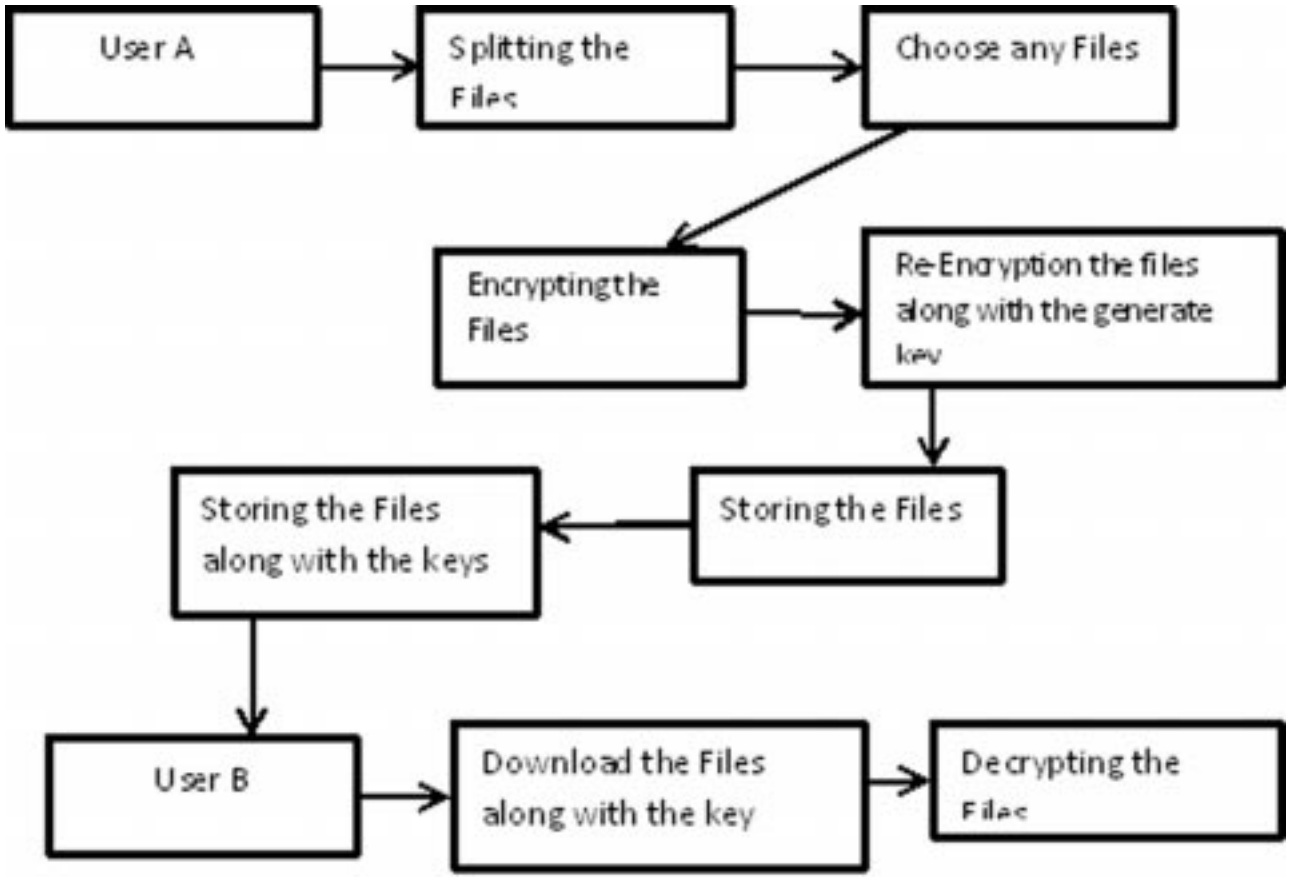

Figure 1: Architecture of Proxy Re-Encryption

4. EXPERIMENTAL RESULTS

4.1. Decentralized erasure code

In the decentralized removal code is a cutting code that separately computes each password sign for a communication. Thus, the encoding procedure for significance can be split into an analogous task of generating code word symbols. A decentralized erasure code is suitable for use in a disseminated storage scheme. After the message symbols are sent to storeroom servers, each storage server alone computes a code word symbol for the received message symbols and stores it. This finishes the programming and storing procedure. The recovery process is the same.

4.2. Proxy re-encryption

In a proxy re-encryption scheme, a substitute server can relocate a cipher text under a public key PKA to a new one beneath an additional public key PK_B by using the re-encryption key $RK_{A->B}$. The server does not know the plaintext through alteration. In planned some proxy re-encryption schemes and functional them to the allocation occupation of sheltered storage systems. In their work, letters are first encrypted by the owner and then stored in a storage attendant. When a user requests to divide his post, sends a re-encryption key to the storage server. The storage server re-encrypts the encrypted messages for the official user. Thus, their system has data discretion and supports the data forwarding purpose. In this work, additional integrates encryption, re-encryption, and encoding.

4.3. Data storage phase

In the data storage stage, user A encrypts his communication M and dispatches it to storage servers. A message M is decaying addicted to k blocks m1;m2; . . .;mk and has an identifier ID. User A encrypts each block mi into a cipher text Ci and sends it to v erratically select storage servers. Upon receiving cipher texts from a user, each storage server linearly combines them with arbitrarily selected coefficients into a secret word symbol and stores it. Note that a storage server may receive less than k meaning blocks and to assume that all storage servers know the worth k in progress.

