

# Data Security Approach in Cloud computing using SHA

Prabhleen Kaur Soul<sup>1</sup>, Sunil Saini<sup>2</sup>

<sup>1</sup>RESEARCH SCHOOLAR

<sup>2</sup>ASSISTANT PROFESSOR

Dept. of Computer Science and Engineering KITM Kurukshetra Haryana, India

\*\*\*

**Abstract** The main idea behind this paper is to provide integrity to the cloud storage area. In order to provide security in cloud computing we use SHA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system. 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. The main goal is to securely store and manage the data so that only authorized users can have access over the data.

**Key Words:** SLA,AES, DES ,HTTPS

## 1. INTRODUCTION

Cloud computing is considered as major part in a business for fulfilling the request at low cost. It is an internet based computing where application, platform, infrastructure are provided as services [2]. The main concept of this technology is that, the customers pay only for those services which used. Resources can be allocated geography anywhere and can provide any type of service that a user wants. Now user needs not to have any type of physical infrastructure. He/she has to just use the services of this technology and pay according to usage of services.

Cloud computing is a novel type of prototype, is coming. This term is a novel term that seems by the fourth season, 2007. The custom of internet and novel knowledge's today, for commercial and designed for the present consumers, is previously portion of daily lifespan. Slightly info is obtainable wherever in the domain at marginally time. That was not probable little ages before. Today it have ascended a lot of potentials of admission to open and isolated info similar to internet speed admittance or the setting out of portable dispositive that permit the linking to internet from virtually universally. Cloud computing discusses[3] to the provision of computing resources concluded the internet. In its place of custody information on your

individual hard drive or apprising requests for your requirements, you practice a facility through the internet, at alternative place, to accumulate your info or use its requests. Doing so can provide increase to convinced confidentiality insinuations. This computing technology is the distribution of facilities through the net. Cloud facilities permit persons and companies to custom software and hardware that are achieved by other peoples at faraway sites. Instances of cloud facilities comprise on the web document stowage, communal interacting sites, webmail, and online commercial services. This computing technology archetypal lets right to use to info and computer servers from wherever that a network linking is offered. This computing technology delivers a common puddle of servers, comprising infor stowage space, networks, computer processing power, and specific business and consumer requests.

## II. Characteristics of Cloud Computing

The characteristics of Cloud computing [5] which explains its relation and difference from the traditional computing are given below:

- **Virtualization:** Virtualization refers to the abstraction of computer resources (CPU, storage, network, memory, application stack and database) from the applications and the end users consuming the service [6]. It is a technique which multiplexes the hardware resources and enables the users to run multiple operating systems on same physical hardware. This technology helps in slicing a single data center or high power server to act as multiple machines. The number of virtual machine, a system may be divided depends upon the hardware configuration of system.
- **On-Demand-Self Service:** Consumer can provision or un-provision the services when desired, without the human interaction with the service provider. Whether it is software, platform or infrastructure everything is offered as a service over the network.

- **Elasticity:** With elasticity, the user is able to acquire more resources in an on demand manner, for a small duration and pays for the capacity or capability they need. When those resources are no longer needed, the user is able to return that capacity.
- **Location Independence:** Enables the users to access the systems using a web browser regardless of their location or what device they use (PC or mobile phone). The services are provided to user residing at any part of the world using their smart phones, laptops, tablets and office computers. These devices can be used wherever they are located with a simple online access point.
- **Multi-tenancy:** The cloud providers serve the multiple companies on same infrastructure and software. This approach is more energy efficient than multiple copies of software installed on different infrastructure [7].
- **Autonomic:** To provide highly reliable services, Clouds exhibit autonomic behavior by managing themselves in case of failures or the performance degradation.
- **Measured Services:** Due to affordable nature of cloud, the user can pay on a pay as peruse model. The cloud provider can measure the levels of storage and processing, bandwidth and the number of user accounts which can be billed accordingly.
- **Maintenance:** Maintenance of cloud computing is easier because they do not need to be installed on each user's computer and can be accessed from different places.
- **Interoperability and Portability:** As the cloud environment is highly dynamic to user requests and due to the concept of virtualization, the leverage of migrating in and out of the resources and applications should be allowed. Also, switching providers should switch between clouds as per their need, and no lock-in period should exist.
- **Reliability and Availability:** Cloud providers still lack in round-the-clock service which results in frequent outages. Therefore, it becomes important to monitor the service being provided using internal or third party tools.
- **Automated service provisioning:** A key feature of cloud computing is elasticity; resources can be allocated or released automatically. So a strategy is required to use or release the resources of the cloud, by keeping the same performance as traditional systems and using optimal resources.
- **Performance and Bandwidth Cost:** Businesses can save money on hardware but they have to spend more for the bandwidth. This can be low cost for smaller applications but can be significantly high for the data-intensive applications.
- **Virtual Machines Migration:** With virtualization technology, an entire machine can be taken as a file or set of files. To unload a heavily loaded physical machine, it is required to move a virtual machine between physical machines. The main objective is to distribute the load in a datacenter or set of datacenters. Then a strategy is required to dynamically distribute load when moving virtual machine to avoid bottlenecks in Cloud computing system.

