DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4636

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

IMPLEMENTING MULTILEVEL DATA SECURITY IN CLOUD COMPUTING

Nidhi Dahiya
Department of CSE & IT
B.P.S. Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat
Sonipat, India

Sunita Rani
Department of CSE & IT
B.P.S. Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat
Sonipat, India

Abstract: Cloud Computing is an information technology type which is used to access information and sharing of data on remote site. By using cloud computing one has not to worry about load of local data storage to store his data. Security And authentication of data is must while using this kind of services. Various factors are presents there which can affect security of data. This paper provide an idea about security and authentication operation .This paper explain some encryption scheme as well as RSA and how to improve security of a data using Symmetric Tokens. This paper proposes a multilevel authentication technique that helps us to enhance the security of data storage in the cloud computing systems. We provide combined approach DES and AES using RSA to protect clients' authentication data such as user name and password.

Keywords: Cloud Computing Storage, Cloud computing Security, Erasable Correcting Code, Tokenization

I. INTRODUCTION

The process of accessing applications on the Internet is called Cloud Computing [1]. The data on cloud is stored on cloud server which can be used later by client and that cloud server is called as data centre. Any user who want to access their data he simply need an internet connection[2]. But cloud cannot provide control mechanism on data centre. Only CSP known as cloud service provider has full control over it[3].Cloud Computing may be used to reduce cost of IT services and effective data. cloud computing provide rich benefits to users like costless services secure data and resources elasticity and fast access from internet Many more essential characteristics are provide by CSP. Before some years this cloud computing terms is used in only web application but now a days it become an business propositions like Amazon EC2 etc. undoubtedly[4]. In cloud environment users store their data into cloud servers set. All these data servers are running in different machine in a distributed manner. There should be enough guarantee that data is unique and correctness is maintained. So client are ensure that their data is secure. For this various security protocols are used[5][6]. In this paper we have used encryption technique that can ensure us the quality and security of data like [7].If any user want to retrieve that data than CSP is communicated .various operations can be performed on this like insertion and deletion and updating of data. This is not easy to manage this kind of services where multi-tenancy is uses. Multi-tenancy is term in which different kind of computer and services are interlinked and providing services and obviously this is not easy to maintain security of systems. For Secure Operation of data by users here we used tokenization process which helps us to recognize unauthorized access[8][9].

cloud computing process basically uses three models to delivery services for information delivery purpose. All these three models enable user to access information[9].Then there is no need for users to be in the same location as the hardware that stores data we can access data through different location in different area. For this we only require an internet connection to connect with cloud data storage and Once the internet connection is established user can access services of cloud computing through various hardware device[6].

This is not necessary that which is type of connection should it be. it can be any type of either wired oriented or wireless connection[3]. Cloud computing is growing day by day in current era. Cloud data storage store data in a wide range services so that it can provide secure and more reliable data to end users[6].

It allows client user to use that application which he is not installed on his/her PC. By data outsourcing user can access data and application without getting worry about storage headache without getting worried by extra expanses on hardware or installment[10]. Client users don't have to worry about security management of data and there is no need to concern about attacks on his /her data.

All this work is done by a team of professionals and for this third party vendors are to used[3][11].And in this cryptography played a very well role in security mechanism.

Most advanced and highly secure data centers are used to processing the need of customers. Due to security Reason and secure data perspective It is necessary to find out the challenges and risk in cloud data storage that can affect security of cloud data[6]. Following are some security threats described into figure that can affect security and quality of data at cloud data storage centre[3][9].

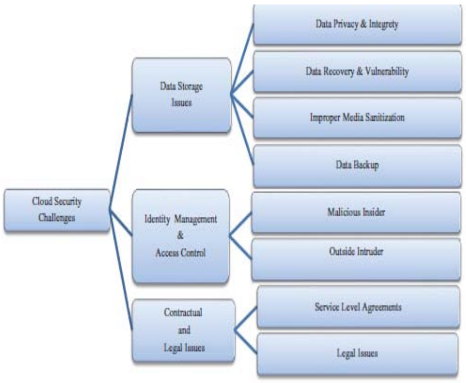

Cloud Security Challenges
Data Storage Issues
Data Privacy & Integrety
Data Recovery & Vulnerability
Improper Media Sanitization
Data Backup
Identity Management & Access Control
Malicious Insider
Outside Intruder
Contractual and Legal Issues
Service Level Agreements
Legal Issues

Figure 1: Data security challenges[3]

Most importantly cloud computing is not just a third party service provider here a no of users logged in every seconds and they update data according to their level and knowledge so this is major concern that data that is to be updated is to secure and correct and updated .

