LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

A Research Paper Writing Proposal

Data Storage Security: A Challenge in Cloud Computing

Submitted To:-

Mr. Kumar Vishal

Submitted By:-

Jatin Roy	(11401078)
Vishal Kumar	(11404028)
Pawan Kumar Kumawat	(11412290)
Ankit Kumar Sharma	(11412004)

Certificate

This is to certify that Jatin Roy (11401078),Vishal Kumar (11404028), Ankit Kumar Sharma (11412004) and Pawan Kumar Kumawat (11412290) have completed their MCA(Hons) Research Paper Writing Proposal titled “Data Storage security: a challenge in Cloud Computing” under my guidance and supervision. To the best of my knowledge, the present work is the result of their original investigation and study. No part of the dissertation proposal has ever been submitted to any other degree or diploma.

The proposal is fit for the submission and the partial fulfillment of the conditions for the award of the degree of Master in Computer Applications.

Date ----------------------------- Signature of the Advisor

Name:

Declaration

We hereby declare that the research paper writing proposal entitled, “**Data Storage security: a challenge in Cloud Computing**”, submitted for the MCA(Hons) Degree is entirely our original work and all ideas and references have been duly acknowledged.

It does not contain any work for the award of any other degree or diploma**.**

Date:

Jatin Roy	(11401078)
Vishal Kumar	(11404028)
Pawan Kumar Kumawat	(11412290)
Ankit Kumar Sharma	(11412004)

Acknowledgement

We would resembling to precise our obligations of thankfulness to our **Guide Mr. Kumar Vishal Sir** who provided us the golden prospect to do this magnificent assignment on the research topic “**Data Storage Security: a challenge in Cloud Computing”**, it also aided us in undertaking a lot of Exploration & we arose to identify approximately so numerous belongings we are truly pleased to them.

Secondly we would also like to thank our parents, faculties and friends who helped us a lot in finalizing this project within the limited time frame.

Introduction

Cloud computing is an emerging technology which provides computing service with the help of internet on request and on pay per use access to a puddle of joint of resources which consists of services, servers, networks storage and applications, these are not actually present with the user of this service. It helps in saving the cost of management and time for organizational process. Various organizations such as education, finance, even automobile, health care are using the cloud technology due to the productivity and effectiveness of services delivered by the pay per usage arrangement which is based upon the various resources such as processing power used, bandwidth consumption, transfer of data, or room space occupied, transactions carried out etc. Cloud computing is totally dependent on internet technology where data or files of client is stored and maintained in the data premise of a cloud providers like Salesforce.com, Amazon, Google and Microsoft etc.

Cloud computing is not a much unknown thing at the present time; it is being used by so many people around the globe who stores their data on it after acquiring it on reasonable price. Most of the companies in the world providing this facility globally, and these are the things that a hacker always in seeks off. Cloud computing works with internet connection which makes it most risky and the vulnerabilities is just another truth part of every technology. Cloud computing based servers are just like a Sundae Ice creams, consisting of so many data from different fields, which attracts the hackers and crackers creating security and data storage issues. One of the most essential phase bring up to security: whereas certain security in cloud computing concerns are in born from the results accepted to develop such facilities, still various new questions arises related to security those are specific to these results, comprising those associated how the facilities are structured and which kind of file or the data could be located in the cloud.

The cloud computing also possesses challenges which are based on securing the integrity and privacy of data owners in cloud. For resolving these issues, our work makes use of the technique which is based on secret key algorithm which allows TPA to carry out the auditing process without requesting the copy of user’s data stored in cloud. TPA is a kind of examiner. There are two types of classifications: public auditability & private auditability. Though private auditability could bring about greater scheme effectiveness, the public auditability authorizes any person, not only the owner of data to test the server of cloud for purpose of accuracy of stored data despite the fact of holding no private data. In order to decrease the load of data owner for management of data, the data of owner will be audited by TPA. Third Party auditor will assist the owners of data to get assured that their data is secure in the cloud and the data management will be quite normal with lesser complexity to the data owners.

Problem Background

The control over the data is limited which may cause several security issues which include distribution of resources, unsecure interface, outflow of data, confidential attacks and availability of data, other research challenge for migrating towards cloud computing include well managed service level agreement(SLA), interoperability, privacy and reliability. The servers based upon cloud computing have been attacked by so many different techniques in past few years. The most known techniques used by hackers/attackers are Sybil, Vendor Lock-in, Malware Injection, Hijacking, DDoS (Distributed Denial of Service).

Users of cloud technology generally don’t physically maintain the storage of their data for longer period, so in order to provide protection on data security , the customary cryptographic primitives cannot be straightly adopted. So for efficiently verifying the accuracy of outsourced cloud data without the native or local copy of the data files becomes a crucial challenge for security facets of data storage in Cloud.

