Middle-East Journal of Scientific Research 23 (2): 223-230, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.02.22106

An Approach for Enhancing Secure Cloud Storage Using Vertical Partitioning Algorithm

[1]*S. Subbiah,* [2]*S. Selva Muthukumaran and* [2]*T. Ramkumar*

[1]PRIST University, Thanjavur, Tamil Nadu, India
[2]Department of Computer Applications, A.V.C. College of Engineering,
Mayiladuthurai, Tamil Nadu, India

Abstract: Cloud computing plays a vital role in the field of distributed computing. The main objective of the cloud computing is to make use of resources effectively in order to reduce the cost of an enterprise. Cloud users face difficulties while they are posting and managing data over cloud environment. Since the posted data is being with the service provider's premises, confidentiality of data and associated issues emerge as a major threat for the data owners. The paper focuses the above issue in a federated cloud environment and presents an algorithm called, vertical partitioning algorithm to protect the data in an efficient manner. The algorithm has been implemented in a java platform and results are compared with the other algorithms and the results shown the efficiency too.

Key words: Cloud Computing · Vertical Partitioning · Cloud security · Service provisioning

INTRODUCTION

Cloud computing is a model for enabling expedient, on demand network make contact with to a shared pool of configurable computing property that can be quickly provisioned and unlimited with minimal organization attempt or service provider communication [1]. It reduces the capital expenses and operational expenditure implicated in the IT Infrastructure of an organization.

Cloud computing has some attributes that are shared, standard service, solution-packaged, self-service, elastic scaling and usage-based pricing. Cloud has three different service models. They are (i) Software as a Service (SaaS) which uses provider's purpose over a network. Instead of purchasing the software, cloud user rents the software for use on a compensate per use representation. (ii) Platform as a Service (PaaS):- It deploys customer applications in cloud. The Cloud contributor gives an atmosphere to application developers, who develop applications and offer those services through the provider's platform. (iii)Infrastructure as a Service (IaaS):- It deals with rent dispensation, storage and network capability. The basic suggestion is to offer the computing services resembling processing power, disk space etc. based on the practice.

The Cloud computing can be deployed in four dissimilar models specifically, (i) Private Cloud-Enterprise owned or leased, (ii) Public Cloud- Sold to the public, mega scale infrastructure, (iii) Hybrid cloud-The arrangement of two or more cloud types, (iv) Community Cloud-shared infrastructure for specific community [2].

The Cloud user's data is stored in the cloud provider's data centers, where we can have the security issues like discretion and Integrity of Information, Accessibility of Information, Repudiation of Information, Shared Platform Issues, Service hijacking, Loss of control and Security Issues [3]. The loss of data security will create loss of data integrity due to third party access, which is the main issue, affects the user's beliefs. This manuscript concentrates on security issues in cloud computing storage and proposing a new algorithm to protect the user's data in the cloud storage. The rest of the paper is prepared as follows: Section II introduces the various security issues. The proposed system's architecture is described in Section III. Section IV describes the related work. The implementation of new algorithm to ensure security to the cloud users is discussed in Section V and finally Section VI concludes the survey.

Corresponding Author: T. Ramkumar, Department of Computer Applications,
A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu, India.

Security Issues and Challenges: The communication among cloud server and cloud user is not fully secured. Because, the cloud user's data will be stored the in the cloud provider and there may chance for theft of data by the third party. There are many physical locations available throughout the world. Many organizations are not comfortable to store their data away from their organizations. Storing data in diverse data centers in dissimilar locations, may lead to unconstitutional access and uses. Proper declaration is not given by the cloud providers for the intelligibility of data. There are numerous security issues which gives trouble for both cloud provider and consumers. The following are the security challenges existing in the cloud computing [18].

Confidentiality, Integrity and Availability of Information: Confidentiality refers to only certified parties or systems having the capability to access confined data. The threat of data negotiation increases in the cloud, due to the augmented number of parties, strategy and applications involved, that leads to an increase in the number of points of access. Reliability means that property can be customized only by approved parties or in authorized traditions and refers to information, software and hardware. Data reliability refers to defending data from unconstitutional deletion, adjustment or production. Data accessibility is a term used by some computer storage manufacturers and storage service providers (SSPs) to explain products and services that ensure that data continues to be accessible at a necessary level of presentation in situations ranging from normal throughout devastating [4].

