# Improved Storage Security Scheme using RSA & Twofish Algorithm at Window Azure Cloud

Amandeep Kaur[1], Sarpreet Singh[2]
[1]Research Fellow, [2]Asst. Professor
[1,2]Sri Guru Granth Sahib World University,Fatehgarh Sahib,Punjab.

***Abstract — Number of users stores their data on Cloud. Data storage security refers to the security of data on the storage media. So, Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. Data must not be stolen by the third party so authentication of client becomes a mandatory task. In this paper, we proposed a new security scheme by using RSA & Twofish algorithm. In this work, both these techniques help to generate a secure key & this key is sending to user by mail service. One more feature of security is added and that is Signature. In this when user stores their data they have to enter a unique signature which will make our scheme more secure and hence the new security scheme helps to increase the security at cloud.***

***Keywords*— Cloud Computing, Data Storage Security, RSA, Signature, Twofish, Window Azure.**

## I. INTRODUCTION

Cloud computing is growing fast with time. Cloud computing illustrate Information Technology as a fundamentally diverse operating model that takes advantage of the maturity of web applications and networks and the rising interoperability of computing systems to provide IT services. Data security is becoming a fundamental obstruction in cloud computing .There are some kind of solution that are provide some security with model, some technology.

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications.

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Cloud computing combines the data-sharing model and service statistical model. From a technical point of view, cloud computing has the following three basic characteristics [3]

- Hardware infrastructure architecture is based on the clusters, which is large-scale and low-cost. The infrastructure of cloud computing is composed of a large number of low-cost servers, and even the X86 server architecture. Through the strong performance, the traditional mainframe's prices are also very expensive.
- Collaborative development of the underlying services and the applications is to achieve maximum resource utilization. By this way, application's construction is improved. But for traditional computing model, applications to be complete dependent on the underlying service.
- The redundant problem among multiple low-cost servers is solved by the software method. Because of using a large number of low-cost servers, Failure between nodes cannot be ignored, so the issue of fault tolerance among nodes should be taken into account, when designing software.[3]

**Benefits**

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

• Cost Savings — Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.

• Scalability/Flexibility — Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also,

the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.

• Reliability — Services using multiple redundant sites can support business continuity and disaster recovery.

• Maintenance — Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.

• Mobile Accessible — Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

**Challenges**

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages.

• Security and Privacy — Perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment.

• Lack of Standards — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.

• Continuously Evolving — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving.

• Compliance Concerns — The Sarbanes-Oxley Act (SOX) in the US and Data Protection directives in the EU are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used. The EU has a legislative backing for data protection across all member states, but in the US data protection is different and can vary from state to state. As with security and privacy mentioned previously, these typically result in Hybrid cloud deployment with one cloud storing the data internal to the organization.

## II. Data Storage & Security in Cloud Computing

Cloud storage is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties, too. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualized the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. The safety of the files depends upon the hosting websites.

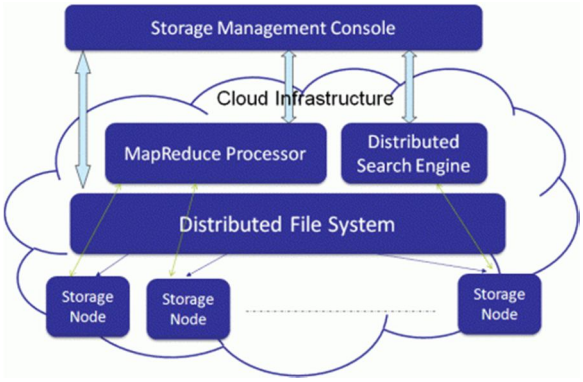


Fig 1: Cloud Storage Architecture

Cloud storage services may be accessed through a web service application programming interface (API), a cloud storage gateway or through a Web-based user interface.

Cloud storage is:

- made up of many distributed resources, but still acts as one
- highly fault tolerant through redundancy and distribution of data
- highly durable through the creation of versioned copies
- typically eventually consistent with regard to data replicas.

Data storage security refers to the security of data on the storage media, which means non-volatile or fast recovery after loss. This security should be taken into account by software engineers in design stage of cloud storage services. It includes not only data redundancy and dynamic, but also isolation. Redundancy is the most basic measures to protect

data storage security, and dynamic means user data may often change, so effective measures are needed to ensure data consistency. Isolation is that since different user's data is stored in the same platform, to guarantee the independence between the data, which means user can only access their own data, and data changes of other users will not affect the current user.