Cloud computing Stores data and information with minimum management effort so client can use that data with the help of internet. but there is one security concern that we can't trust over the security These techniques, while can be useful to ensure the storage correctness without having users possessing data cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations[3][4]. As a complementary approach, there are many researches that proposed distributed protocols and various other protocols to ensure security and data storage accuracy across various servers. once again, from these distributed scheme there is not a schemes which can help us in dynamic data operations. because of this, their applicability in cloud data storage can be drastically limited. and security can't be trusted highly[10].

In this paper, our main propose is to develop an effective distributed scheme for security of cloud data storage . We provide combined approach DES and AES to protect clients' authentication data such as user name and password. and we combined this approach with the help of RMI[8][9]. CSP a cloud service provider ensures the security of data over cloud data storage using firewalls and virtualization[8].
For securing data in this paper we are using symmetric tokens [8][12]

II. CHARACTERISTICS OF CLOUD COMPUTING

To better understand Cloud computing, the US National Institute of Science and Technology (NIST)
define it as: "Cloud computing is an information technology environment that allow us for enabling reliable and highly secure, convenient, on-demand network access on a shared pool of configurable computing resources which are connected with each other in a autonomous environment.

(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or client and service provider interaction. This cloud computing model promotes reliability as well as scalability and availability and is contain of five basic and very important characteristics that every cloud model should have, also composed of three service models, and four deployment models".

NIST define cloud computing essential characteristics as follows [3][5]:

1. **On-demand Self-service**: In cloud environment multiple users logged in to complete their data services which they want to access. Cloud computing environment enables users to maintain the data they want to access and whenever they need they can access it on from any machine which is logged on in cloud environment. This Reduce the need of extra database extra [11]

2. **Multitenancy :** As the term implies to have more than one tenants ,is a process in which one tenants connect with other tenants and shares resources[9][19]. Regardless of the end-user platform, users benefit from the cloud and control them through standard mechanisms[5].

3. **Resource Pooling**: Resource pooling means if you are logged in a cloud environment than you don't have need to extra resources like hardware devices or software services ,you simple can use than on a remote machine you can multiple type of resources[11][19].

4. **Confidentiality**: Confidentiality is a main requirement to manage control over the data of various organizations that may be situated across various distributed databases. Confidentiality is a must when we are doing in a public cloud because there are chances that can affect integrity of data[13]. Confidentiality and protection of end users information and profiles at every levels will provide info security principles at various levels of cloud applications[14]

5. **Elasticity**: rapid elasticity means that you can allocate resources at run time and also release them dynamically when particular machine don't require it. This also need less amount of memory and provide more level of scalability[11]. This provides scalability for more or fewer resources on demand automatically. This Elasticity concept also led to more security and this is the reason why denial of service attack are decreasing day by day[4][19].

6. **Measured services:** Resource pooling is maintain by measuring of devices automatically there is a metering capability which is used to measured the devices and resources according to their type of service storage, their data bandwidth, processing, bandwidth, and active user accounts[11]. This provides transparency for both the cloud vendor and the clients by monitoring, controlling, and reporting resource usage for the utilized service[3][19].

III. PROBLEM STATEMENT

Cloud Computing is not secure computing model because there are many data security challenges.

Data correctness and accuracy of data that is stored in different data storage is maintained by various encryption he data security is provided to the data which is stored in storage cloud by using the various encryption technique that provide a efficient and highly secure data[15]. But still there is a problem through which the data integrity can be endangered i.e when data is transferring from the storage cloud to computational cloud for processing. So, in this thesis we are going to secure data in this stage to make the cloud computing more reliable technology for customers. There May be a problem when a unauthorized user try to access the cloud at first time cloud may ignore that request but for multiple time there is problem to ignore each and every time. so in this we have to find out the user or request which is coming again and again and also unauthorized[9].

for doing this there may be another problem arise which is to remember IP Address or Mac address of that machine so that we can block them. for this purpose we will use AES and DES and RSA along with homomorphic tokens[8][10].

Whenever any user want to access some resources given by server system that system has to log in and then authentication process have to be done. sometimes there are some files or resources which we do not want to access to particular user because of hacker of confidentiality of files then we want a mechanism which ensure the security of that files or resources. for this purpose we will apply a block operation method .and we will also apply symmetric token for no of files that we want to make safe and secure[8][12][16].