### III. Challenges of Cloud Computing

The following are the challenges faced by cloud computing environment [10]:

- **Security and Privacy:** It deals with securing the stored data and to monitor the use of the cloud by the service providers. This challenge can be addressed[9] by storing the data into the organization itself and allowing it to be used in the cloud. So the security mechanisms between the organizations and the cloud need to be robust.
- **Service Delivery and Billing:** The service level agreements (SLAs) of the provider are not adequate to guarantee the availability and scalability as it is difficult to assess the cost involved due to dynamic nature of services.

- **Energy Cost:** Cloud infrastructure consumes enormous amounts of electrical energy resulting in high operating costs and carbon dioxide emissions [10].

### IV. Purposed Work

The purpose of the work is to inspect the safety restriction and focus the present dangers trendy cloud computing real safety procedures intended for cloud computing schemes. It determination contribution the academics to categorize safety provisions by several stages to distinguish the fears in the numerous cloud computing prototypes modeled by mutually interior and exterior customers. Therefore, it will beneficial to

explain cloud safety protocols that guarantee the safety of the cloud environment.

Although cloud computing has been widely used, the research on resource management in cloud environment is still an early stage. The main objective of the research work is to investigate the relevant efficient and enhanced resource utilization approaches for cloud based system. A brief description of the work to be carried out is as under:

- Scheme will be developed to maintain the integrity of information exchange between participating systems.
- Scheme will be developed to authenticate the participating system involved in communication.
- Scheme will be developed to ensure the confidentiality of the information exchanged between participating systems.
- A secure model will be developed which will comprise the above developed schemes.

Similar to entire computing schemes, cloud computing organizations essentially reveal safety problems since the early phases i.e. requests phases and project phases of its improvement procedure. It resolve principal to an extra vigorous, safe and fewer errors willing to system than those systems that categorize safety substances only on one occasion, once the scheme is addressed. Owing to the difficulty of the cloud environment, actual progress of a cloud computing scheme desires an inspection of these safety difficulties and precondition thus frequent approaches might be recognized prior in the expansion procedure that drive reflect the complete cloud. In cloud computing environs, inner fears have gradually improved above the previous little ages. Inner hazard depicts to individuals fears which monitor inside the association. Inside customers in a connotation usually have extra info of the data reserved there in and in future, extra well-informed about how to charge that information and requirements than do external customers. While inside fears cannot be totally detached, some actual fences can be developed to ease them.

#### 4.1 Symbolization and Initiations

- FEncode: This is a script document that subjects the encoded information and document is kept in CSP3.
- FTemp: It is determined through information handling period (recovery process and drive to be free) and this one is a provisional document.
- Gen\_Key(): This produces a protected key.
- Ks: This is a key which is produced through Gen\_Key procedure in CSP-2.
- Encoding (): This is encoding procedure to encrypt document.
- Decoding (): This is a decoding procedure to decipher document.