The existing algorithms are not much efficient and reliable for providing end to end security to data from hackers. Most common practice the hackers use via cloud computing is attack of data intrusion and data breaching. Data breach is very familiar now days, every hour so many attacks were being caught by cloud computing providers. Still few cloud storage providers are not providing the storage of data in encrypted format which is a crucial aspect in term of data security. If some of the cloud storage providers are providing the storage of data with encryption, they are doing this with storing the encryption/decryption key which is linked up with stored data which can easily be accessed by attackers which will result in accessing the data. Data loss is another part of data breaches when user lost his encryption key and when the attacker modifies that data by gaining access to the server.

Literature Review

In paper[1] the authors Rabi Prasaad Padhey, Maanas Ranjan Patraa Suresh Chandra Sataapathy have described that the control over the data is limited which may cause several security concerns which include outflow of data, unsecure interface, resource distribution, availability of data and inside attacks. The authors of this research paper have clearly stated about the various models of cloud, security risks and problems that are faced by cloud computing companies. This paper examines the essential research and experiments that exists in cloud computing technology such as data security, security aspects of network and virtualization and provided best practices to service providers and also enterprises which are opting the cloud technology in order to get advantage of cloud service to increase the growth of the company.

In paper[2] the authors D.Pratiba, Dr.G.Shobha have described that the auditability for cloud data storage security is of essential importance by which users would be provided with an option of an external audit party to verify the integrity of outsourced information once required. Threshold-multisignature scheme and Third Party Auditor are used for the above mentioned purpose. This paper suggests a privacy-preserving public auditing[2] system for providing security on storage of data in cloud computing, where the party which is auditing can accomplish the storage auditing deprived of demanding the native copy of data. This paper also describes the basic attributes of threshold-multi signature schemes and describes that the suggested scheme fulfill these attributes and eradicates the current attacks to which other related schemes are subject.

In paper[3] the authors Nelson Gonzzalez, Charlees Miers ,Fernanndo Redeıgolo ,Marccos Simpl´ıciooand, Makaann Pourzandi have recognize the important problems and have grouped them into model which is formed from seven categories such as interfaces, virtualization, network, security of data, security authority, compliance, and legitimate concerns. They have set up test beds using OpenNebula and have explored aspects of security and also the virtualized servers which are based on VMware using test bed networks. The analysis lead to a large exploration of PaaS results, and permitted them to validate that mainly they use virtual machines supported virtualization technologies like XEN, VMWARE, and KVM, which frequently lack concerns of security, they also stated that Amazon modified the source code of XEN to incorporate safety attributes, however the changed code isn't accessible in public and there seems to be none article describing the modifications introduced.

In paper [4] the author Dr. Sunil Batra, has described that Cloud computing is a mixture of technologies evolved over the years, but it has also accepted sufficient amount of vulnerability issues. Vulnerability can be defined as, by using the information of securing went in to wrong hands which use that in creating a loop hole in the system to breach the data.

In paper [5] the authors Yanpeichan, Vern paxson, Randy H. Katz, described that, few of the cloud security issues are fundamentally new or intractable. Mutual auditability key concept must be discussed in brief so that the data providers and users must be in a reciprocal trustworthiness. Security shows main issues for the extensive acceptance of cloud computing, on the other hand either the data is secured or not, cloud computing still exists from a long time. Security is the key challenge in cloud computing, so much vulnerabilities in cloud still exists had hackers continue to exploit these security holes. The best way to secure the cloud computing is to search the security holes and healing them by using effective security concepts.The authors have described that the past reminds that the emerging security designs early in the development can pay off significantly as systems evolve and accumulate more dissimilar functionality.

In paper [6] the authors Mahimaa joshi & Yudhveer Singh Moudgil has refer to the problem of constructing a top level of protected cloud storage service where the service provider is not trusted by the users. A high level architecture must be created, by combining recent and nonstandard cryptographic primitives. The architectures should definitely provide benefits to both users and service providers and give an analysis of recent advance study in cryptography. Many company access the best performance. Several major changes in cloud computing is done to store the different-different information and also run able application. There are two phases first is platform as services (PaaS) and second is software as a services (SaaS), these platform provide help to customers. Cloud storage provider does not know any detail about customer, in a private cloud the data is managed and owned by consumer and located on foundation and in public cloud the data is owned and managed by a cloud service provide and is located on premise. The author has mention that consumer data is away from the boundary of its control and could be generated by itself to untested party.

In paper [7] the authors Neha Tirthaani, Ganesan has described that there are few important policy and these include issues of privacy, anonymity ,security ,liability and reliability and one of the most important issue is data security and the most effective way to remove this problem is to protect all data is doing data encryption. Authors of this paper have discussed about the safety threats such as preservation of the data reliability, whacking of the data and data protection. The large data and time intense encryption calculation related to apply any encryption method have been proved as obstruction in this field. They have considered a design for cloud structural design which ensures progress of data at server and client end. They used non instability of Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism for connection and organization.