IV. ENSURING SECURITY IN CLOUD DATA STORAGE

This is very important to maintain security of cloud data centre where all the data is stored. each and every time when an client logged in data centre are updated gradually and manually[3][4]. so it should be in mind that data which is updated should be correct and unique so Replication of data be avoided, so it is must that the data which is updated is absolutely correct and secured and should be original data no fake one .for this purpose we are using symmetric token along with encryption scheme with RSA and RMI [8] [10][18]. So the correctness and uniqueness of the data files which are being stored on the distributed cloud servers must be guaranteed to be original and safe as well[5]. In this paper our main concern is on authenticated users and to provide files and data only to that users which are authenticated by systems and modification and deletion of operation are to be done by authorized users with unique and original data[12]. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures[12][16]. for example if we talk about distributed case when such inconsistencies can be successfully detected to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors and to find replication and redundancy in data[9].

To solve these kind of problems, our main scheme for ensuring cloud data storage is presented in this section. the first part decide the basic coding tools that are used to distribute data. Then, the homomorphic token is generated[8][12][6]. When any unauthorized user tried to access out data than that users IP address will be automatically block after three attempted[9].

The function we are using to compute token computation belongs to a family of universal hash function chosen to preserve the homomorphic properties[8][9][16], which can be perfectly integrated with the verification of erasure-coded data[4][12]. Subsequently, A challenge response protocol is also used to verify the storage correctness as well as identifying misbehaving servers[4][8][16] to block the server which is not authenticated . Finally, the procedure for file retrieval & error recovery based on erasure-correcting code is outlined[7][8][17].

V. IMPLEMENTATION

Before making any project or other object we first make a design for that that help us to find out the problem that can occur in that particular later we make implementation in that project. so we can say that implementation phase is that stage of a project making in which design phase is turned into final working or implementation. this is the most required and important phase in a system making process that should be handled properly and efficiently and results are reflet ted on our process. So we can say this is the most critical stage in our phase of making a project. which helps us to achieving a successful new system and in giving the user, confidence that the new system will work and be effectively[10] . The implementation phase involves many kind of factors like careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover & evaluation of changeover methods.

Modules

Implementation phase of our thesis contains 4 modules which are ensuring security of data. first one is client module and then data storage module than authentication server which uses different authentication protocols for additional behaviours of users.

1. **Client Module:** In this module, the client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. On the server side, it checks the client name and its password for security process. If it is satisfied and it then received the queries from the client and search the corresponding files in the database. Finally, find that file and send to the client (figure 5.1 below). If the server finds the intruder means, it set the alternative path to those intruders.

2. **Storage of data module :** In cloud computing all users save their data on cloud server that is running at simultaneously different systems. data is stored on different data centres that are managed and organized by a third party vendor know as CSP. Users normally

store their data using CSP on cloud server[4][7]. That data which is to be stored should be secure and original and correct so quality assurance should be present effectively. There are multiple of users are connected through a Multitenancy and sometimes it is difficult for them to monitor the performance and security maintaining .Than there is a option called as TPA(third party auditor)[10][12][18].This TPA helps them to maintain and manage all the security and feasibility. so users don't need to take extra headache for this kind of operation In case users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA [18] of their respective choices. For security a third party vendor called as TPA(Third party auditor) can be hired to make security of data[4]. which is used to manage and secure the data so users don't have extra headache of security and other factors .cloud data storage module is shown in figure 2 below.

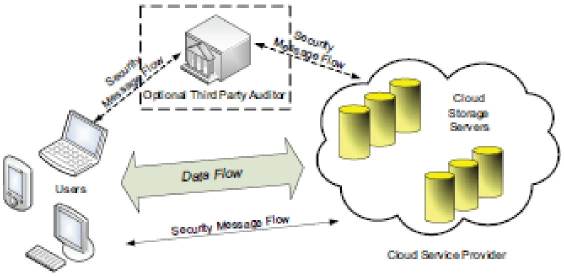


Figure 2: Cloud data storage module[4]

3. **Cloud Authentication Process :** The very first process is authentication which is done with the help of provide username and password to each use[9]r. The Authentication Server (AS) functions as any AS would with a few additional behaviours added to the typical client-authentication protocol. The first step is to sending the client authentication[8][9]information to the masquerading router. A ticketing authority is used here it means whenever any user want to access a files a token is generated ,and controlling permissions on the application network is applied to make security[4] . The other optional function that should be supported by the Authentication server is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request[12].