Repudiation, Service Hijacking and Loss of Control: Systems must make sure that a party cannot consequently not accept (reject) an operation. To defend and guarantee digital conviction, the parties to such systems may utilize Digital Signatures, which will not only authorize the correspondent, but will also, 'time stamp' the contract, so it cannot be claimed consequently that the operation was not sanctioned or not valid etc. Session hijacking occurs when the attacker steals the user's session id to gain unconstitutional access for the information or services residing on a computer system. Most customers are aware of the danger of letting data control out of their hands and storing data with an outside cloud computing provider. Data could be compromised by the cloud computing provider itself or other aggressive enterprises which are customers with the equivalent cloud computing provider. There is a lack of simplicity for customers on how, when, why and where their data is processed. This is in opposition to the data protection obligation that customers know what happens with their data [5, 6, 16].

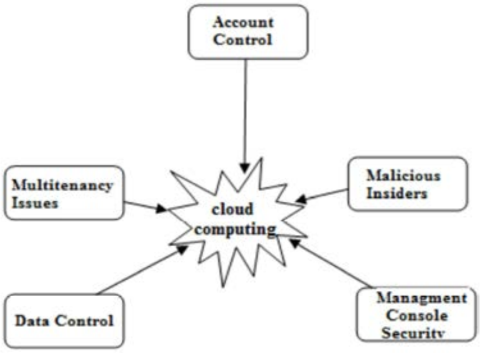

Fig. 1: Categorization of Threats [14]

Security Standards for Cloud: Here are seven of the detailed safety issues Gartner says customers should increase with vendors before selecting a confuse vendor. Gartner programmed few issues associated with cloud like advantaged user contact, Authoritarian compliance, Data position, Data Segregation, Recovery, Exploratory Support and Lon-term capability [19, 20].

Dimitrios Zissis *et al*. categorized the various types of threats in cloud computing environment. They are, (i) Account Control(ii)Malicious Insiders(iii) Management Console security(iv) Data Control (v) Multitenancy Issues[14]. These issues are also play vital role in the cloud storage environment.

Related Work: To secure the cloud storage, five layers approach proposed by Bashir Alam *et al*. There are five layers namely, the External Layer, Conceptual Middle Layer, Conceptual Layer, Physical Middleware Layer and Physical Layer. The main function of the service provider is to supervise and supply the services with full transparency and security. The conceptual level heterogeneity amongst dissimilar databases like SQL, DB2, Oracle etc. This coating represents the logical structure of the complete database and deals with the domestic processing on data. This layer provides the capability of defeat the heterogeneity across the dissimilar platforms like windows, Mac OS, Linux etc. This layer represents the physical representation of the data. In a cloud database service, the backend is creature overseen by a Physical layer that's dependable for the continuous monitoring and configuring of the record to accomplish optimal scaling, high accessibility and multi-tenancy and efficient reserve distribution in the cloud [21].

Xinyu Leit *et al*. proposed Model which has some transformations on the Matrix Multiplication Computation (MMC) to get an encrypted MMC problem which is sent to the cloud and then transforming the outcome returned from the cloud to get the accurate result to the innovative MMC difficulty. Subsequently a randomized Monte Carlo confirmation algorithm with one-sided error is introduced to productively handle result authentication. In this paper they are suggesting protocol which ensures correct, secure and robust cheating resistant [7].