In paper [8] the authors Deyan Chen and Hong Zhao have stated about providing a concise but all-round analysis on security of data and privacy safeguarding issues, the basic challenges are division of active data and authorization personnel. Authors aim is to design a set of balance identity management and privacy protection structures across applications or cloud storage service related with cloud computing across all levels of data life cycle. The first advantage is that data security is prior as data is saved on online stage, Secondly the demolition, when the data is no longer required it can be destroyed and if required it can be restored and mention disadvantage the challenges in the privacy issues subsist everywhere. While dividing the data but it is calculated for data security and privacy protection issue is to design a site of integrated identity management and privacy protection framework across application or cloud computing services.

In paper [9] the authors, G.L Varaprasad, Sumathi Karanam, P.Venkata SubbaReddy have implemented the cloud storage security mechanism. This will consider cloud structural planning with three gatherings in particular such as cloud service provider, third party auditor and cloud client. The third party auditor is capable to monitor all exchanges for check of reliability. The two difficulties determined in this arrangement were the capability to provision various check at once and the capability to provision request block authentication for reliability and also the third party auditor is proficient to equipped TPA services to the community. The authors assembled a model, a convention Java simulator that exhibits the evidence of concept.

In paper [10] the author C. Balasubramnian, T. Prasanthi, S. KimssukhaSelvi, K. Kala has implement the Auditing Protocol for Secure Data. They theoretically overdrawn down and uncertainly tried the effectiveness of the integrity preserving protocol. The cloud storage system model consists of the following main three entities as illustrated. They are- Client: The consumer, who is an single client or an association, cravings to store and access their huge amount of information in the cloud. Cloud Service Provider: The CSP, who deals with the cloud servers and gives storage as service on its base to the cloud clients taking into account pay every service basis. Third party Auditor (TPA): The TPA, who reviews cloud information for the client furthermore confirms the capacity accuracy of information being outsourced from the cloud.

In paper [11] the author Ashish Badiye, Neeti Kapoor and Pooja Shelke have described the specific security issues:- Privileged user access: outsourced services bypass the "physical, logical and personnel controls" which causes data loss and breach the confidentiality of data. The approval of users and authentication of data must be done. Data location: while using the cloud server users are unaware that where the data is actually going to store. Leaking of this information is harm to data. Data segregation**:** The encryption techniques which were been used by the cloud storage providers where must be designed and checked by professionals. Encryption calamities can make data entirely unusable and done to segregate data at rest. Recovery: recovery of data on a failure or server crash cause loss of data, in that case, the recovery of data is main concern. Investigative support**:** when hackers are using the cloud servers for doing some anonymous work in that case investigating entire server for that data is not a possible work. Long-term viability: Keeping backup for such an event when the cloud service providing company get acquired by big companies, in such cases, the Backup of data must be kept.