4. **Secure data modification :** If anyone user want to delete of insert his data or other files he is related to a block level operation and authentication process should be done[8] If any error or problem in security seems to present for a particular client user that should be blocked using symmetric token applied on that file where chances of security broken can be present[10][12][16].

Algorithm:

1. First of all initialize the cloud system with some resources that client or either end users want to access.
2. Start the server window or module by authentication of administrator using start server command .
3. Add new users to use the cloud server resources. While allocating new user apply two security parameters – password and secret key[9]. The security parameters are further protected by using two encryption algorithms-Data Encryption standard (DES) and Advanced Encryption Standard (AES)[6].
4. Add new resources to be used by registered users. While allocating resources create symmetric token with value false (resource is available to particular client) or true (resource is not available to particular client).
5. Start the server service so that any client can access the server resources.
6. Start the Client module by authentication of user. If user successfully login then display the list of available resources for that client.
7. The client can select the particular resource and download the resource information. If client tries to access the restricted resource (Symmetric token set to true) then its information is stored on the cloud server as attacker.
8. The administrator can view the attacker list from server module and block the client IP address if client continuously tries to access the restricted resources.

Activity Diagram

An activity diagram is characterized by states that denote various operations. Transition from one state to the other is triggered by completion of the operation. The purpose of an activity is symbolized by round box, comprising the name of the operation. An operation symbol indicates the execution of that operation. This activity diagram depicts the internal state of an object.

Figure 3 below shows the activity diagram of our implementation.

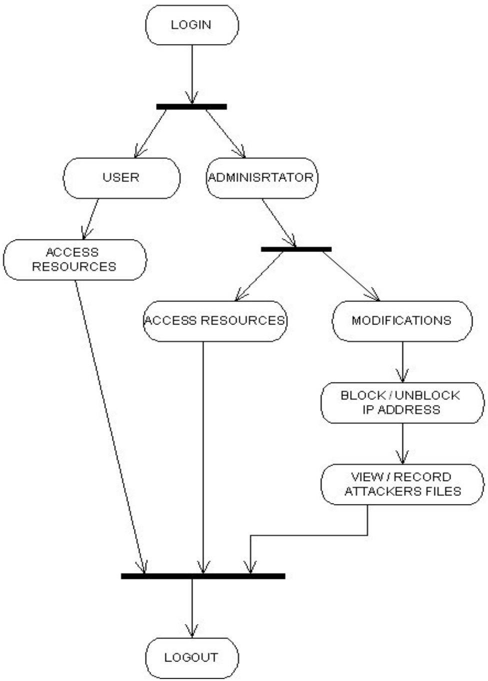


Figure 3: Activity Diagram

Sequence Diagram

The sequence diagrams are an easy and intuitive way of describing the system's behaviour, which focuses on the interaction between the system and the environment. This notational diagram shows the interaction arranged in a time sequence. The sequence diagram has two dimensions: the vertical dimension represents the time and the horizontal dimension represents different objects. The vertical line also called the object's lifeline represents the object's existence during the interaction.
Figure 4 shows the sequence diagram of our implementation.

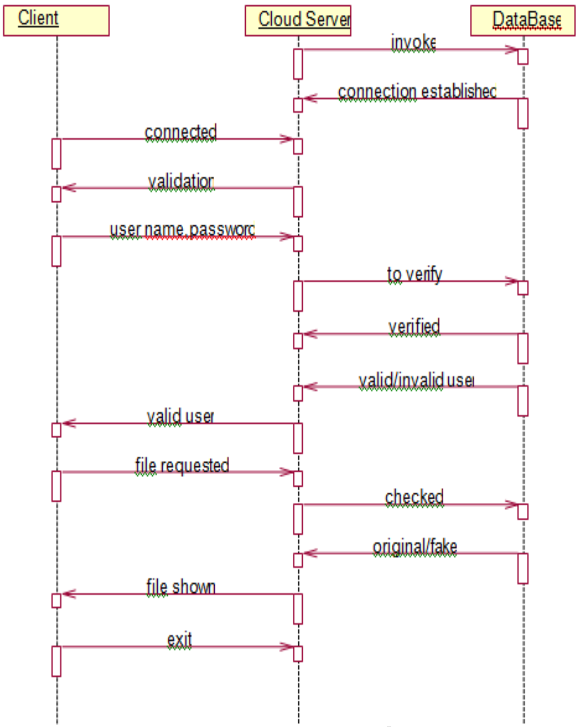
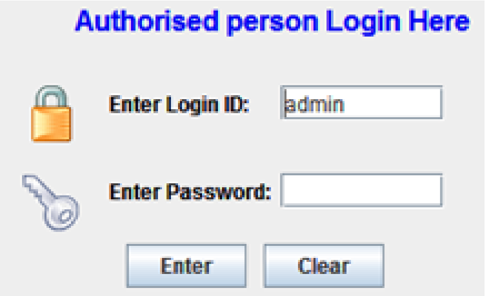


