Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 01, pp.44634-44639, January, 2017

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

DYNAMIC KEY BASED DATA OWNER CENTRIC MODEL FOR ENSURING DATA SECURITY IN CLOUD

[1], *Varsha Yaduvanshi, [2]Manish Rai and [3]Dr. Mohit Gangwar

[1, 2]Department of Computer Science and Engineering, RKDF College of Engineering, Bhopal, India
[3]Department of Computer Science and Engineering, Bhabha Engineering Research Institute, Bhopal, India

ARTICLE INFO

Article History:
Received 25th October, 2016
Received in revised form
15th November, 2016
Accepted 14th December, 2016
Published online 31st January, 2017

Key words:

Cloud, Security, Data,
Encryption, Cloud SIM.

ABSTRACT

Cloud computing is model which uses combine concept of "software-as-a-service" and "utility computing", provide convenient and on-demand services to requested end users. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, thus infecting the entire cloud and affects many customers who are sharing the infected cloud. This paper firstly lists the parameters that affect the security of the cloud then it explores the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, and infected application and security issues. It discusses a new technique to tackle these issues and problems.

Citation: Varsha Yaduvanshi, Manish Rai and Dr. Mohit Gangwar, 2017. "Dynamic key based data owner centric model for ensuring data security in cloud", *International Journal of Current Research*, 9, (01), 44634-44639.

INTRODUCTION

Storing data in the cloud can be considered quite attractive form of outsourcing focused on daily data management (Mell and Grance, 2011). Despite this claim, but the real responsibility for managing the data falls within the company that owns the data. With this in mind, it is important to understand some of the causes of data corruption. Such causes advise keeping the big responsibility of cloud services, some basic best practices for the use of secure data storage to the cloud, as well as the methods and standards for monitoring the integrity of the data regardless of data storage (Sullivan, 2012). In order to achieve higher security and redundancy of the data stored in the cloud at the same time locally. One of the main advantages of storing data in the cloud, is unlimited access to the data, with no limitations lies in the time and place of access (Williams, 2010). This property is used by firms whose occupation takes place in various remote locations. For such companies it pays to enter into cloud solutions and, therefore, that this eliminates the burden of physical storage devices, use the same computer and multiple access data in real time (real-time reporting) (Williams, 2010). In this case, it is important to create storage cloud to think about the specialty store. Although there are hundreds of cloud storage, each storage site is oriented to other requirements, such as storing communication by e-mail, store employee profiles, documentation storage projects, etc. (Williams, 2010). Of course, requirement may also store all types of documents.

Cloud computing

Cloud computing has been intended as the next generation paradigm in information Technology. From this cloud computing environment, both resources and applications are provided through the Internet as a service on demand. Cloud environment is comprised of software and hardware resources in the data centers that run different services over the internet or network to satisfy the user's needs and it depends on sharing resources instead of having local servers to handle application for a certain individual or organization (SwapnaLia Anil and Roshni Thanka, 2013; Salve Bhagyashri and Gurav, 2014). Since there is no infrastructure investment requires, shrink or expand the resources based on on-demand and the payment based on usage, it becomes popular among different technology aspects. The numerous cloud enterprise systems looks for these advantages to be used in various applications. The service of the cloud makes it possible to access the data at anytime from anywhere. Cloud computing utilize the networks of a huge group of servers naturally brings a low rate data processing with specialized connection. Therefore, cloud computing has an interesting new model of IT service provisioning and support driven by productivity and economic benefits. Cloud computing can be separated into two subsections such as the cloud and the user. In most scenarios,

Corresponding author: Varsha Yaduvanshi,
Department of Computer Science and Engineering, RKDF College of Engineering, Bhopal, India.

the individual user is connected to the cloud environment through the internet. This process is also possible for an organization to connect the private cloud via the internet. Therefore, both subsections are alike other than the utilization of the public and private cloud or the network (Yunchuan Sun *et al.,* 2014; Abhinay *et al.,* 2013). The cloud computing has the normal functions such as, the user requests to the cloud and the cloud response to the user (Tejaswi *et al.,* 2012). The elasticity and multi-tenancy are two key features of the cloud environment (i.e.) sharing the same service instance, among the various tenants and elasticity enables a service based on the present cloud service demand. Characteristics of this service are to improve the service availability and resource utilization. Cloud services are divided into three service models such as Infrastructure-as-a-service (IaaS),Platform-as-a-service (PaaS), Software-as-a-service (SaaS). Each service has various implementations as shown in Figure 1, which complicates progress of standard security model for each cloud service.