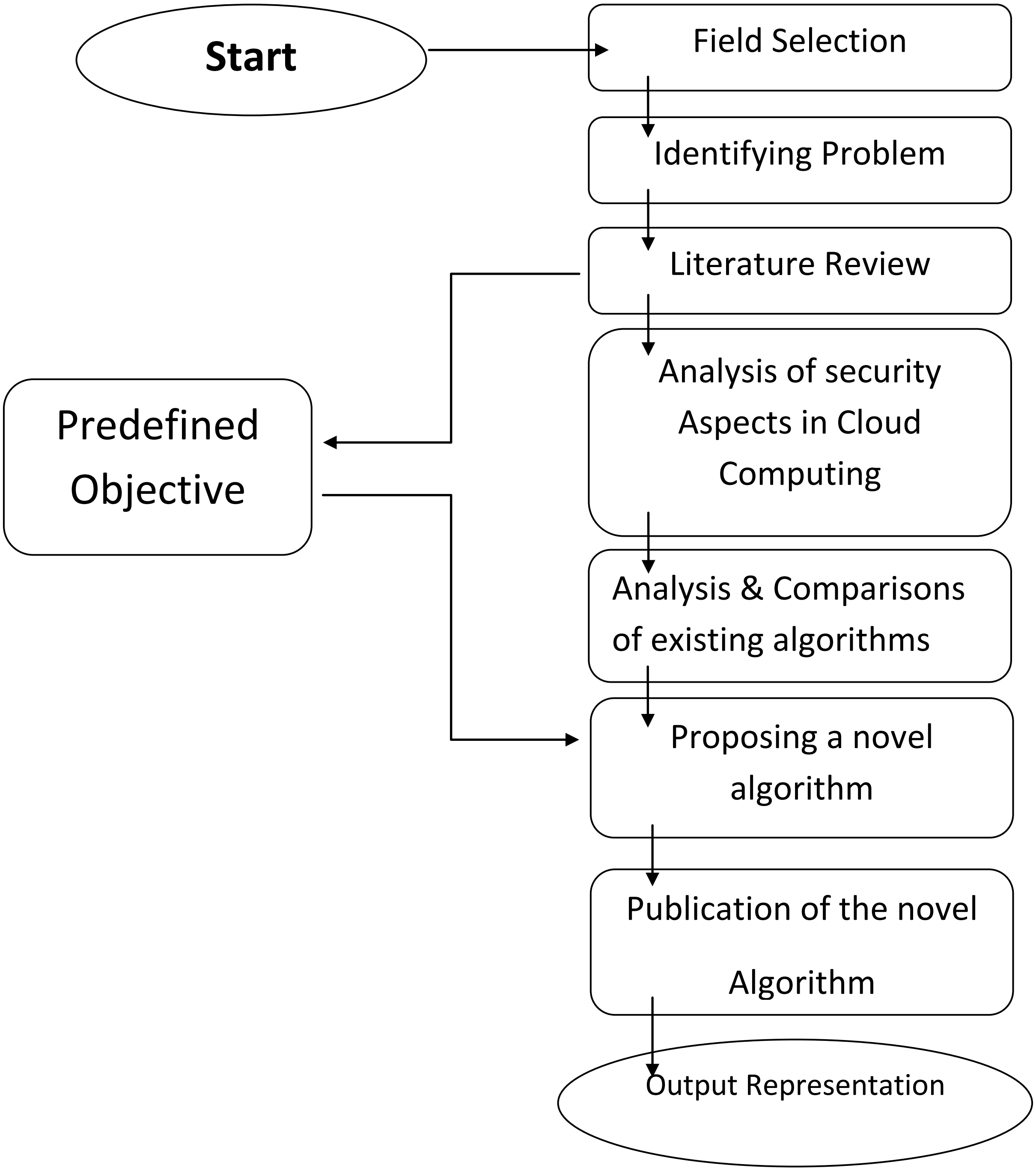
Objectives of the Study

The major objectives of our topic of research are as follows:

- To get knowledge about different security aspects of cloud computing which should further expand the scope of research in a broad way.
- To analyze the existing algorithm which are based on providing the security in cloud computing.
- To compare the existing algorithms which are already providing security for storing data in cloud on the basis of various parameters such as key length, security, speed and block size.
- To eradicates the participation of the data owner by inspecting that whether the data of owner kept in cloud are certainly unbroken, and also to support data owners to be certain that their data are secure in cloud.
- To devise a novel algorithm for providing more efficient and reliable security for storing the data in the cloud server.

Research Methodology

A research study consists of two different aspects Secondary and Primary sources. The collection of data for research study is done by both Secondary and Primary. Secondary data have some operational features which describes that data already exist and is easily available. And it is versatileto a certain extent and can be used in several purposes. The future research consists of Primary data as per our experimental results.


Start
Field Selection
Identifying Problem
Literature Review
Analysis of security Aspects in Cloud Computing
Predefined Objective
Analysis & Comparisons of existing algorithms
Proposing a novel algorithm
Publication of the novel Algorithm
Output Representation

Expected Research Outcomes

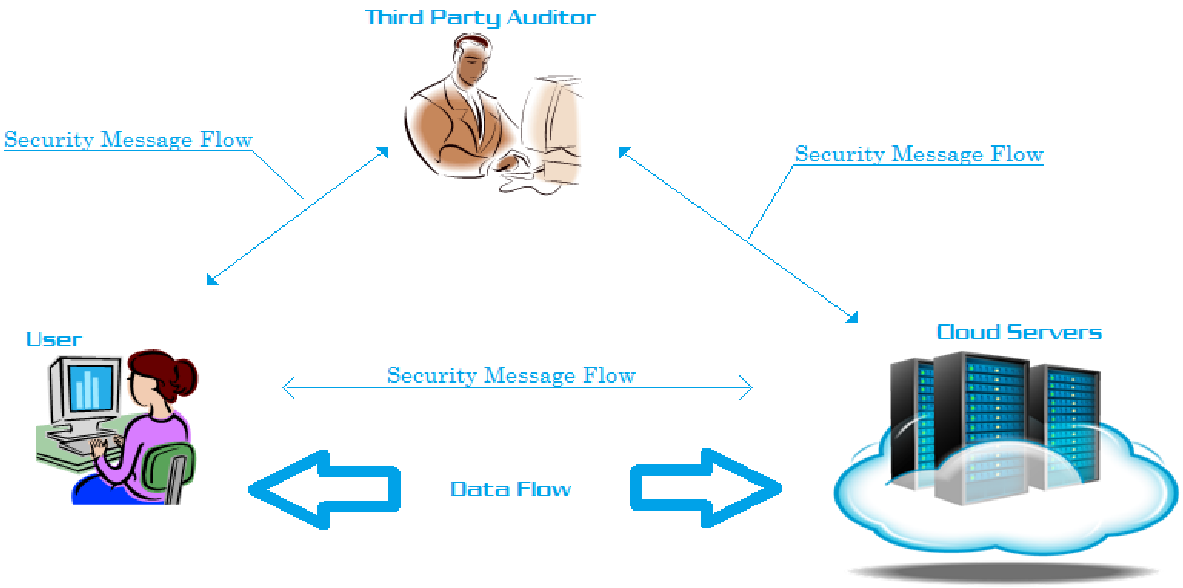
- The analysis report for different security aspects in cloud computing, we also researched on new vulnerable points in cloud computing which can be emerged and before taking any risk we would be providing convenient and effective security aspects which save the data from getting breached.
- The novel cryptographic technique provides secrecy to the data stored in the cloud servers without storing the encryption/decryption key, which is beneficial in preventing intrusion of data or breaching the data.
- In this paper, we are considering that allowing a task to the TPA (Third Party Auditor), in place of cloud user in order to validate the truthfulness of the data or the files stored in the cloud. Here work is focused on VJE algorithm which results in storing the data on cloud server directly in encrypted form.
- Proposal for an intelligent security system which can be used by cloud service provider in order to improve the security aspects in cloud computing.