Security threats faced by cloud information storage can come beginning two different sources. On the one hand, a CSP can be self-interested, untrusted and probably malevolent. Not only does it yearning to move data that has not been or is infrequently accessed to a lesser tier of storage than decided for economic reasons, but it may also effort to hide a data loss occurrence due to organization errors, Byzantine failures and so on. On the other hand, there may also exist an reasonably aggravated opponent, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period. Two types of adversary proposed viz weak and strong. Weak Adversary: The challenger is concerned in corrupting the user's data files stored on personality servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its personal fraudulent data to thwart the unique data from being retrieved by the consumer. Strong Adversary: This is the nastiest case situation, in which we presume that the challenger can negotiation all the storage servers so that he can calculatedly adjust the data files as long as they are within dependable. In fact, this is correspondent to the case where all servers are colluding mutually to hide a data loss or altered form occurrence. To accomplish the storage accuracy, Fast localization of data error, energetic data support, dependability and light weight, there are three algorithms developed. Token pre computation, Correctness verification and Error Localization and Error Recovery algorithms are used to ensure the data security in the cloud [8].

For a security over cloud environment, this paper gives the idea, which followed by banking sector. Here, rules are framed and to be followed for the customer successful transactions. They are (i). All the cards only should be active through internet banking and transactions should be via the IP range of the company. (ii) Some accounts necessitate having a phone numeral to call and text message verification. If the substantiation is not received contained by a certain period of time, the contract will be cancelled; (iii) Transactions necessity be approved by a fax or an e-mail. Otherwise, after a confident period of time, the reverse operation is generated by the system and the first contract will be cancelled; (iv) transaction tracking codes will be sent throughout a channel. One or more receiver numbers can be used to substantiate the transactions. Based on these considerations, in the next segment a security explanation for card transactions is projected [9].

Mark D.Ryan proposed three types security in cloud computing viz. (i) Homomorphism encryption- it is an encryption technique that allows a part that holds cipher texts to perform certain operations on the cipher texts, which mirror the corresponding operations on the plaintexts. In the case of simple homomorphism encryption, there is just one operation on the plain text that has a corresponding operation on the cipher text.(ii) Key translation in the browser- With this approach, data is encrypted before being uploaded to the cloud and the data owners retain the keys. However, dissimilar parts of the data may be encrypted with unusual keys and some of the clients participating in the service may execute "key translation" in order to agree to data items to be forwarded to planned recipients.(iii)Hardware-anchored Security – to achieve confidentiality from the cloud provider is based on special hardware on the cloud side. The idea is that the cloud provider is able to decrypt the data, but is able to offer guarantees about the circumstances in which it does that. Those guarantees will promise that the data owners that the data is handled in agreement with their policy [10].

Mehmet Yilidiz *et al*. proposed a dynamic security model for cloud security. This model is based on eight aspects and includes four layers. Network, Storage, Servers and Application layers. It includes one enterprise level principles at the highest level and a system management aspect. It also includes two kinds of dynamic security types: horizontal and vertical. The horizontal type is specific to each layer end to end. Here, horizontal dynamic security policy for storage does only cover the security objects related to storage. The vertical type is designed to cover the interfaces between layers. Some security objects between servers and storage may be partially belonging to each layer. The vertical dynamic policies ensure that any common object or exception is covered [11].

The EU's Data defense instruction (95/46/EC) gives consumers certain basic rights with reverence to their personal data while requiring "data controllers" to go behind rules and limitations with deference to their data dispensation operations. Consumers are permitted to notice of the characteristics of any data controller and the purposes for which their private data are being together and otherwise processed. This Directive requires data controllers to pursue eight core ideology of data isolation protection that define the individual rights of consumers and the responsibilities of data controllers that process personal data. These data processing rights and responsibilities concern to the dispensation of personal data by companies regardless of the context and should be implicit to apply to cloud-computing systems. In the EU, businesses may not assemble, store, use or disclose consumers' private data unless they observe with the Data Protection Directive and any more thorough regulations that have been adopted in the associate States' laws. This means private data may only be collected and processed for particular, unambiguous and legitimate purposes and may not be processed unpredictably with those purposes (legitimacy and finality). The data question must be fully conversant on the details of the dispensation, counting who has access to the data, how it is stored and how the focus can review it (transparency). Personal data must be sufficient, relevant and not unnecessary in relation to the purposes for which it is composed and further processed (proportionality). Supplementary, businesses are required to provide enough security for consumers' personal data to avoid unauthorized contact to the data [12].