Figure 4: Sequence diagram

VI. RESULTS

The first screen of our implementation result will display the administrator authorization screen as shown in figure 5 below.



admin

Figure 5: Authorization screen

The main screen of our implementation will display as shown in figure 6 below.

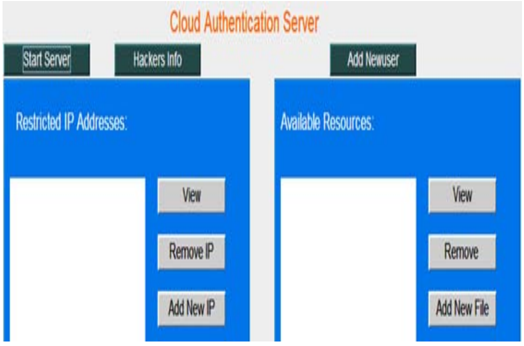


Figure 6: Main screen

The client authentication window will display as shown in figure 7 below.

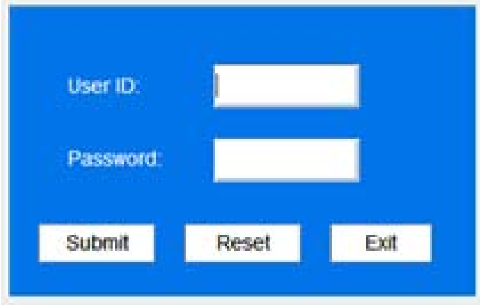
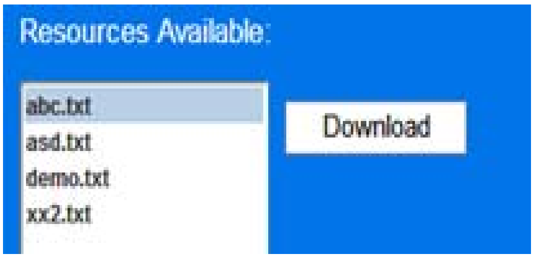


Figure 7: Client Authorization screen

After successful authorization the list of available resources are provided as shown in figure 8 below.



\

Figure 8: Available resources

Comparisons with existing Techniques:

RSA is a block cipher that maps every message to an integer. The cloud provider encrypts the data using the public key while the cloud user decrypts the data using the private key[6]. RSA algorithm involves three steps - key generation, encryption and decryption.

While ECC algorithm security is relies on the difficulty of solving ECDLP[6]. After comparing we come to know that ECC be implemented on 160-bit address also offer the same security against compared with 1024-bit RSA attacks[10].

That led to improved performance and better storage requirements.

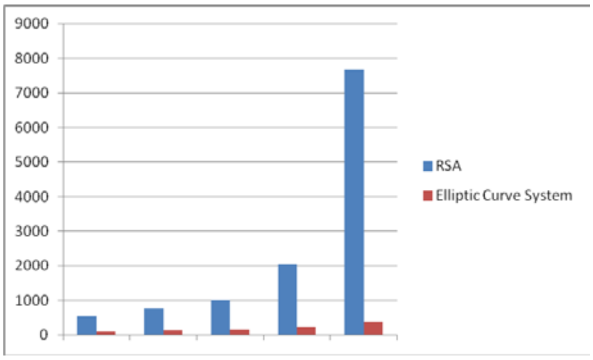


Figure 9:Comparative Bit Lengths

Comparative Bit Lengths between existing & proposed techniques(symmetric token):

It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. Depend on the key size this technique encrypt the data blocks of size 128 bits in 10, 12 and 14 round.. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices. while using symmetric token the bit length. A graph Below presents a comparison of the approximate parameter size between strength elliptic curve systems, RSA & proposed algorithm. which makes our proposed techniques that is symmetric token using is security.