Experimental Work

Proposed System

To let off the load of management of data of the data owner, TPA will audit the data of client. It eradicates the involvement of the data owner by inspecting that whether his data stored in the cloud are certainly unbroken, which can be essential in accomplishing economies of scale for Cloud Computing. The released audit report will help data owners to assess the risk of their subscribed data services to the cloud, and would also be treasured to the cloud service provider to advance their cloud built service platform. Therefore TPA will help data owners to make sure that their data are secure in the cloud and also the management of data will be quite easy and less troubling to data owners.

The TPA will be totally automated and will be capable of accurately monitoring confidentiality and reliability of the data and uniquely incorporate it with random mask technique to accomplish a privacy stabilizing public auditing system for cloud data storage security. The practice of the novel algorithm initiated for encryption can be useful to the data transmission security. The data which is to be transmitted will be encrypted, even if the data are taken by intruders, that encrypted data would not be consisting any corresponding due to which the data cannot be restored. Only the data owner knows about the key, the cloud providers don’t know anything about key. Also, because of the attributes of encryption, the cloud can work on cipher text, hence dodging the encrypted data to the customary efficiency of procedure. The privacy of user is secure because files of user are encrypted in cloud storage. In this report, we have introduced a vigorous audit service for reliability verification of untrusted and subcontracted storages. Our proposed audit system, which is based on the novel audit scheme architecture, can provision dynamic data tasks and timely unusual detection with the help of quite a few operational techniques, such as index hash table, random sampling and fragment structure. An evidence of perception prototype has been implemented to assess the feasibility and capability of our proposed approaches.



We have considered data storage & sharing of services in the cloud with three bodies: cloud, third party auditor (TPA), and users who may take part as a group. Users in a particular group include one main user and number of users present in that group. 0riginal user is the original holder of data, and shares the data in cloud with other users. Other users in that particular group can download, view and modify shared data based upon the access control policies. Cloud use to provides storage of data and sharing of services for users, and has plenty storage space. The TPA is able to validate the integrity of the shared data based on demands from users, without downloading or accessing the local copy of the entire data. When any user wishes to verify the integrity of the shared data, user or data owner first sends an auditing request to Third Party auditor. After approval of the auditing request, the TPA produces an auditing note to the cloud provider, and then retrieves an auditing proof of the shared data from the cloud. Then TPA verifies the accuracy of the auditing evidence. Finally, the TPA will send an auditing report to the data owner based on the outcome of the verification.

Protecting Data with Encryption

By utilizing encryption for data we can protect the confidential data of data owners. Nearly all the cloud service providers support data storage with encryption, but very few offer provision for data at rest. If the data is sensitive then the encryption terminology used by the cloud service provider need to be match with the sensitivity level of data that is being hosted. Many policies need particular elements data to be encrypted, so here encryption plays a major role in order to satisfy the above needs. Encryption is influential tools that have to be used efficiently for safe-guarding the confidential data of user. It is the user who only can assertively make use of cloud providers believing that their personal data is secured by the encryption.

Comparison of existing algorithms

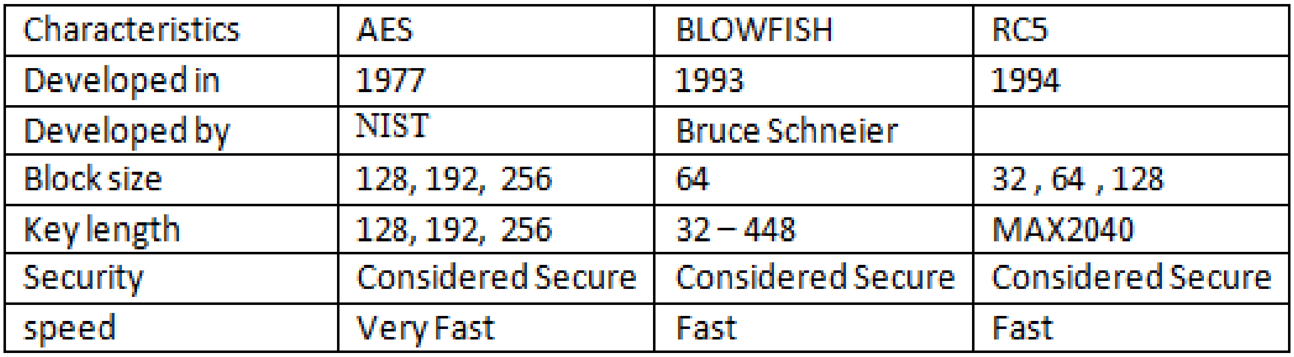
Cloud system developers, designers, architects and Testers must consider the following points.