Sandeep K. Sood proposed construction has been structured to make available complete protection to the data throughout the complete process of cloud computing, be it in cloud or in transfer. Consequently multiple mechanisms and accessible techniques are applied to protect the critical information from unauthorized parties. The planned frame work is separated into two phases. First phase deals with procedure of transmitting and storing data securely addicted to the cloud. Second phase deals with the recovery of data from cloud and presentation the generation of requests for data contact, double confirmation, authentication of digital signature and reliability, thereby providing approved user with data on passing all security mechanisms [13].

Another secure model and protocol that will enable data sharing amongst a group of users specified by the data owner. These techniques implemented in health monitoring systems and are not limited in any way to medical applications and can be applied to other Cloud applications. For secure transmission of data ElGamal encryption and Proxy re-encryption [15].

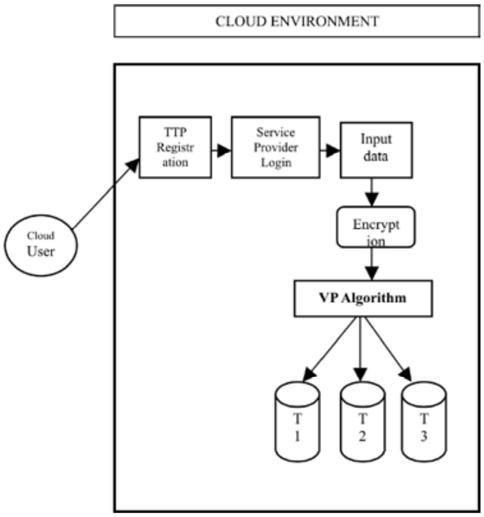

Fig. 2: Secured Cloud Storage using VP Algorithm

An incorporated approach to secured clouds h to an integrated secure cloud platform to facilitate aims to embody all of the above ideology. The first step is to identify the threats and necessities of Critical Infrastructures. This infrastructure generally focus on Hacking attacks, DDoS attacks, Insider attacks, Equipment failures, End –to –end issues,espionage and data loss or corruption [17].

Nancy *et al.* gives the recommendations regarding the reform in EU and US regulations on customer sensitive data. The reforms include (i) expanding the legal definitions of sensitive data that deserve heightened data protection (ii) reducing regulatory constraints that currently limit EU and U.S businesses from taking full advantage of the benefits of cloud computing [22].

Architecture of Proposed Work

Proposed Using Vertical Partitioning: In our proposed system, we are introducing a new algorithm which will give the high end security for the cloud user's data. The following Fig.2 shows the architecture of the proposed system. In this architecture we have different components like, Trusted Third Party Registration, Secured login in mechanism, Encryption of input data and Vertical Portioning Algorithm. In this cloud architecture, the user registers his profile with the trusted third party. The trusted third party verifies the users profile and allowing entering into the service provider. In this service provider by giving the login details the user can able to upload the data to the cloud as well as retrieve the data from the cloud. The end result of algorithm will be stored in cloud provider. In this proposed architecture high end security will be achieved when upload the user's input to the cloud provider. If the user wants to retrieve the data, then the data available in the different databases are integrated, decrypted and shown to the cloud users. In this architecture, we have shown only the storage of data in the cloud.This architecture assures that no third party will access cloud users data.

Algorithmic Implementation of Proposed Work: The above problem is implemented in the java platform and the results obtained are discussed below. The username and password is validated through login screen. Next, the user has to select the input data for the encryption using RSA and Elliptic Cryptography. The Encrypted data is splited using vertical partitioning and placed in the different tables. When retrieving the data, the encrypted data is collected from the different tables and given to decryption mechanism. The following algorithm is implemented and tested in java platform.

A user of RSA creates and then publishes a public key based on the two large prime numbers, all along with a supplementary value. The prime numbers must be kept covert. Anyone can use the public key to encrypt a message, but with presently published methods, if the public key is large adequate, only someone with information of the prime factors can possibly decode the communication [23].