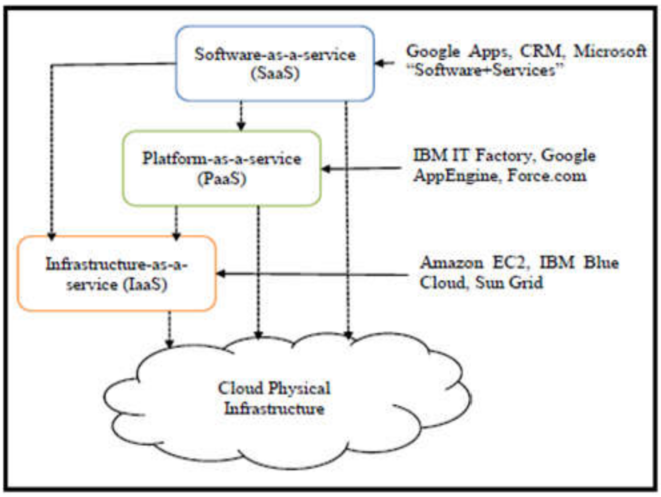


Fig. 1. Cloud Service Model

Choosing a cloud provider

Each provider serves a specific function, giving users more or less control over their cloud depending on the type. When you choose a provider, compare your needs to the cloud services available. Your cloud needs will vary depending on how you intend to use the space and resources associated with the cloud. If it will be for personal home use, you will need a different cloud type and provider than if you will be using the cloud for business. Keep in mind that your cloud provider will be pay-as-you-go, meaning that if your technological needs change at any point you can purchase more storage space (or less for that matter) from your cloud provider. There are three types of cloud providers that you can subscribe to: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three types differ in the amount of control that you have over your information, and conversely, how much you can expect your provider to do for you. Briefly, here is what you can expect from each type.

- Software as a Service - A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud.
- Platform as a Service - A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.
- Infrastructure as a Service - An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software that they need.

As you go down the list from number one to number three, the subscriber gains more control over what they can do within the space of the cloud. The cloud provider has less control in an IaaS system than with a SaaS agreement (Alexa Huth and James Cebula).

Various data security aspects in cloud

The proposed cloud security data model is based on a three-layer system structure, in which each layer performs its own duty to ensure the data security of cloud layers. The first layer is responsible for cloud user authentication. It is designed as OTP authentication module and uses digital certificates issued by the appropriate users and also manage user permissions. The second layer manages the user's data encryption by using AES algorithm (Cartrysse and Van der Lubbe, 2004), which is the most secured and faster encryption algorithm (Sullivan, 2012). For sensitive data such as one's personal information (ex. credit card number) should be encrypted and sent to the cloud .Data integrity is provided by using algorithms like MD5 (ZhaoYong-Xia and and Zhen Ge, 2010) and RSA (Aayush Chhabra and Srushti Mathur, 2011; Uma Somani *et al.,* 2010). For non-sensitive data such as one's local information (ex. address details), it should protected by using digital signatures and sent to the cloud. It also protects the privacy of users based on fine-grained attribute based access control policies through access control policy algorithms. Access control mechanisms are tools to ensure authorized user can access and to prevent unauthorized access to information systems. Such mechanisms should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls (Farzad Sabahi, 2011). The third layer supports the faster user data recovery by using Byzantine fault tolerance algorithm methods. With three-level structure, user authentication is used to ensure that data is not tampered. The user authenticated can manage the data by operations: Add, modify, delete and so on. If the user authentication system is deceived by illegal means, and malign user enters the system, file encryption and privacy protection can provide this level of defense. In this layer user data is encrypted, even if the key was the illegally accessed, Through privacy protection, malign user will still be not unable to obtain effective access to information, which is very important to protect business users' trade secrets in cloud computing environment. Finally, the rapid restoration of files layer, through fast recovery algorithm, makes user data be able to get the maximum recovery even in case of damage (Dai Yuefa *et al.,* 2009).

Main advantages of the proposed system are

- Highly expressive, fine grained access policies.
- Private user keys with attributes.
- Encrypted files for trusted storage.
- Files can encrypt under policy over attributes.
- Files can be decrypted only if attributes satisfy policy.
- Fault Tolerance System is added.