1. Minimizing the user private information to be uploaded on cloud server.
2. Protecting the information
3. User control maximization
4. Specifying and limiting the purpose of data usage.

Encryption algorithms are playing a vital role over the network. Encryption algorithms convert the data in an unreadable format and generate a key which is helpful in decrypting the data. Security algorithms are further sub divided in two categories:[2]

1. Symmetric

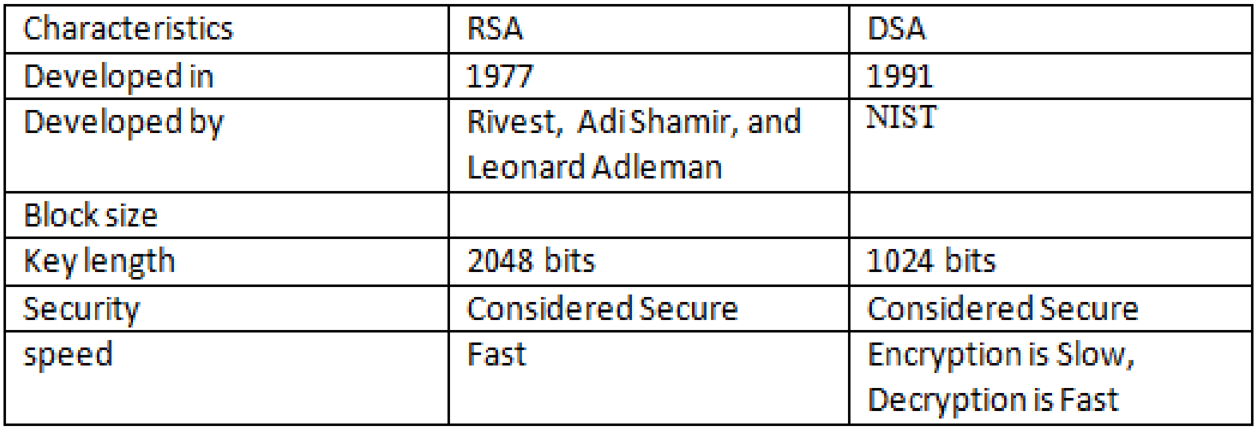
   AES, BLOWFISH and RC5 Encryption Techniques emerged and improved. The block size, speed and secrecy of key makes it more reliable.



Characteristics	AES	BLOWFISH	RC5
Developed in	1977	1993	1994
Developed by	NIST	Bruce Schneier	
Block size	128, 192, 256	64	32 , 64 , 128
Key length	128, 192, 256	32 – 448	MAX2040
Security	Considered Secure	Considered Secure	Considered Secure
speed	Very Fast	Fast	Fast

2. Asymmetric

   RSA and DSA are Asymmetric type of encryption which works on key for encryption.