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ (n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of m = 2 is c = 2^7 % 33 = 29
- The decryption of c = 29 is m = 29^3 % 33 = 2

Elliptic curve cryptography (ECC) is an advance to public-key cryptography based on the arithmetical structure of elliptic curves over finite fields. NIST suggested fifteen elliptic curves. Specifically, FIPS 186-3 has ten recommended finite fields:

- Five prime fields F_P for definite primes p of sizes 192, 224, 256, 384 and 521[25] bits. For each of the prime fields, one elliptic curve is suggested.
- Five binary fields F_2^m for m equal 163, 233, 283, 409 and 571. For each of the binary fields, one elliptic curve and one Koblitz curve was preferred.

The NIST recommendation thus contains a total of five prime curves and ten binary curves. The curves were apparently selected for optimal security and accomplishment effectiveness [18].

Algorithm:

Step 1: Creation of validation

TTP Registration→ Service provider Login

Step 2: Read the input file

r= {a_1, a2, a3…a_n}

Step 3: Encryption Algorithm

r = {cipher (a_1, a2, a3…a_n)} using RSA or
r = {cipher (a_1, a2, a3…a_n)} using ECC

Step 4: Vertical Partioning Algorithm

r=r_1+r_2+r_3…r_n

Step 5: Decryption Algorithm

r= {plain (r_1, r2, r2…r_n)} using RSA
Or
r= {cipher (a_1, a2, a3…a_n)} using ECC

In our proposed system, the user will register his details with the trusted third party (TTP) for secured login in the service provider. After successful registration he has keys through RSA or ECC algorithm for his data storage or retrieval. Through these keys, he has sent the request to the service provider. The service provider verifying the details and ask for the options like storage or retrieval. If the user wants to store the input data is divided into n number of attributes and the attributes will be stored in the different databases by using Vertical Partioning algorithm. In other case, for retrieval the data from the various databases are integrated through vertical partitioning and decrypted either by RSA or ECC. The Vertical Partioning algorithm is explained as follows.

Consider a relation r= {a1, a2, a3…a_n}, which is going give as input data given by the cloud user. The given table has attributes a1, a2, a3…etc. .These attributes are divided and perform the vertical Partioning. For each and every vertical partitioning is done using randomized model. It can be divided into required number of Partioning. Each splitting is stored in different cloud servers. Before storing it into a cloud server it checks for the already stored data on the servers, if the fields are same (already existing and new one) then the splited column will be moved to another cloud database. Then the splitted file will be uploaded into the different cloud servers. If a user wants to down the load the file, then he has to get the two types of keys. One is the trusted third party key and another one is one time password. Then the user has to tell the required fields to the third party auditor. It will pass the field values to each and every cloud server. Then data will be given to the requested server. There will be a stored accountability will be maintained in the trusted third party. And the accountability will be intimated to the owner of the data. Stop the process.

RESULTS AND DISCUSSION

The above mechanism implemented successfully and the results are verified with existing and end results are verified with the previous systems. In this mechanism, one input file in the size of 100 kb given to the systems and uploaded by using the RSA and ECC Algorithms. The encrypted data is stored in the different databases by using the Vertical Partitioning Algorithm. While retrieving the uploaded data by these two different algorithms, the execution time is calculated.

