

Total Survey of Data Security Issues in Cloud Computing
Mr. Sagar D. Rushi *, Prof. Pragna Makwana, Prof. Kishori Shekokar

* M.E. Computer Student, Sigma College of Engineering & Technology, India
Asst. Prof., Computer, Sigma College of Engineering & Technology, India
H.O.D., Computer, Sigma College of Engineering & Technology, India

Abstract

In today's IT era cloud computing is the most preferable research topic. In cloud computing data storage, data transfer can be possible. So that, data security is the main aspect of cloud computing and also for any other network. For data security in cloud computing various methods are used. This review paper gives the total review of data security in cloud computing. This review paper also gives overview of cloud computing and its characteristics.

Keywords: Cloud Computing, Cloud Security, Data Security, AES.

Introduction

In today's IT era cloud computing is an important technology. Cloud computing is the network access of pool of resources (i.e network storage, Machines, operating system, applications). In cloud computing data storage, data transfer and many other works can be done. So we can say that those all data has to be secure. It seems that data security is main aspect of cloud computing. Cloud computing syndicate grid computing, virtualization, distributed computing, network computing etc. figure 1 shows the architecture of cloud computing.



Figure [1] Architecture of cloud computing [1].

In simple way the cloud computing is one kind of platform which provides cloud usage to their users. Cloud computing permits an access to data and resources from anyplace at any time. But the condition is only that there is an internet access to that particular used of cloud computing. Various cloud providers are there like amazon, yahoo, Google etc. Various cloud services used in recent and past years are online storage, social networking sites, online data backup etc.

As shown in figure we can say that cloud computing provides 3 kinds of services like Platform as Services (PaaS), Software as Services (SaaS), and Infrastructure as Services (IaaS). Some examples of PaaS are Google Apps, Facebook, YouTube, etc. Examples of SaaS are Microsoft Azure, Google App Engine, and Amazon Simple DB/S3. Examples of IaaS are Amazon EC2, GoGridetc [2].

Some characteristics provided by cloud computing is as follow which can be shown in figure 1.

- On demand self service
- Ubiquitous Network access
- Location Independent Resource Pooling
- Rapid Elasticity
- Pay Per Use

In cloud computing data security, data integrity, and data leakage all are important and main concern. For all of this cryptographically solutions are available. We can get data security in cloud computing using RSA algorithm, AES algorithm, DES algorithm, IDEA algorithm etc. In this research paper we are giving total review of data security methods using in cloud computing.

Possible Issues over Cloud Computing:

Cybercriminal's major effects on cloud computing and especially for data security. Possible attacks are like flooding attacks, port scanning, Insider attack etc. we have solutions for these kinds of issues.

Data Security of Cloud Computing using AES Algorithm:

AES is the symmetric key block cipher algorithm with which we can provide data security of cloud computing [8]. This block cipher uses 128 bit block size and key length can be 128, 192, and 256. It means for 128 bit key length AES performs 10 rounds, for 192 bit key it performs 12 rounds and for 256 bit key it will perform 14 rounds. All of these rounds perform some steps. Key expansion, Pre round, rounds and last final round.

Advantages of AES:

- AES performs well in both software and hardware platform under wide range of environments.
- It provides Inherent facilities with which processor resulting in very good software performance
- AES has speedy key setup time and good key ability.
- Less memory for implementation.
- Good potential for benefiting from instruction level parallelism.
- No serious weak keys in AES [8].

Related work

Jun Hu et al. [2] addresses data security access control model of secured data accessing based on MAC access control, which originates from the government cloud platform construction. This model includes necessary technical strategies to ensure the security of data accessing. They also study about the relationship of risk factor and expected solutions. Here, authors were talking about data access security model and gives data access process after the 3-stage control technology. So, main achievement is high reliability can provide a reference for the government of cloud construction [2].

A review of data security issues in cloud environment presented by SahilZatakiya et al. [3] authors said that cloud computing is novel pattern of computing where resources are provided on demand via internet usage. Here, author discussed and analysed security and privacy issues related with cloud and its data storage. They also discuss about various attacks over cloud computing. Here, authors were talking about different security problems and attacks on cloud computing environment. In this paper they identify some challenges like security issues, data challenges and also give solutions regarding those issues. They also include some attacks with their properties. Big challenge is that to make data very secure and consumed performance cost is less than others [3].

N Hemalatha et al. [4] addresses a comparative analysis of encryption techniques and data security

issues in cloud computing. In this paper they discuss a perspective of cloud computing technologies essential characteristics, classification, delivery models and various encryption mechanisms. After studying and comparative study made on several encryption techniques are used for maintaining security and confidentiality over a cloud [4].