One of the biggest security concerns people have when moving to the Cloud is related to the problem of keeping data secure and confidential. In this respect, some particular problems arise: who can create data, where the data is stored, who can access and modify data, what happens when data is deleted, how the back-up is done, how the data transfer occurs, etc. All of this is known as data security lifecycle. Data life cycle refers to the entire process from generation to destruction of the data. The data life cycle is divided into seven stages. See the figure below:

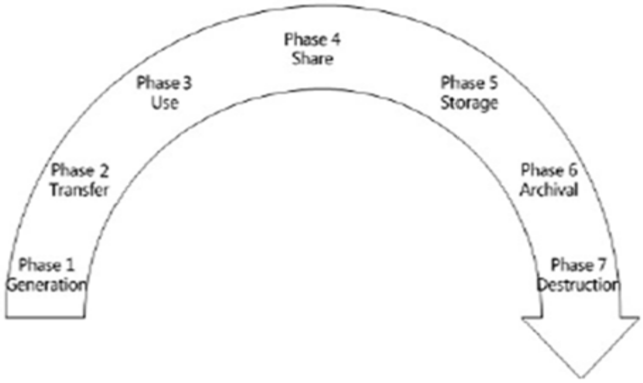


Fig. 2. Data Security Life Cycle

A. Data Generation

Data generation is involved in the data ownership. In the traditional IT environment, usually users or organizations own and manage the data. But if data is to be migrated into Cloud, it should be considered that how to maintain the data ownership.

B. Data Transfer

Within the enterprise boundaries, data transmission usually does not require encryption, or just have a simple data encryption measure. For data transmission across enterprise boundaries, both data confidentiality and integrity should be ensured in order to prevent data from being tapped and tampered with by unauthorized users.

C. Data Use

The owners of private data need to focus on and ensure whether the use of personal information is consistent with the purposes of information collection and whether personal information is being shred with third parties, for example, Cloud service providers.

D. Data Share

The data owners can authorize the data access to one party, and in turn the party can further share the data to another party without the consent of the data owners. Therefore, during data sharing, especially when shared with a third party, the data owners need to consider whether the third party continues to maintain the original protection measures and usage restrictions.

E. Data Storage

The data stored in the Cloud storages is similar with the ones stored in other places and needs to consider three aspects of information security: confidentiality, integrity and availability.

Literature review

Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era. Cloud computing is an emerging model of business computing. In this paper, we explore the concept of cloud architecture and compares cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues (Tejaswi et al., 2012). Data security has a major issue in cloud computing environment; it becomes a serious problem due to the data which is stored diversely over the cloud. Data privacy and security are the two main aspects of user's concern in cloud information technology.

Numerous techniques regarding these aspects are gaining attention over the cloud computing environments and are examined in both industries and academics. Data privacy and security protection are becoming the most significant aspects for the future enhancement and development of cloud computing technology in the field of business and government sectors. Thus, in this paper, the cloud computing security techniques are assessed and its challenges regarding data protection are discussed. The main aim of this proposed work is to enhance the data privacy and security for the reliable cloud environment. This comparative research investigation of the existing cloud security approach regarding the data privacy and security techniques utilized in the cloud computing. It will be useful to enhance the security of data storage in a cloud environment (Uma Somani et al., 2010). Cloud computing is a natural evolution for data and computation centers with automated systems management, workload balancing, and virtualization technologies. In this paper, the authors discuss security issues, privacy and control issues, accessibility issues, confidentiality, integrity of data and many more for cloud computing. Current solutions for these security risks are also discussed. In addition, we make a list of security items that all users should be aware of before opting to use cloud based services and discuss methods for allowing the user to select specific security levels of security for items. This paper aims to present a survey in cloud computing, which gives solutions for challenges faced by cloud .Further this helps to find out the solution for the drawbacks found in given methods and come up with new solution or method to secure the cloud (Williams, 2010).