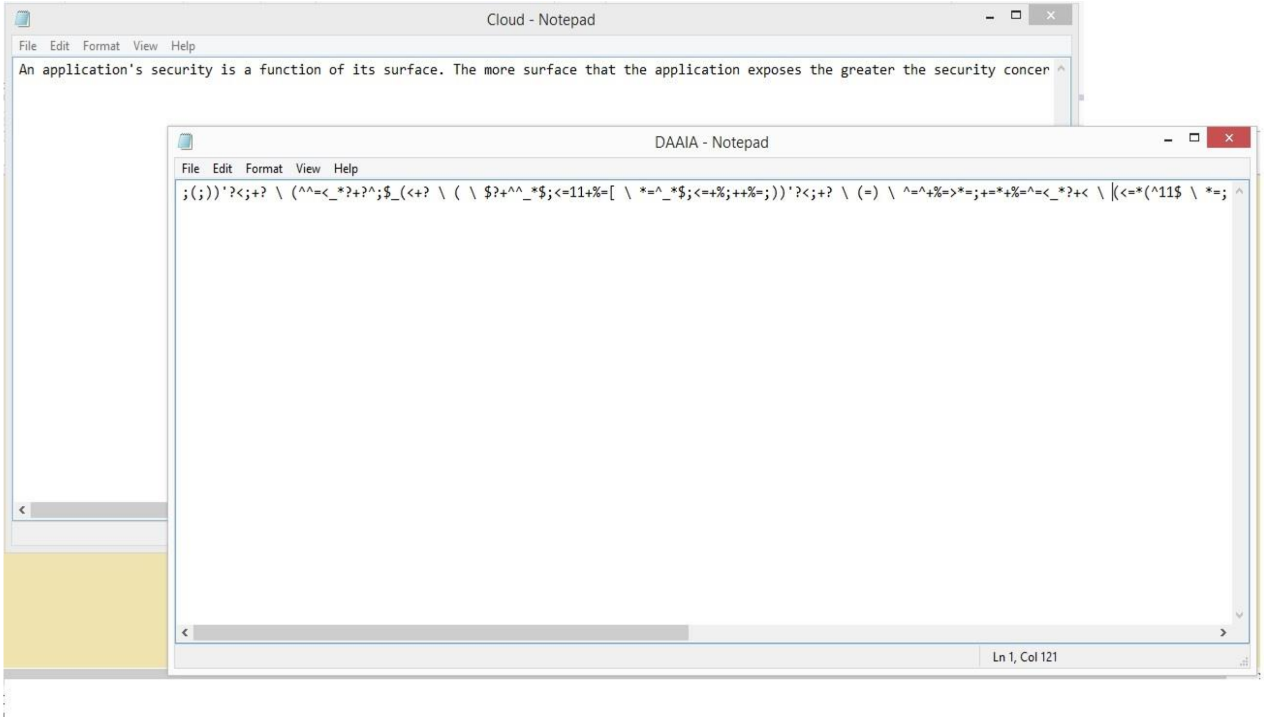


Characteristics	RSA	DSA
Developed in	1977	1991
Developed by	Rivest, Adi Shamir, and Leonard Adleman	NIST
Block size		
Key length	2048 bits	1024 bits
Security	Considered Secure	Considered Secure
speed	Fast	Encryption is Slow, Decryption is Fast

Implementation

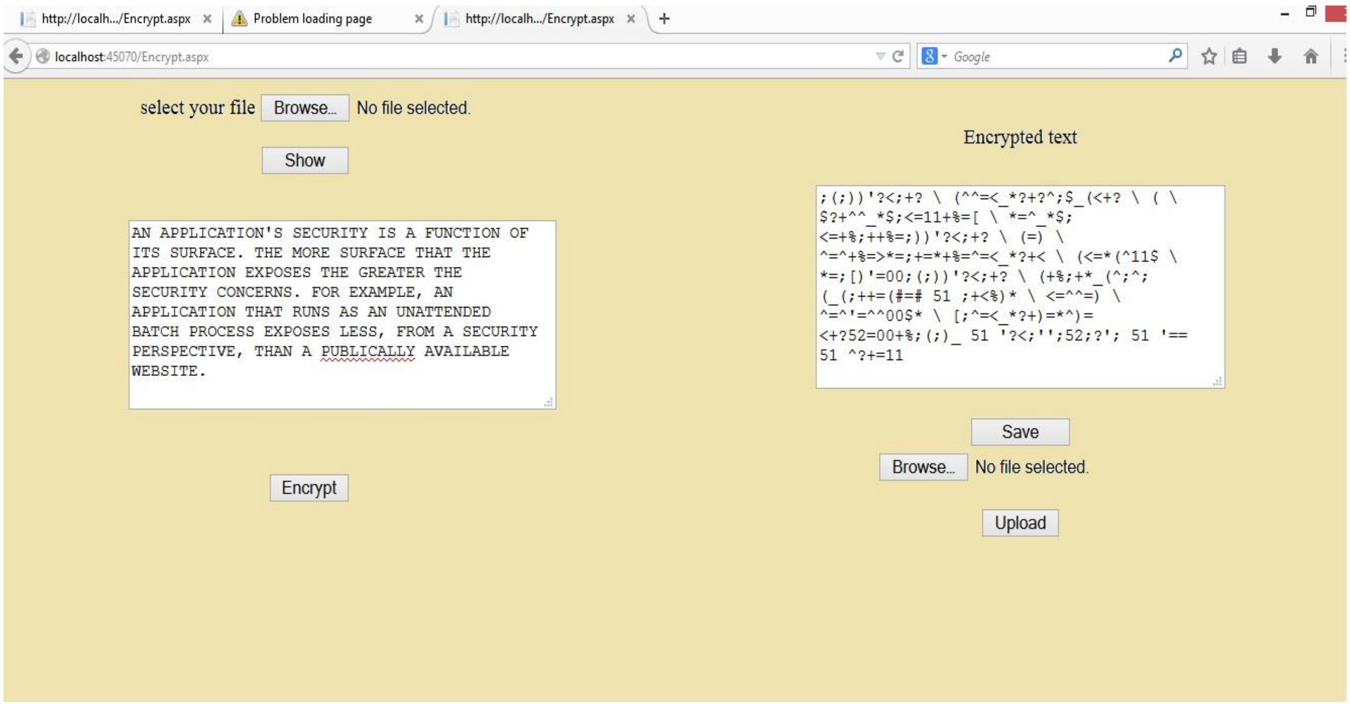
By getting through above encryption methods we have gone through few draw backs which were risky in the terms of encryption, because once they get violated attackers can easily decrypt the data. So we are proposing our new technique' VJE algorithm'. We have used azure platform as a cloud server for deploying our proposed algorithm. This algorithm will encrypt the data present in file by directly uploading to the cloud server and it can be decrypted only when the authorized personnel is going to download the file.