### 2.1 Data Security Issues in Cloud Computing

With the gradual promotion of the application, any private information in the facilities of the cloud computing may be found on any equipment. In order to protect the user's information from reveal, Siani Pearson put forward design principles in design process of cloud computing services to ensure that user's message and business information would not leaked out. It includes:

- Transmit and store user's information as little as possible. After systemic analysis, the cloud computing applications will collect and store the most necessary information only.
- Security measures will be adopted to prevent unauthorized access, copying, using or modifying personal information.
- Achieve user's control to the greatest degree. Firstly, it is necessary to allow the user to control the most critical and important personal information. Secondly, it is available to manage personal information by a trusted third party.
- Allow users to make choice. Users have the right to select the use of personal information. Besides, they can join or leave freely.
- Make clear and limit the purpose of use of data. Personal information must be used and handled by the person with specific identification for specific purpose and owner of information should be notified before using.
- Establish feedback mechanism to ensure that safety tips and detailed measures of the service will be provided to the user timely.
- It can maximize the security of user's data after introducing principles above.

## III. Proposed Scheme To Improve Security

In the Cloud Computing environment, important data, files and records are entrusted to a third party, which enables Data Security to become the main security issue of Cloud Computing. Cloud Computing is the buzz word of the tech industry right now when client is accessed data from the cloud. Data must be stolen by the third party, so authentication of client becomes a mandatory task.

In the current scenario, when the cloud computing is new to services, we are thinking about the safest server of this world. But as the time will move on there will be lot of different aspects which the hackers will see. At that time, we can't put our entire data to one server hence at that time a distributed architecture would be required which can share the data pattern. Our basic problem is to create a distributed architecture systems in which each and every system has a partial knowledge about the other network and when the all network will combine only then we can access the data. In the future if someone would try to access the data, he will have to hack each and every server and it would provide the administrator more time to save the system.

So, this work proposed new security scheme using RSA & Twofish encrypting schemes. It also mails the private key to user's mail id & add signature to each data file to enhance the security.

### 3.1 Proposed Model

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

a. Implementing the RSA algorithm of Encryption and Decryption.
b. Implementing the TWOFISH algorithm of Encryption and Decryption.
c. Implement mail method for sending private key to user's id.
d. Providing accurate data security by adding signature.

In this proposed work, the user can upload any type of data. When user upload any type of data then it is saved at window azure cloud in encrypted form using algorithm RSA & Twofish algorithms and locked each data file with signature.

### 3.2 System Design

Data Storage in Cloud Computing reached to very high level so; security is the need of the Cloud Environment. This proposed scheme use RSA & Twofish algorithm to generate a key & add signatures to lock the data each and every time for increasing security.

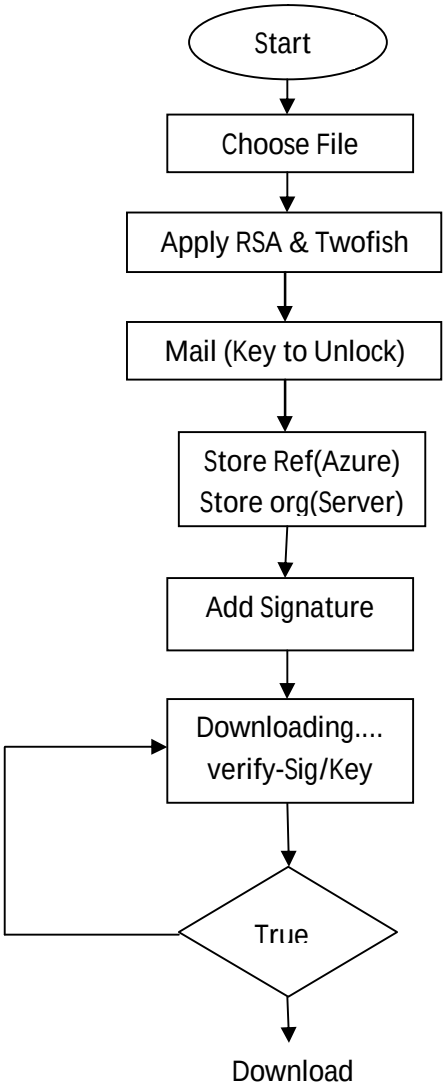


Fig 2: System Design for Proposed Work

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

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

**Mail Server:** When user upload data, then RSA generate a pubic key & a private key. This private key automatically picked by session but public key again encrypted by using Twofish algorithm and is sending to user by mail service. This key is used when user download their content or data.

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

### 3.3 Algorithm level Design

Fig 3 represents the algorithm level design of the proposed system with improved security scheme.