This procedure negotiates of numerous additional rules. The customers interrelate over the gateway server over HTTPS procedure to upload their information. The Docker repository clustering procedure Docker Swarm obligates the situation superior arrangement on gateway server. Thus document send by customer is directly promoted towards a nodule of the swarm collection wherever swarm supervisor leads an indication to introduce a repository and the information drive be equestriennes arranged it and the repository will procedure open SSL procedure to encode the information through AES, RSA or some supplementary typical encoding procedure. As quickly as the encoding is complete, the repository dismisses and the encoded information is haggard back towards the gateway server besides previously endorsed towards the stowage server. The document is stimulated after gateway server to additional knots and servers through SSH procedure. The stowage server obligates a collection of Docker nodules successively that receipts disk space after the chief scheme. Glusterfs procedure is castoff to band the information interested in numerous pieces and also duplicates it to a reserve nodule uncertainty some and accumulation it on the repository collection. In circumstance, the customer stresses to transfer his information he sets an appeal over HTTPS on gateway server and at that time the gateway server recovers the document from the stowage server and forward it to its nodule for

decoding that includes similar procedure as encoding. The decoded information is dragged after the gateway server and then accessible for the customer to get it.

Our suggested arrangement has two key assistances:

1) Effectiveness and safety: - The strategy suggested through the innocuous is to depend on a unrestricted and reserved key encoding will be clear, effective in the practice of undisclosed key gen and Hash procedure. Therefore each interval constraints are produced and key interchange proceeds place so extra protected than symmetric and asymmetric procedure. Though, our strategy is supplementary effectual than the other procedures, since, it does not need a lot of information encoded in subcontracted and not any extra supports on the representation chunk, and proportion is supplementary protected since we encode information to avoid illegal third revelries to distinguish its subjects.

2) Open verifiability: We strategy a main difference to deliver free authentication. Permit, person supplementary than owner for info on the server has verified proficient since it does not require the info for individual chunk encoding.

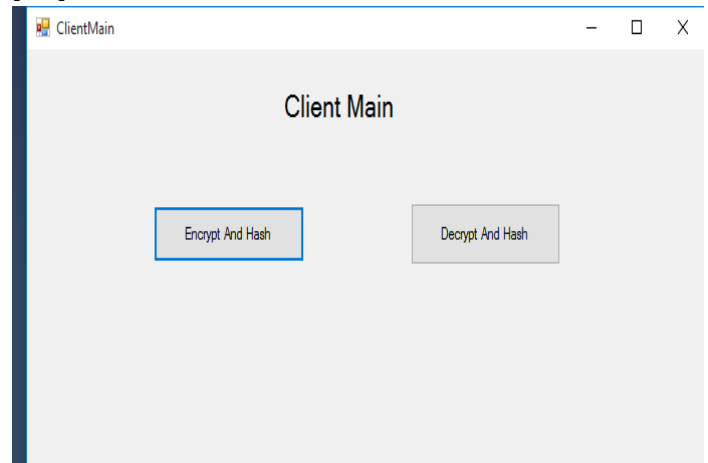
### V. Result Analysis

Implementation is the phase of the development at what time the conjectural proposal is revolved out into a functioning method. Therefore it can be reflected to remain the maximum precarious phase in attaining an effective novel scheme and in giving the customer, sureness that the novel system wills effort and stay operative. The operational phase includes suspicious preparation, examination of the present system and it's limitations on execution, conniving of approaches to accomplish exchange and assessment of exchange approaches.

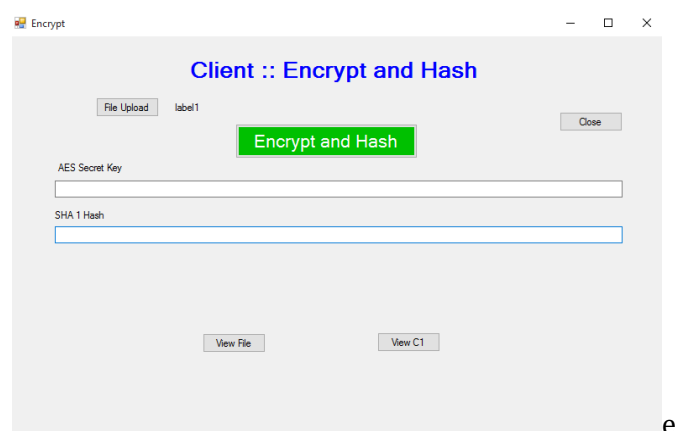
Here, our goal is to measure the Encryption and Decryption speed of each algorithm for different packet sizes. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased,

the power consumption of this encryption technique is decreased. By considering different sizes of data blocks (0.5MB to 20MB) the algorithms were evaluated in terms of the time required to encrypt and decrypt the data block. All the implementations were exact to make sure that the results will be relatively fair and accurate