For implementing our new encryption technique we have created novel algorithm which helps in encryption and decryption of the files. The concept of key also plays major role in improving the security, here the user is not providing any key to encrypt the data , instead the key is automatically generated which is further enhancing our proposed algorithm for securing the storage of data in cloud.



```
An application's security is a function of its surface. The more surface that the application exposes the greater the security concer
```

```
;(;))'?<;+? \ (^^=<_*?+?^;$_(<+? \ ( \ $?+^^_*$;<=11+%=[ \ *=^_*$;<=+%;++%=;))'?<;+? \ (=) \ ^=^+%=>*=;+=*+%=^=<_*?+< \ (<=*(^11$ \ *=;
```



http://localh.../Encrypt.aspx
Problem loading page
http://localh.../Encrypt.aspx
localhost:45070/Encrypt.aspx
Google
select your file
Browse...
No file selected.
Show

```
AN APPLICATION'S SECURITY IS A FUNCTION OF
ITS SURFACE. THE MORE SURFACE THAT THE
APPLICATION EXPOSES THE GREATER THE
SECURITY CONCERNS. FOR EXAMPLE, AN
APPLICATION THAT RUNS AS AN UNATTENDED
BATCH PROCESS EXPOSES LESS, FROM A SECURITY
PERSPECTIVE, THAN A PUBLICALLY AVAILABLE
WEBSITE.
```

```
;(;))'?<;+? \ (^^=<_*?+?^;$_(<+? \ ( \
$?+^^_*$;<=11+%=[ \ *=^_*$;
<=+%;++%=;))'?<;+? \ (=) \
^=^+%=>*=;+=*+%=^=<_*?+< \ (<=*(^11$ \
*=;[)'=00;(;))'?<;+? \ (+%;+*_(^;^;
(_(;++=(#=# 51 ;+<%)* \ <=^^=) \
^=^'=^^00$* \ [;^=<_*?+)=*^)=
<+?52=00+%;(;)_ 51 '?<;'';52;?'; 51 '==
51 ^?+=11
```

Future scope

- The proposed algorithm has been implemented in Azure platform, and working effectively. Now, we are focusing on efficiency and secrecy of the data which is being generated by our novel algorithm.
- To implement and modulate the proposed algorithm on servers, which let us know how and what type of complexity the servers is getting and to overcome it.
- To check out the security issues in our proposed algorithm and rectifying by utilizing it on the active cloud server.
- We will test our proposed algorithm on different hacking techniques, so that we can find out our weak points of algorithm and try to overcome on those aspects.

References

1. Rabi Prasad Padhy,ManasRanjanPatra, Suresh Chandra Satapathy“ Cloud Computing: Security Issues and Research Challenges” IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011

2. D.Pratiba, Dr.G.Shobha“Privacy-preserving public auditing for data storage security in cloud computing” International Journal of computer engineering technology (IJCET) Volume 4, Issue 3, May-June (2013), pp. 441-448

3. Nelson Gonzalez, Charles Miers ,Fernando Red´ıgolo ,Marcos Simplıcioand MakanPourzandi“A quantitative analysis of current security concerns and solutions for cloud computing” Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, **1**:11

4. Dr. Sunil Batra, “Preliminary Analysis of Cloud Computing Vulnerabilities”Journal of Engineering, Computers & Applied Sciences (JEC&AS), Volume 2, No.5, May 2013

5. YanpeiChen,VernPaxson,Randy H. Katz “What’s New about Cloud Computing Security?”Technical Report No. UCB/EECS-2010-5 , January 20-2010

6. Mahimajoshi&Yudhveer Singh Moudgil “Secure cloud storage” , International Journal of Computer Science & Communication Networks,Vol 1(2), 171-175,oct-nov. 2011.

7. NehaTirthani, Ganesan R “Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography.”Provided by International Association for Crypto logic Research, Nov 2013.

8. Deyan Chen and Hong Zhao, “ Data Security and Privacy Protection Issues in Cloud”, provided by Cmputing 2012 International Conference on Computer Science and Electronics Engineering, 2012

9. Sumathi Karanam, G.L Varaprasad , P.VenkataSubbaReddy “ Outsourcing and Discovering Storage Inconsistencies in Cloud through TPA”. Sumathi Karanam et al, Int.J.Computer Technology & Applications,Vol 4 (5),864-868 Sept-Oct 2013

10. T. Prasanthi, C. Balasubramanian, S. Kimsukha Selvi, K. Kala “An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing”. Proceedings of the World Congress on Engineering 2014 Vol I,WCE 2014, July 2 - 4, 2014, London, U.K.

11. Ashish Badiye*, Neeti Kapoor, Pooja Shelke “ Some Forensic & Security Issues of Cloud Computing”. International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, October 2013