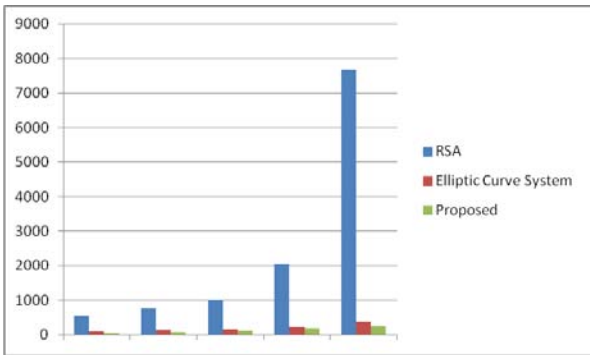


Figure 10:Comparative Bit Lengths between existing & proposed techniques

VII. Conclusion & Future Scope

In this paper, we investigated the challenges and security threats in cloud data storage, which is essentially a distributed storage system. and we have described a new technique which can help us to remove that challenges. we have used tokens which is an flexible and effective distributed scheme[4] that can secure data. we have used symmetric tokens on including block update, delete, and append operations. We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and We are using Remote Method Invocation for networking which communication homogenous objects in future we can use CORBA or SOAP to perform communication between heterogeneous objects. We have used symmetric token to save resources of clouds from hackers which is static in nature but in future we can use non symmetric tokens to protect resources dynamically from unauthorized users..

VIII. References

[1] A. T. Velte, T. J. Velte, R. Elsenpeter, “Cloud Computing, A Practical approach” First Edition, 2009.

[2] R. Velumadhava Rao, K. Selvamani “Data Security Challenges and Its Solutions in Cloud Computing” International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India

[3] N. Vurukonda, B. T. Rao, "A Study on Data Storage Security Issues in Cloud Computing," 877-0509 © 2016 DOI: 10.1016/j.procs.2016.07.335.

[4] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,”IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.

[5] S. Kumar and R.Subramanian , “An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing,” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[6] Dr. S. A. Abbas, A. A. B. Maryoosh, “Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography,” Journal of Computer Engineering, Volume 17, Issue 4, Ver. I, PP 48-53 DOI: 10.9790/0661-17414853 (July – Aug. 2015).

[7] K.Govinda, Dr. E. Sathiyamoorthy, "Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud", Published by Elsevier Ltd., Procedia Technology, April, 2012.

[8] Z .C. Nxumalo, P. Tarwireyi, M. O. Adigun," Towards Privacy with Tokenization as a Service," Department of Computer Science, University of Zululand ,Empangeni, South Africa IEEE-©2014.

[9] S. Subashini, V. Kavitha -Anna University Tirunelveli, India,” A survey on security issues in service delivery models of cloud computing“ ELSEVIER- Journal of Network and Computer Applications Volume 34, Issue 1, January 2011, Pages 1–11.

[10] Prof. S. R. Pardeshi, Prof. V. J. Pawar, Prof. K. D. Kharat," Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques",

[11] S. Bollavarapu and B. Gupta, “Data Security in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.

[12] A. Kumar, H. Prasad, S. Chandra, "Homomorphic Token and Distributed Erasure-Code for cloud," International Journal of Research in Computer and Communication Technology, Vol 2, Issue 10, ISSN (Online) 2278- 5841, October- 2013.

[13] M. k. Sarakar, S. Kumar, "A Framework to Ensure Data Storage Security in Cloud Computing," IEEE 1–216, 2016.

[14] H. Ziglari, S. Yaahiya," Deployment Models: Enhancing Security in Cloud Computing Environment," IEEE ©2016.

[15] M. P. Babitha, K. Remesh Babu," Secure Cloud Storage Using AES Encryption", *(*ICACDOT*)* ©2016 IEEE

[16] Mr. V. Biksham, Dr. D. Vasumathi, "Query based computations on encrypted data through homomorphic encryption in cloud computing security," International Conference on Electrical, Electronics, and optimization Techniques (ICEEOT) ©2016.

[17] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," in Trust and Trustworthy Computing, vol. 6101, Eds. Springer Berlin Heidelberg, pp. 417–429, 2010.

[18] P. Garg, V. Sharma, "An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function", IEEE ©2014.

[19] Y. Tabbii, I. Enjajjar, A. bankaddour," Security in Cloud Computing approaches and solutions," IEEE ©2014.