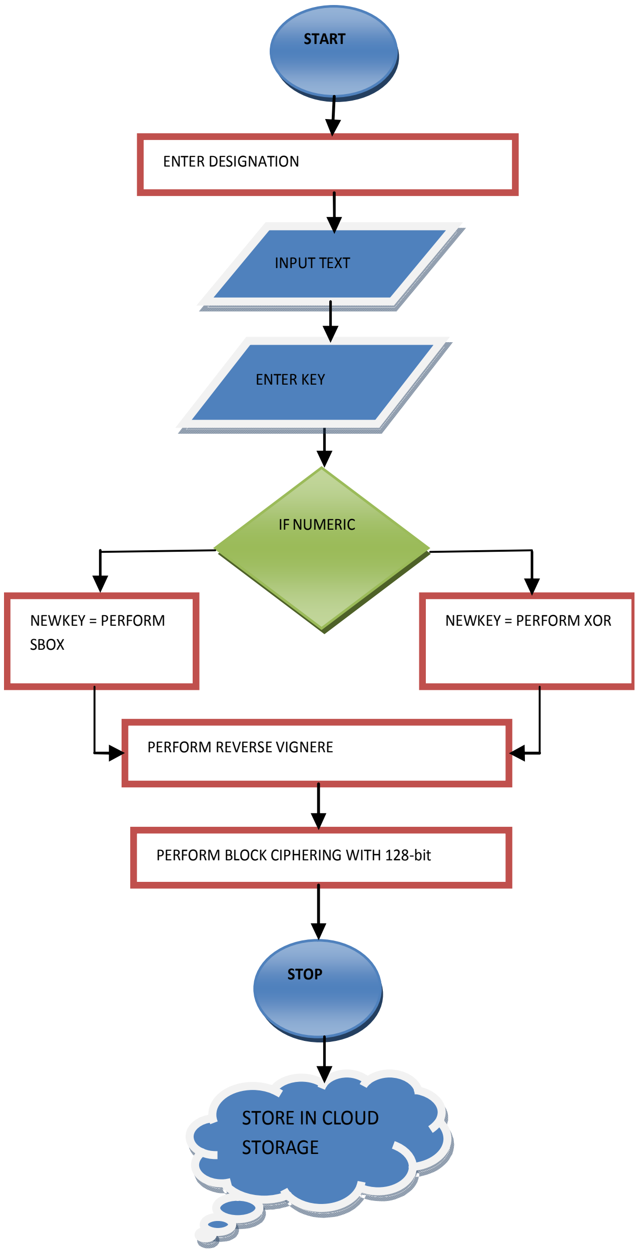


Figure 3. Proposed Work Architecture

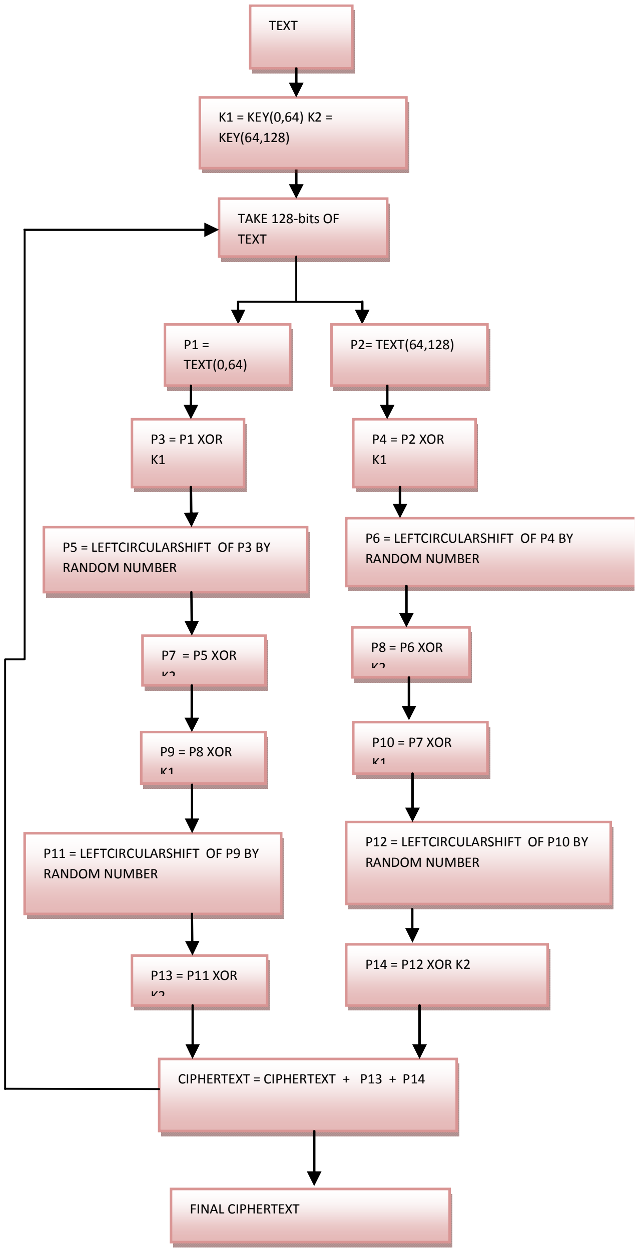

TEXT
K1 = KEY(0,64) K2 = KEY(64,128)
TAKE 128-bits OF TEXT
P1 = TEXT(0,64)
P2= TEXT(64,128)
P3 = P1 XOR K1
P4 = P2 XOR K1
P5 = LEFTCIRCULARSHIFT OF P3 BY RANDOM NUMBER
P6 = LEFTCIRCULARSHIFT OF P4 BY RANDOM NUMBER
P7 = P5 XOR K2
P8 = P6 XOR K2
P9 = P8 XOR K1
P10 = P7 XOR K1
P11 = LEFTCIRCULARSHIFT OF P9 BY RANDOM NUMBER
P12 = LEFTCIRCULARSHIFT OF P10 BY RANDOM NUMBER
P13 = P11 XOR K2
P14 = P12 XOR K2
CIPHERTEXT = CIPHERTEXT + P13 + P14
FINAL CIPHERTEXT

Figure 2. Proposed Work Architecture

Cloud computing is a technology which satisfies customers dynamic resource demands and makes the job easier to work on all platforms for the user. Cloud computing is the delivery of computing services over the Internet. Security is the main criteria when working on cloud, as the third party involvement will be there. Secure architecture should be used to provide services through the cloud. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. Methods show how to overcome the security issues of the cloud (Yunchuan Sun et al., 2014).

Proposed work

Objective

After reviewing various work, the main thing which needs to get attention is security of data in a cloud environment. This proposed work is concentrating on the data security issue through the dynamic key utilization.

Table 1. Comparison of Existing Works

Reference No.	Advantages	Limitations
16	organization can store large amount of data	Time Efficiency gets sacrificed.
17	Concentrate on Virtualization	Missing other aspects
18	This article a mechanism using the content-based watermarking technique	Memory Issue is there.
19	Authentication, Authorization And File Synchronization	Less Time Efficient

Work