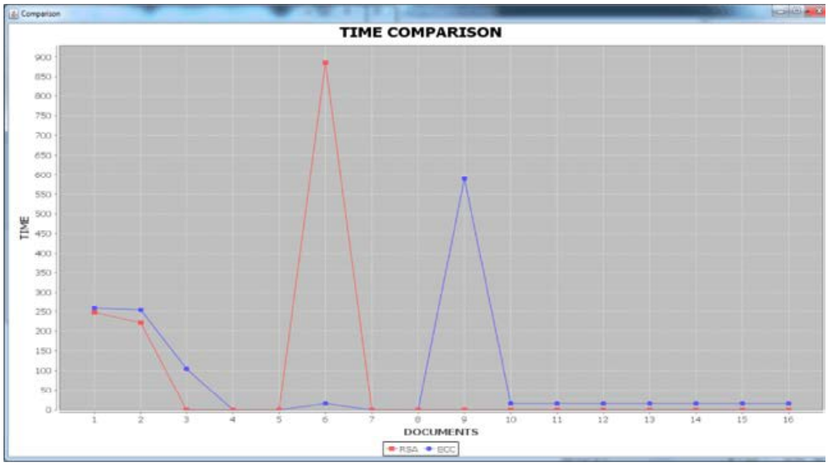

Fig. 3: Time Comparison of RSA and ECC while input upload

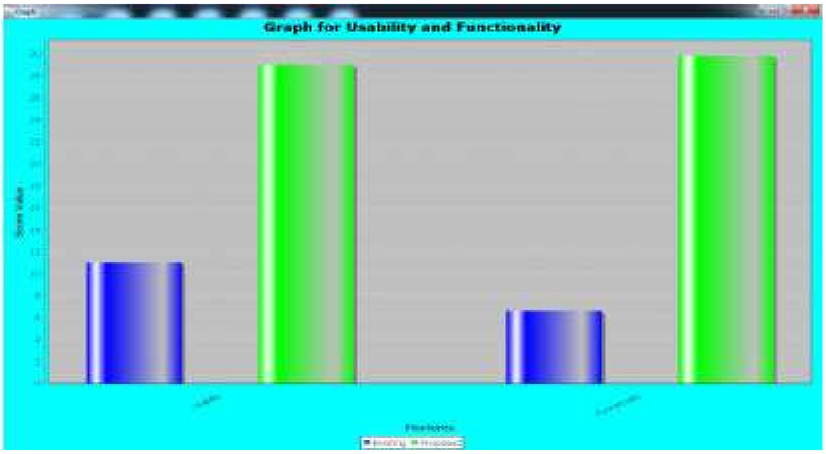

Fig. 4: Graph between Usability and Functionality

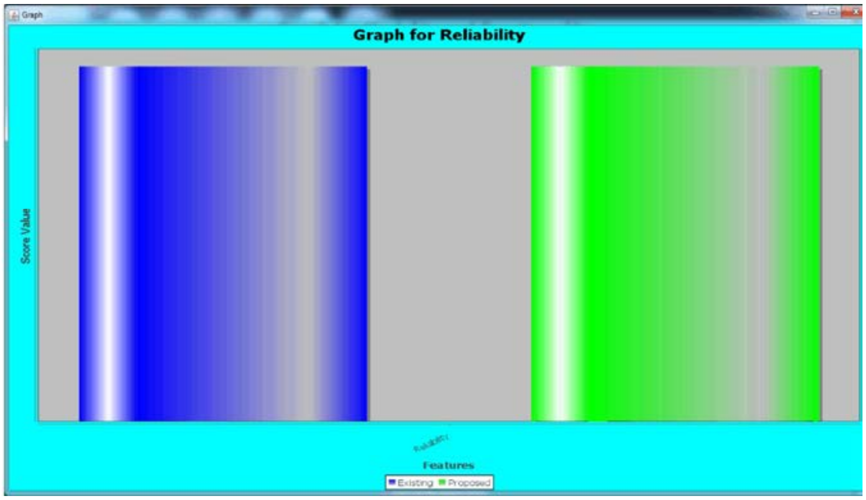

Fig. 5: Reliability of the software between Existing and Proposed

Here, the size, time and security level are taken as parameters to conduct the testing. Comparing the ECC algorithm is taking less time for the given input data while upload the file and retrieve the file. Here, 100kb comma separated value file is tested by both algorithms. For retrieving the uploaded file, RSA taking 78 seconds to download the data, whereas ECC is taking 16 seconds. The results are compared by using line chart given below

CONCLUSION

The benefits of the clouds computing are to achieve the economics of scale, reduce the spending on technology infrastructure which is globalize your workforce as very cheap, steam line process, reduces capital cost, improves accessibility and monitoring the projects more effectively. Another focus, as a cloud provider, they have to ensure the security of user's data. The cloud computing security issues are discussed and new algorithm for protecting the data is developed. The test result shows that the new algorithm is used to protect the data more efficiently. The above system tested with various users and collected the feedback about the reliability of the software is compared with the previous one.