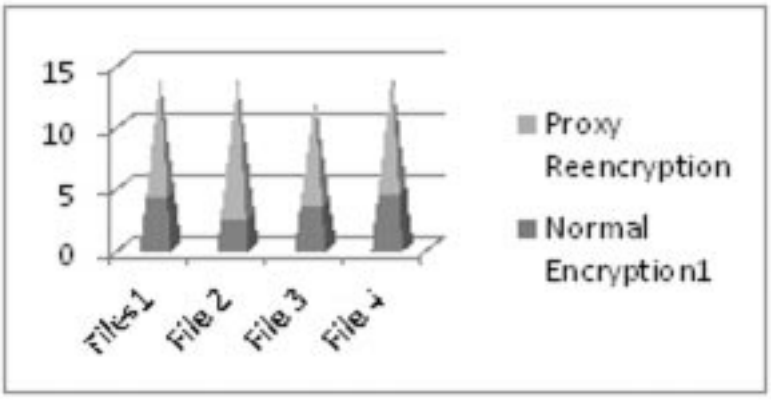

Figure 2: Performance of Proxy Re-Encryption

◊◊E{◊GD◊◊◊◊◊2◊◊◊A◊◊◊◊VI◊◊◊◊◊w
◊
◊WZ◊◊etM~
/◊◊i1L◊”◊uu◊◊

Figure 3: Encrypted File along with The key

rvnaveen
rvnaveen2594@gmail.com
concept-conference

Figure 4: Decryption File format .fcfd from

5. CONCLUSION

In a cloud-based system, there are yet many problems which have to be solved. Cloud computing is a difficult tools with reflective implications not only for Internet services but also for the Information Technology sector as a whole. Still, some issues continue living, mostly related to service-level agreements (SLA), safety and time alone, and power effectiveness. As described, currently protection has lot of loose ends which scares away a lot of prospective users. In anticipation of a proper safety part is not in position, possible users will not be capable to power the reward of this technology. This safety part should supply to all the issues arising from all information of the cloud. Each part in the cloud must be analyzed at the worldwide and micro level and an incorporated result must be considered and deployed in the cloud to attract and captivate the possible consumers. Until then, cloud background will stay cloudy.

REFERENCES

[1] Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi. "Data security in Cloud Computing with Elliptic Curve Cryptography," *International Journal of soft Computing and Engineering,* **2(3),** 2012.

[2] M.Bhavana Sharma. "Security Architecture of Cloud Computing based on Elliptic Curve Cryptography(ECC)," *International Journal of Advances in Engineering Sciences*, **3(3)**, 2013.

[3] F.Amounas and E.H.El Kinani."ECC Encryption and Decryption with a Data Sequence,"*Applied Mathematical Sciences*,**6**,2012.

[4] Lo'ai Tawalbeh1, , Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari1. "A Secure Cloud Computing Model based on Data Classification," *First International Workshop on Mobile Cloud Computing Systems, Management, and Security*, 115, 2015.

[5] Alowolodu O.D , Alese B.K, Adetunmbi A.O., Adewale O.S and Ogundele O.S. "Elliptic Curve Cryptography for Securing Cloud Computing Applications," *International Journal of Computer Applications,* 2013.

[6] PENG Yong, ZHAO Wei, DAI Zhong-hua and CHEN Dong-qing," Secure cloud storage based on cryptographic techniques," *The Journal of China Universities of Posts and Telecommunications*,**(11),**182-189, 2012.

[7] Dimitrios Zissis and Dimitrios Lekkas. "Addressing Cloud Computing Security Issues," 583-592, 2012.

[8] Koorosh Goodarzi and Abbas karimi. "Cloud Computing Security by Integrating Classical Encryption, ".*International Conference on Robert PRIDE,*320-326, 2014.

[9] Neha Mishra, Shahid Siddiqui and Jitesh P.Tripathi. "A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues," *BVICAM's International Journal of Information Technology* ,**7**, 2015.

[10] Chandu Vaidya and Prashant Khobragade. "Data Security in Cloud Computing," *International Journal on Research and Innovation Trends in Computing and Communication,* **3**,167-170, 2015.

[11] A.P. Bhutada and S.L.Magar. "Executing DES Algorithm in Cloud Data Protection," *International Journal of Innovative Research in Engineering and Technology.Leiutis,* **1(1).** 2015.

[12] Shivali munjal and Ramandeep singh. " Data Security in Cloud Computing," *IJSER*, **5 (3),** 2014.

[13] SaraswatVijay.ReportontheProgrammingLanguageX10,x10-lang.org,2010 /http://dist.codehaus.org/x10/documentation/languagespec/x10-latest.pdfS[accessed on:17June2010].

[14] Kaufman LM. "Data security in the world of cloud computing, security and privacy," *IEEE* **,7(4)**:61–4, 2009.

[15] Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L et al. "The CLOUDME Open-Source Cloud-Computing System," *Proceedings of the 2009 ninth IEEE/ACM international symposium on cluster computing and the grid,* 124–31, 2009.

[16] Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al. "Security guidance for critical areas of focus in cloud computing," *Cloud Security Alliance*, **2(1)**. 25, 2009.

[17] M.Mohamed Sirajudeen and Dr. K. Subramanian, "Security Issues on Data Transfer under Clouds – An Overview," *International Journal of Information Technology Infrastructure.* **3(5),** 2014.

[18] M. Sugumaran ,BalaMurugans D. Kamalraj. "An Architecture for Data Security in Cloud Computing," *World Congress on Computing and Communication Technologies.* 2014

[19] M.Ali, S.U.Khan and A.V.Vasilakos. "Security in Cloud Computing: Opportunities and Challenges," *Information Science,* 2015.

[20] Gopinath.v and Bhuvaneswaran R.S. "Study on Secure Cloud Computing with Elliptic Curve Cryptography," *International Journal of Computer Science Issues*, **11(5),** 2014.