The proposed encryption algorithm is double layered approached. Which means at the first layer, it uses two pre-existing approaches for the encryption of user data and in the second layer, this algorithm uses a new approach of encryption of the data. In the proposed work, an architecture which is a combination of various cryptographic algorithms: Encryption/ Decryption algorithm, and key generation algorithm is developed to gain the high security on the data storage in cloud computing. This proposed work architecture shows that the proposed work uses the dynamic key while doing encryption of the data for the cloud environment. In this work, key is randomly generated. This key generation process is done based on the data type. If data is of numeric then key is generated in one way. If key is alpha-numeric then key is generated in another way. Which will ensure the dynamicity and this dynamicity provide more security to the proposed encryption work. Figure 2 show the proposed block ciphering technique. This flow chart shows the working of it in details.

RESULT ANALYSIS

Cloud SIM

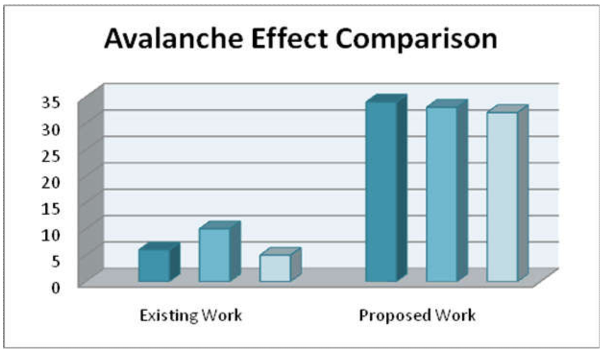
A Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services. The Cloud Computing and Distributed Systems (CLOUDS) Laboratory, formerly GRIDS Lab, is a software research and development group within the Dept. of Computer Science and Software Engineering at the University of Melbourne, Australia.

Table 2. System and Software Configuration

Hardware configuration	Software configuration
Processor : 2.13GHz Intel core duo	Operation System : windows-7,8
RAM : 2GB	j2se : version 8
Hard-Disk : 500MB	jar - cloudsim : 3.0.3

Table 3. Comparison of Avalanche Effect with First Text and 3 keys

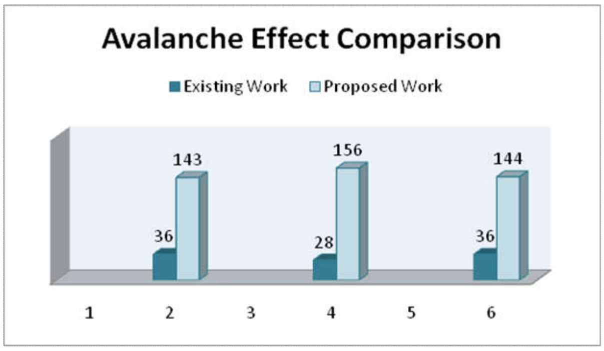
Input Text	Key	Existing Work (ZhaoYong-Xia and Zhen Ge, 2010)	Proposed Work
Hello World	antiinflammatory	6	34
Hello World	chemoluminescent	10	33
Hello World	dedifferentiated	5	32