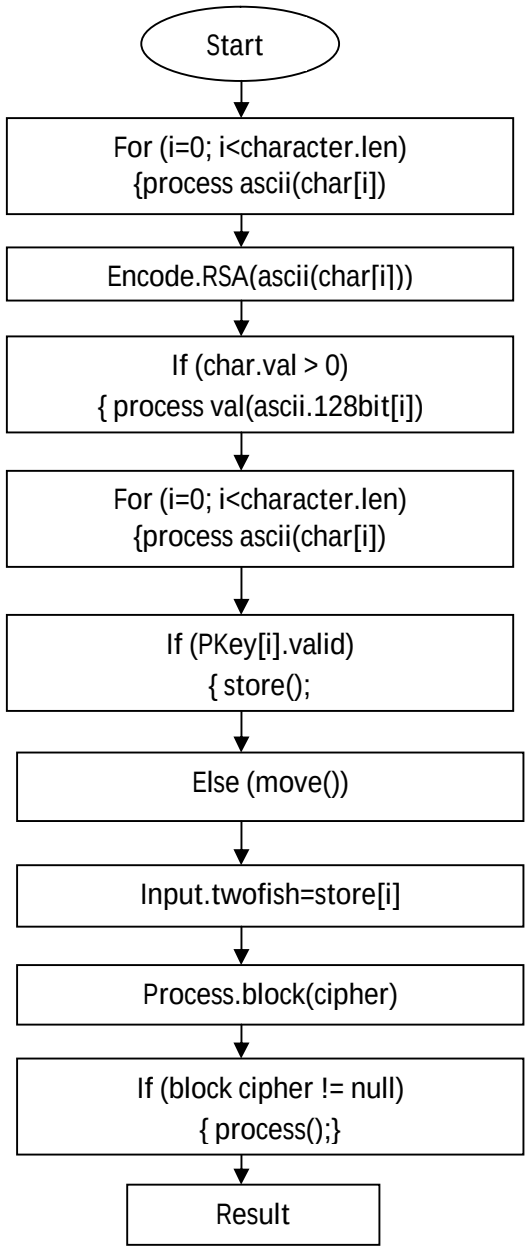


Fig 3: Algorithm level Design of Proposed work

In this proposed system, user can download the file only if user has a valid key with valid signature. If the user has no valid signature then he is unable to download file. So because of this no unauthorized person get access & no one is able to collect the data means no data loss.

## IV. RESULTS

This proposed model compare with the previous approach and showing the results in Fig 4 and it concludes that this new improved scheme using RSA & Twofish algorithms with signatures having better

results. It means security level can be increases or improved with the help of this new scheme. This new enhanced scheme increase the security by using private key generated with RSA & Twofish algorithms and with signature and results that it increases security & reduces data loss.

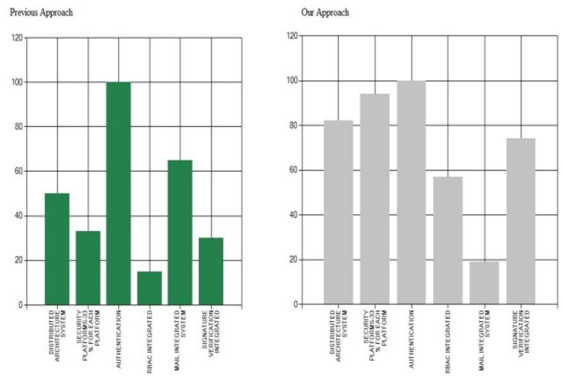


Fig 4: Previous Approach & New Approach

## V. CONCLUSION

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. In this paper, we proposed a security approach, which is improved Security Approach, for the cloud computing network to increase the security level & prevent from unauthorized access. Similarly, this approach can achieve better results than the previous approach. It is expected that the data loss will be reduced and increased security using RSA & Twofish algorithm's private key along with signature.

## REFERENCES

[1] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "*Ensuring Data Storage Security in Cloud Computing*", In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.

[2] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "*Cloud security issues*" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.

[3] J. Brodkin. Gartner: "*Seven cloud-computing security risks*", Infoworld, 2008.

[4] Vamsee Krishna and Sriram Ramanujam," *Data Security in Cloud Computing*", Journal of Computer and Mathematical Sciences,vol. 2, Issue 1, 28 February, 2011.

[5] Hassan Takabi, James B. D. Joshi and Gail-JoonAhn**,** "*Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments*" Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops, p.393-398, July 19-23, 2010.

[6]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.

[7] 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.

[8]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.

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

[10] Jintao Liu,School of Electronics and Computer Science University of Southampton, "*Cloud Computing Security*" ,2009.

[11] Er. Rimmy Chuchra,Lovely Professional University,Phagwara, India, "*Data Security in Cloud Computing*", International Journal Nov.,2012.

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

[13] 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.

[14] 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.

[15] Uma Somani, KanikaLakhani, Manish Mundra,*"Implementing Digital Signature with RSA EncryptionAlgorithm to Enhance the Data Security of Cloud in Cloud Computing"*, in 2010.