Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.80 – 85

RESEARCH ARTICLE

Enhancing Content Security using MD5 & UTF8 Encoding at Window Azure Cloud

Harjinder Kaur[1], Sarpreet Singh[2]

[1]Research Fellow, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India
[2]Assistant Professor, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

[1] sidhu89harry@yahoo.com; [2] ersarpreetvirk@gmail.com

Abstract— Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Data security is one of the biggest concerns in adopting Cloud computing. In Cloud environment, users remotely store their data and relieve themselves from the hassle of local storage and maintenance. However, in this process, they lose control over their data. Since the data transmission on the internet or over any networks are vulnerable to the hackers attack. We are in great need of encrypting the data. So, in this paper we describe the enhancement in security using MD5 & UTF8 Encoding schemes. In this work we also include a signature to add more security while uploading the contents & also by making restrictions on the number of transactions per user.

Key Terms: - Cloud Computing; Content Security; MD5; UTF8; Signature; Window Azure

I. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. Cloud is a new business model wrapped around new technologies such as server virtualization that take advantage of economies of scale and multi-tenancy to reduce the cost of using information technology resources. It also brings new and challenging security threats to the outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data.

The term cloud computing probably comes from (at least partly) the use of a cloud image to represent the Internet or some large networked environment. We don't care much what's in the cloud or what goes on there except that we depend on reliably sending data to and receiving data from it. Cloud computing is now associated with a higher level abstraction of the cloud. Instead of there being data pipes, routers and servers, there are now services. The underlying hardware and software of networking is of course still there but there is now higher level service capabilities available used to build applications. Behind the services are data and compute resources. A user of the service doesn't necessarily care about how it is implemented, what technologies are used or how it's managed. Only that there is access to it and has a level of reliability necessary to meet the application requirements. Cloud computing really is accessing resources and services needed to perform functions with dynamically changing needs. An application or service developer requests access from the cloud rather than a specific endpoint or named resource. What goes on in the cloud manages multiple infrastructures across multiple organizations and consists of one or more frameworks overlaid on top of the infrastructures tying them together. Frameworks provide mechanisms for:

- self-healing
- self-monitoring
- resource registration and discovery
- service level agreement definitions

In the context of distributed environments, data and applications are deployed at various geographical locations and needs to be available locally most of the time. Authentication is one of the key concerns in such environment. When a user accesses server programs remotely, the first important step is that the server must authenticate the fact that the client runs on behalf of a legitimate user. This fact also applies to the cloud computing paradigm. Cloud computing [1] makes easier for users to access services distributed across Internet. However, the cloud infrastructure is a bit different from traditional client/server infrastructure. Cloud is a dramatically evolving distributed environment, with which millions of users sign in more than one million supporting websites. Thus the authentication efficiency and manageability are the primary objectives. In short, to provide a secure and efficient authentication mechanism is important.

Usually, encryption and authentication are combined to provide stronger security to information. Encryption helps to ensure that information within a session is not compromised. In the past, authentication was almost synonymous with password based encryption [2] systems, where the key for authentication is derived from the password. But today's security system must do more, such as involving multi-factor authentication, and utilizing a large number of cryptographic objects, *etc*.. However, from a client's point of view, no matter how the authentication and encryption measures vary, convenience is as important as security. A secure but complicated solution would not be popular. While authentication provides proof of identity, encryption ensures confidentiality, but both do not describe the privileges an entry processes. This is called access control. To manage access control to encrypted content stored on distributed untrusted storages is a practical and challenging topic. Most access control models require a great deal of trust in the server operator. Should the operator prove unworthy of this trust, he or she could abuse the server's key material to decrypt any data stored on the system. Thus an access control mechanism with less trust on access server is preferable.

II. CONTENT STORAGE IN CLOUD COMPUTING

High-level architecture description of cloud data/content storage services is illustrated in Fig. 1. The architecture consists of four different entities: *data owner*, *user*, *cloud server* (CS), and *Third party Auditor* (*TPA*).

Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. Under the cloud paradigm, the data owner may represent either the individual or the enterprise customer, who relies on the cloud server for remote data storage and maintenance, and thus is relieved of the burden of building and maintaining local storage infrastructure.

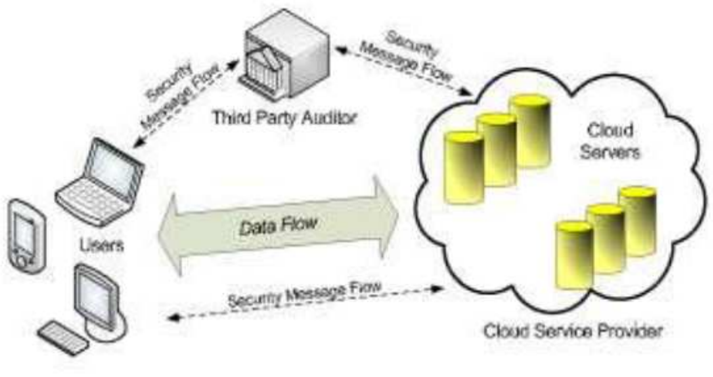

Fig. 1 Storage Architecture of Cloud Computing

In most cases cloud data storage services also provide benefits like availability (being able to access data from anywhere), relative low cost (paying as a function of need), and on demand sharing among a group of trusted users, such as partners in a collaboration team or employees in the enterprise organization [3,4].

III. SECURITY IN CLOUD COMPUTING

Cloud computing is becoming very popular computing paradigm for network applications in open distributed environments. In essence, the idea is to host various application servers in a virtual network environment (Cloud) and offer their use through the concept of (Web) and other services. Contrary to classical network applications approach in the form of client–server model, in a cloud environment users do not access individual application servers, do not establish direct connections with them, do not send request messages directly to those servers, and do not receive direct replies from them. Instead, clients access those application servers through cloud access proxies, special servers that perform publishing and exporting various (usually Web) services available in a cloud. In such environments, security has much more important role than in classical network, client– server, environments. Not only that the same, standard, security services are needed (authentication, authorization, confidentially, integrity, authorization, etc.), but their provision must be offered to clients transparently and in an environment comprising distributed components and delegated authorities. Cloud computing makes security not only much more important, but also much more difficult to organize and manage, due to the transparent nature of cloud resources, components, and services.

There are still many open and interesting issues regarding cloud computing paradigm and standards are still evolving. But, it is a general opinion that security is indeed one of the most important issues. In the recent IDC report over 74% of users think that security is dominant issue for widespread use of cloud computing services.

3.1 Major Risks of Cloud Computing Security

There are a lot of security issues in cloud computing service environments such as virtualization, distributed big data processing, serviceability, traffic-handling, application security, access control, authentication, cryptography and etc. Especially, data access using various resources needs user authentication and access control model for integrated management and control in cloud computing environments.

Cloud computing security is a hot topic for research, its freshness, interestingness and recognition created an appeal for researches to pursue this topic in specific. Many security concerns evolved while weighing the benefits of using cloud computing over local resources. Below are the major risks introduced by the cloud are:

- Data Storage
- Legal and Regulatory Risks
- Privacy and Confidentiality
- Availability
- Integrity
- Computationally feasible
- Proper usage metering
- Internal and external attacks
- Abusing cloud's resources

IV. PROPOSED SCHEME TO ENHANCE SECURITY IN DATA STORAGE

Encryption helps to ensure that information within a session is not compromised. Authentication and access control measures ensure legitimate and appropriate access to information, and prevent inappropriate access to such resources. While encryption, authentication and access control each has its own responsibility in securing a communication session, a combination of these three mechanisms can provide much better protection for information. So, this work proposed a enhanced approach using MD5 & UTF8 encrypting schemes. It also includes the signature & restricts the number of transactions per user to enhance the security.

4.1 Proposed Model

The proposed modal focuses on following three objectives which are helpful in increasing the security on content/data storage and are simulated by visual studio environment using Azure Cloud.

a. To propose Enhanced Security Scheme using MD5 & UTF8 Encoding Schemes.

b. To implement security by adding digital signature.

c. Restrict roles as per their transactions.