Graph 1. Comparison of Avalanche Effect with First Text and 3 keys

Table 4. Comparison of Avalanche Effect with Second Text and 3 keys

Input Text	Key	Existing Work (ZhaoYong-Xia and Zhen Ge, 2010)	Proposed Work
The earliest authenticated human remains in South Asia	chemoluminescent	36	143
The earliest authenticated human remains in South Asia	dedifferentiated	28	156
The earliest authenticated human remains in South Asia	antiinflammatory	36	144



Graph 2. Comparison of Avalanche Effect with Second Text and 3 keys

Conclusion

Cloud, is prone to manifold security threats varying from network level threats to application level threats. In order to keep the cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like security issues, accessibility issues, confidentiality, integrity of data. Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. In addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning. In this paper various security concerns related to the three basic services provided by a Cloud computing environment are considered and the solutions to prevent them have been discussed. The improvement is done in proposed work with the comparison of the existing work is not fixed. IT gets change with the changing with plain text along with various keys. There is improvement over 100% in most of the cases.

REFERENCES

Aayush Chhabra and Srushti Mathur, Modified RSA Algorithm - A Secure Approach, 2011.

Abhinay B. Angadi, Akshata B. Angadi, Karuna C. Gull, 2013. “Security Issues with Possible Solutions in Cloud Computing-A Survey”, *International Journal of Advanced Research in Computer Engineering & Technology,* (IJARCET), Vol.2, Issue 2.

Alexa Huth and James Cebula. “The Basics of Cloud Computing”.

Cartrysse, K. and J.C.A. Van der Lubbe, 2004. " The Advanced Encryption Standard: Rijndael," Supplement to the books” Basic methods of cryptography” and “Basismethoden cryptografie”, October.

Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan and Tang Chaojing, 2009. "Data Security Model for Cloud Computing," Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22.

Farzad Sabahi, 2011. “Cloud Computing Security Threats and Responses,” 2011.

Manas M N, Nagalakshmi C K and Shobha G,” “Cloud Computing Security Issues And Methods to Overcome”,” International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2014.

Abhinay B.Angadi, Akshata B.Angadi and Karuna C.Gull, “Security Issues with Possible Solutions in Cloud Computing-A Survey”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

Santosh Kumar and R. H. Goudar, “Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey,” International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012.

Rex Cyril1 B. and DR. S. Britto Ramesh Kumar, “Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey,” International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 04 | July-2015.

Maninder Singh Bajwa, Himani and Dr. Sandeep Singh Kang, 2015. "An Enhanced Data Owner Centric Model for Ensuring Data Security in Cloud," IEEE, 2015.

Mell, P., Grance, T. 2011. The NIST Definition of Cloud Computing, USA, Gaithersburg.

Salve Bhagyashri, Prof. Y.B. Gurav, 2014. “A Survey on Privacy-Preserving Techniques for Secure Cloud Storage”, *International Journal of Computer Science and Mobile Computing,* Vol. 3, Issue. 2, PP.675 – 680.

Sullivan, D. 2012. TechTarget: Hybrid cloud: It's not as secure as you think. (cit. 2012-08-25). Available: http://search cloudcomputing.techtarget.com/tip/Hybrid-cloud-Its-not-as-secure-as-youthink

SwapnaLia Anil, Roshni Thanka, 2013. “A Survey on Security of Data outsourcing in Cloud”, *International Journal of Scientific and Research Publications,* Vol. 3, Issue 2.

Tejaswi, B., L.V. Reddy, M. Leelavathi, 2012. “A Survey on Secure Storage Services in Cloud Computing”, *Global Journal of Computer Science and Technology Cloud & Distributed,* Volume 12 Issue, 0975-4172.

Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), 2010.

Williams, M. 2010. A Quick Start Guide to Cloud Computing: Moving Your Business into the Cloud, USA, Kagan Page.

Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, 2014. “Data Security and Privacy in Cloud Computing”, *International Journal of Distributed Sensor Networks,* Volume 2014, Article ID 190903, 9 pages.

ZhaoYong-Xia and Zhen Ge, 2010. "MD5 Research," Second International Conference on Multimedia and Information Technology.

****