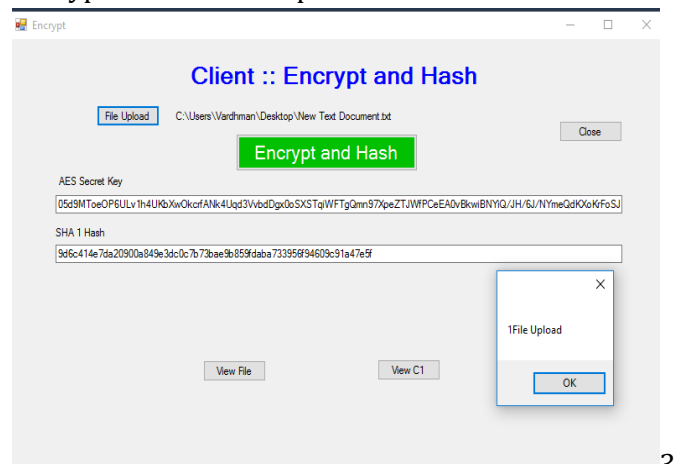
Firstly open the .NET. Encrypt and hash for encryption purpose.



File successfully uploaded” after uploading of file.

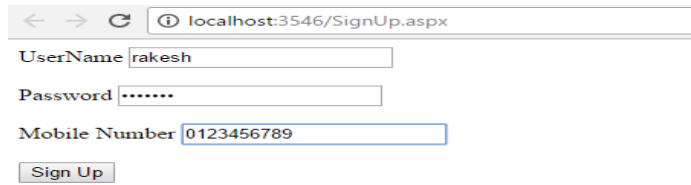


encrypted file of that uploaded file.



fields username, email id and mobile number of the

user which are used earlier .



Now we have to choose the file which is to be uploaded by clicking on choose file button. Then click on upload file button to upload it.

## VI. Conclusion and Future Scope

In this proposal, we have offered a summary of information stowage safety in cloud computing and projected a frame constructed on encryption system. To guarantee the safety of customers' information in cloud stowage, we planned an operative and effective encryption approach for improving safety on data-at-rest. We have presented that our arrangement nearly assures the safety of information when it is kept in the information center of some Cloud Service Provider (CSP). It will assist to construct a ideal to protect the information in the arena of cloud calculation. This architecture is capable to expand the client fulfillment to a countless degree and it will appeal numerous nominees in this arena for developed as well as upcoming investigation farms.

## REFERENCES

- [1] Aderemi A. Atayero, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", In Journal of Emerging Trends in Computing and Information Sciences, Vol-2, No.10, pp.546-552, October 2011
- [2] Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue, "Security Issues and Solutions in Cloud Computing". In 32<sup>nd</sup> International Conference on Distributed

Computing System Workshops, pp.573-577, 2012 (2012)

[3] W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah, M.t. Abdullaha, "Cloud-Based Intrusion Detection Service Framework". In the Proceedings of the International Conference on Cyber Security, pp. 213-218, IEEE, June 2012 .

[4] Abhishek Jain, Ashwani Kumar Singh, "Distributed Denial of Service (DDoS) Attacks – Classification And Implications". In Journal of Information and Operations Management, ISSN: 0976-7754 & E-ISSN: 0976-7762, Vol. 3, Issue 1, pp 136-140, 2012

[5]<http://www.symantec.com/connect/articles/justify-ing-expense-ids-part-one-overview-rois-ids>

[6]<http://netsecurity.about.com/cs/hackertools/a/aa030504.htm>

[36] Sanjay B Ankali, Dr. D V Ashoka, "Detection of Request Layer DDoS Attack for Internet". In International Journal of Advanced Networking and Applications, Vol-o3, Issue: 01, pp. 984-990, 2011.

[7]S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A.Ghalasi, "Cloud Computing- The business perspective", Decision Support Systems, Vol. 51(1), pp. 176-189, 2011.

[8]The NIST Definition of Cloud Computing, <http://csrc.nist.gov/publications/nistpubs/800-SP800-145.pdf>.

[9] I. Brandic, "Towards self-manageable cloud services", IEEE International Conference on Computer Software and Applications, pp. 128-133, 2009.

[10] M. Alhamad, T. Dillon and E. Chang, "A survey on SLA and performance measurement in cloud computing", On the Move to Meaningful Internet Systems: OTM 2011, Springer Berlin Heidelberg, pp. 469-477, 2011.