Authors also classified cloud computing in various parts. Here, they also talk about data integrity, data security, data storage, data backup and recovery, data confidentiality and all. The main challenge is to provide security and privacy to protect data in cloud. Here, they analyse the importance of data privacy and security. They compare various encryption techniques used in cloud environment [4].

Zhang Xin et al [5] addresses a research on cloud computing data security model based on multi-dimensions. Here, they talk about the complete data security model which is based on multi-dimension. This model adopts multi-dimension architecture of three-layer defence. First is authentication of user, second no access to unauthorised user. So, they said that each and every layer has their own job and they combine them with each other and provides the data security in cloud computing [5].

Here, authors were talking about challenges which are facing by cloud computing. Two things are happened here, 1) summarisation of data application mode and gives data application system model in cloud system. 2) Evaluates the basic security of cloud computing data platform [5].

A scalable and efficient user authentication scheme for cloud computing environments presented by FarazFatemi M. et al[6]. Here, they proposed an efficient and scalable user authentication scheme for cloud computing. Summary of this paper is that, designing this user authentication and access control model will enhance the reliability and rate of trust in cloud. In this there are two separate servers which stores authentication and cryptography resources from actual servers to decrease dependency of user authentication and encryption process from main server. This model provides reliability too [6].

Data security and authentication hybrid cloud computing model presented by Jingxin K. W. et al[7]. Here, they discuss various methods to protect user data. This security includes single encryption, multilevel virtualization and authentication interface. Main frame of this paper is authentication. Authentication used in this paper is based on CA and PKI model which gives better performance [7].

Following table 1 shown below, the comparison of other algorithm used in data security over cloud computing at the end of paper.

Conclusion

In advance IT world cloud computing and its security of data storage, data sharing and all are the main issues of it. After studying various research paper regarding data security issues we can say that data security over cloud computing is the most important aspect of it. Some security solutions were given by so many authors. The main challenge is that to give a very secure data storage, data transfer data sharing etc. so many algorithms are used there. This review paper summarised this solutions and issues of data security over cloud computing.

After studying all reviews and research paper we can say that there are so many crypto graphical algorithms with which we can solve data security problem over cloud computing. Like DES, RSA, IDEA and AES. Now a days AES is the most power full algorithm for data security. This AES performs with 128 bit keys only. In future we can increase the key size and number of rounds and we can get better data security over the cloud computing.

Acknowledgements

I would like to thank my college to giving me this opportunity to make and publish this review paper. I also would like to thank my HOD Ms. Kishori Shekokar who provide me valuable knowledge and guidance how to write and publish paper.

I would like to thank my guide Ms. Pragna Makawana who help me through out the paper and givige me her valuable knowledge. And like to thank my friends Mr. Puneet C. Chandhok and Siddharth K. Chakravarty who help me through out my paper with their valuable knowledge.

References

- [1] A survey of intrusion detection techniques in Cloud; ChiragModi, Dhiren Patel, BhaveshBorisaniya, Hiren Patel, Avi Patel, MuttukrishnanRajajaran; In Journal of Network and Computer Applications 36 Page No 42-57, 1084-8045, © 2013 Elsevier.
- [2] Jun Hu, Lei Chen, Yunhua Wang, Shi-hong Chen, Data Security Access Control Model of Cloud Computing, International Conference on Computer Science and Application - IEEE, 2013, page 29-34.

- [3] SahilZatakiya, Pranav Tank, A Review of Data Security Issues in Cloud Environment, International Journal of Computer Applications – IJCA, page – 14-18, 2013, volume- 82.
- [4] N. Hemalatha, A. Jenis, A. Cecil Donald, L. Arockiam, A comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing, International Journal of Computer Applications – IJCA, Page – 1-6, 2014, volume – 96.
- [5] Zhang Xin, Lai Song-qing, Liu Nai-wen, Research on based on Multi-Dimension, International Symposium on Information Technology in Medicine and Education – IEEE 2012, page 897-900.
- [6] FarazFatemiMoghaddam,Shiva Gerayeli Moghaddam,SohrabRouzbeh, Sagheb KohpayehAraghi,NimaMoradAlibeigi,Shirin Dabbaghi Varnosfaderani, A Scalable and Efficient User Authentication Scheme for Cloud Computing Environment, IEEE – 2014, page 508-513.
- [7] Jingxin K. Wang, XinpeiJia, Data Security and Authentication in Hybrid Cloud Computing Model, IEEE – 2012, Page 117-120.
- [8] MdAsifMushtaque, Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security, International Journal of Computer Science and Engineering – IJCSE 2014, Volume 2, Issue 4, Page 76-82.
- [9] AbhaSachdev, MohitBhansali, International Journal of Computer Application IJCA – 2013, Volume 67, Issue 9, Page 19-23.