In this proposed work, admin has a single duty that is to make restrictions over number of transactions per user as per his role. After login, the user can upload the text or image data only if they have any transaction left. When user upload any type of data then it is saved at window azure cloud in encrypted form locked with digital signature.

4.2 Basic Block Design

Data Storage in Cloud Computing reached to very high level so; security is the need of the Cloud Environment. This proposed enhanced scheme use MD5 & UTF8 Encoding schemes & add signatures to lock the data for more security.

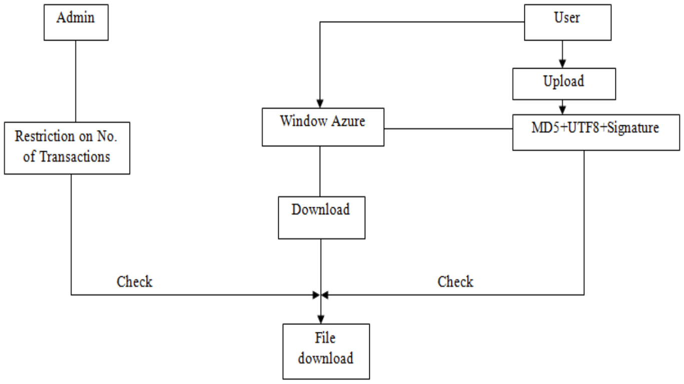

Fig 2: Basic Block Design of Proposed Work

This scheme is proposed to enhance the security in cloud data storage systems. The Block design of the proposed work is shown in Fig 2.

Admin: In an organization, admin create roles for users & also specify the number of transactions per user as per their role.

User: A user can upload/ download file. When uploading file MD5 & UTF8 Encoding schemes are used to encrypt data & digital signature is included to lock that data and when downloading file inverse MD5 & UTF8 are used to decrypt data & digital signature is used to unlock the file.

Window Azure: Window Azure Cloud is used to store data in the encrypted form.

4.3 System level Design

Fig 3 represents the system design of the proposed system with enhanced security scheme.

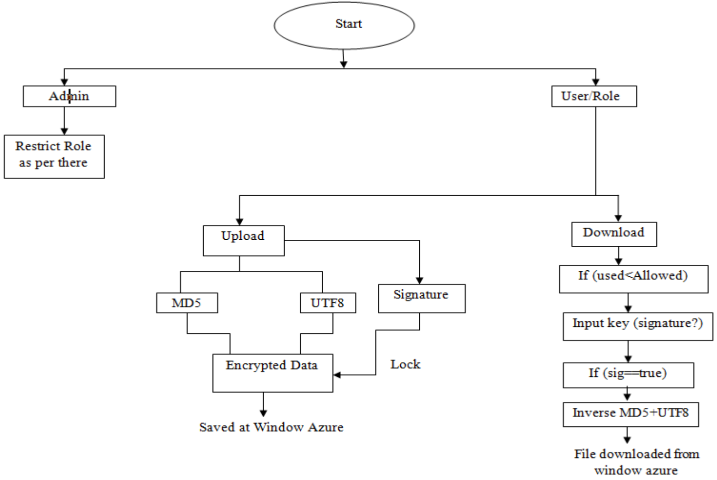

Fig 3: System level Design of Proposed work

In this proposed system, user can download the file only if it is valid user with valid number of transactions. If the user has no valid transaction left then he is unable to upload or download file. So because of this if in any case unauthorized person get access then he is not able to collect all the data means data lost will be less. In second case, if user has a transaction then he has to enter the digital signature to access or download the file.

V. RESULTS

This proposed model compare with the previous approach which uses a crossbreed algorithm and showing the results in Fig 4 and it concludes that this new enhanced approach using MD5 & UTF8 Encoding schemes with digital signatures having better results. It means security level can be enhanced or improved with the help of this new scheme. This new enhanced scheme increase the security by making restriction on number of transactions per user as their role, using MD5 & UTF8 Encoding algorithms and with digital signature and results that it increases security & reduces data loss as well as unauthorized access.