REFERENCES

1. Mell, P. and T. Grance, 2014. The NIST Definition of Cloud Computing, Recommendations of National Institute Standards and Technology, U.S. Department of Commerce,http://www.csrc. nist. gov/ publications/nistpubs/800-145/SP800-145. pdf 145/ SP800-145.pdf.
2. Ross A. Lumley, 2010. Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business", the George Washington University, Report GW-CSPRI-2010-4, 18: 1-10.
3. Behl Akil and Kanika Behl, Security Paradigms for Cloud Computing, International conference on Computational Intelligence, Communication Systems and Networks, pp: 201-205
4. http://searchstorage.techtarget.com/definition/data-availability.last accessed on 27.10.2014.
5. http://www.yourwindow.to/information security/gl _ nonrepudiation. htm. Last accessed on 3.10.2014
6. Neela, K.L. and V. Kavitha, 2013.A survey on Security issues and Vulnerabilities on Cloud Computing, International Journal of Computer Science and Engineering Technology, 4(7): 855-860.
7. Xinyu Lei, Xianofeng Liao, Tingwen Huang and Feno Heriniaina, 2014. Achieving security, robust cheating resistance and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud", Journal of Information Science, pp: 205-217.
8. Cong Wang, Qian Wang and Kui Ren, 2009. Ensuring Data Storage Security in Cloud Computing", Proceedings of IEEE Conference978-1-4244-3876-1/09.
9. Nayer A. Hamidi, Mahdi Rahimi G.K. Alireza Nafarieh, Ali Hamidi and Bill Robertson, 2013. Personalized Security Approaches in E-Banking Employing Flask Architecture over Cloud Environment, Proceedings of 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013), Procedia Computer Science, 21: 18-24.

10. Mark D. Ryan, 2013. Cloud computing security: the Scientific Challenge and a Survey of Solutions, the Journal of System and Software, 86: 2263-2268.
11. Mechmet Yilidiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth, 2009. A Layered Security Approach for Cloud Computing Infrastructure, Proceedings of 10th International Symposium on Pervasive Systems, Algorithms and Networks (IEEE), pp: 763-768.
12. http://www.dataprotection.ie/docs/EU-Directive-95-46-EC/89.htm.last accessed on 28.10.2014
13. Sood Sandeep, K., 2012. A combined Approach to ensure data security in cloud computing, journal of Network and Computer Applications, 35: 1831-1838.
14. Zissis Dimitrios and Dimitrios Lekkas, 2012. Addressing Cloud Computing Security Issues, Journal of Future Generation Computer Systems, 28: 583-592.
15. Danan Thilakanathan, 2014. Shiping Chen, Surya Nepal, Rafael Calvo and Leila Alem, A Platform for Secure Monitoring and sharing of generic health data in the cloud, Journal of Future Generation Computer Systems, 35: 102-113.
16. http://www.cepis.org/index.jsp?p=641&n=825&a=4758. Last accessed on 26.10.2014.
17. Mackay, M., T. Baker and A. Al-Yasiri, 2012. Security-Oriented Cloud Computing Platform for Critical Infrastructures, Journal of Computer Law and Security Reviews, 28: 679-686.
18. http://en.wikipedia.org/wiki/Elliptic_curve_cryptography. Last accessed on 27.10. 2014.
19. Brodkin, J., Gartner: Sevencloud-computing security risks, available at: www.infoworld.com /d/security-central/gartner-seven-cloud-computing-security-risks-853
20. Cloud Computing Security Considerations A Microsoft Perspective, Microsoft Whitepaper,2010 available at http://www.mcirosoft.com/ malaysia/ ea/ whitepapers.aspx
21. Alam Bashir, M.N. Doja, Mansaf Alam, Shweta Mongia, “5-Layered Architecture of Cloud Database Management System”, proceedings of AASRI Conference on Parallel and Distributed Computing and Systems, 2013, pp: 194-199.
22. Nancy J. King and V.T. Raja, 2012. Protecting the privacy and security of sensitive customer data in the cloud, Journal of Computer Law and Security review, 28: 308-319.
23. http://en.wikipedia.org/wiki/RSA_ (cryptosystem). Last accessed on 28.10.2012.