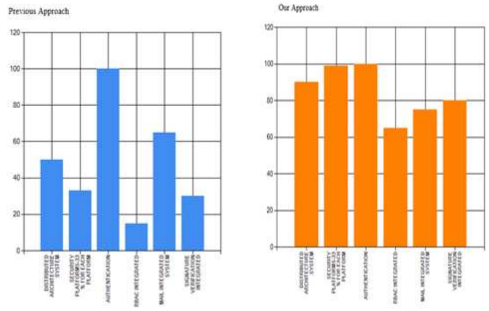

Fig 4: Previous Approach & Enhanced Approach

VI. CONCLUSION

In this paper, we proposed a security approach, which is Enhanced Security Approach, for the cloud computing network to increase the security level & prevent from unauthorized access. Similarly, this enhanced approach can achieve better results than the previous approach using crossbreed algorithm. It is expected that the data loss will be reduced by implementing the restrictions on number of transactions according the role of the user and enhanced the security using MD5 & UTF8 encoding schemes along with digital signature.

REFERENCES

[1] Academic Room. Cloud computing. www.academicroom.com/topics/cloud-computing.

[2] RSA Laboratories. Pkcs #5: Password-based cryptography standard.

[3] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[4] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in , cloud Computing", 2010.

[5] M. Sudha, Dr. Bandaru Rama Krishna Rao, M.Monica, „A comprehensive approach to ensure secure data communication in cloud environment‟ International Journal of Computer Application (0975-8887), Volume 12- No 8, Dec 2010.

[6] Palivela Hemant , Nitin.P.Chawande, Avinash Sonule, Hemant Wani,‟ Development of Server in cloud computing to solve issues related to security and backup‟, in IEEE CCIS 2011.

[7] Jianyong Chen, Yang Wang, and Xiaomin Wang, "On demand security Architecture for cloud computing", 0018- 9162/12, published by the IEEE Computer society in 2012.

[8] John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of cloud computing" published by the IEEE computer and reliability societies in July/August 2009.

[9] Nabendu Chaki, "A Survey on Security issue in Cloud Computing " in 6th International conference on Electrical Engineering/Electronics, Computer, Telecommunication and Information Technology, May 2009.

[10] Nils Gruschka and Meiko Jensen ,"Attack surface : A taxonomy for attacks on cloud services" in 2010 IEEE 3rd international conference on cloud computing.

[11] Cong.Wang and Kui Ren Wenjing Lou and Jin Li "Towards Publicity Auditable Secure Cloud Data Storage".

[12] Dr.R.Manicka Chezian and C.bagyalakshmi "a survey on cloud data security Using encryption technique" in International journal of advanced research in computer engineering & technology , Volume 1, Issue 5, July 2012.

[13] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in cloud computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume 2, Issue 3, July2012.

[14] Parsi Kalpana, Sudha Singaraju, "Data security in cloud computing using RSA algorithm", International

Journal of research in computer and communication technology, IJRCCT, ISSN 2278-58,Volume 1, Issue 4, September 2012.

[15] Salvatore J. Stolfo, Melek Ben Salem, Angelos D. Keromytis, "Fog computing: Mitigating Insider data theft attacks in the cloud".

[16] Jonathan Katz,"Efficient cryptographic protocol preventing man in the middle attacks", Doctoral Dissertation submitted at Columbia university, ISBN: 0-493-50927- 5,2002.

[17] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the Clouds : A Berkeley View of Cloud Computing, 2009.

[18] J. Shneidman, C. Ng, D.C. Parkes, A. AuYoung, A.C. Snoeren, A. Vahdat, and B. Chun, "Why Markets Could (But Don‟t Currently) Solve Resource Allocation Problems in Systems," Challenges, 2005, p. 7.

[19] A. Das and D. Grosu, "Combinatorial auction-based protocols for resource allocation in grids," Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International, 2005.