DATA SECURITY ISSUES IN CLOUD COMPUTING

Abstract: With the development of cloud computing, Data security becomes more and more important in cloud computing. Cloud Computing provides the way to share distributed resources and services that belong to different organizations or sites.Since Cloud Computing share distributed resources via network in the open environment thus it makes security problems.In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system.

INTRODUCTION:

With the development of cloud computing, Data security becomes more and more important in cloud computing. Cloud Computing provides the way to share distributed resources and services that belong to different organizations or sites. Since Cloud Computing share distributed resources via network in the open environment thus it makes security problems In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system.The security issues raised by the cloud paradigm are not always dealt with the user’s point of view.It have a growing impact on enterprise information technology system and business activities in many large and small organizations. There is a lack of knowledge as how cloud computing impacts the confidentiality and privacy of data stored, processed and transmitted in cloud computing environments.

CLOUD ARCHITECTURE:

The systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Cloud models are as follows:

1)Delivery Models

i)SaaS

ii)PaaS

iii)IaaS

2)Deployment Models

i)Private cloud

ii)Community cloud

iii)Public cloud

iv)Hybrid cloud

3)Management Models (trust and tenancy issues)

i)Self-managed

ii)3rd party managed (e.g. public clouds and VPC)

DATA SECURITY:

Several aspects of data security, including:

1)Data-in-transit

Confidentiality plus integrity using secured protocol

Confidentiality with non-secured protocol and encryption

2)Data-at-rest

Generally, not encrypted , since data is commingled with other users’ data

Encryption if it is not associated with applications

3)Processing of data, including multitenancy

For any application to process data.

METHODOLOGIES IN OUR RESEARCH:

1)Systematic literature review on data security issues.

2)Mitigation strategies analysis.

3)Proposing new best method regarding data security,

Intially we collect the information on data security issues and their mitigation strategies in cloud computing.Then we analyse those mitigation strategies their drawbacks and propose a new method regarding data security in cloud computing.

PILOT IMPLEMENTATION

1)Initally using systematic literature review we have mentioned the data security issues in cloud computing.

2)We have mentioned the best mitigation strategies for those data security issues we have identified.

3)Analysing those mitigation strategies and to mention drawbacks and to mention a new methodology for data security in cloud computing.

Hence our pilot implementation is three step implementation.

DATA SECURITY ISSUES IN CLOUD COMPUTING:

1. Data Integrity:The stored data in the cloud may suffer from enormous damage occurred during the transition period the transition operations. It includes risks both from inside and outside.

2. Data intrusion:Data Privacy there is a chance of gaining access of our accounts password by the intruders. The intruder can make unwanted changes.

3. Data Loss:Data loss may occur sometimes if there is no backups and redunction.

4. Data Confidentiality:The confidential data should be not exposed to anyone and should be kept secured.

5. Data non- repudiation:The transmission of message of the between third party.

MITIGATION STRATEGIES:

G . Monika and Y. Kal

6. Strategies and Encryption

Techniques for Data Security

From the above data, security is the major issue in the cloud computing environment and researchers.Professional has found some strategies and encryption techniques to solve the issues. Some of them are as follows:

To secure the data from the malicious attack, the data should be encrypted by using the proper cryptography methods. Here there are the mitigation strategies.

1)Symmetric key cryptography method is one of the best encryption method.One key is used by both sender and receiver.The key which is condfidential can be a text or string where each letter can be shifted by number of places.

2)Asymmetric cryptography method where two of both the private and public keys are used to prevent their data from malicious attacks.Elliptic curve are used to do encryption.

3)Hash function cryptography is also one of the type using commas and other symbols including data.

4)Image steganography:Sending the data using images where the data is embedded in the images.

5)Pixel key pattern which is used as a tool image processing in computer visualization.

Hence these are the best mitigation strategies to over come the data security issues in cloud computing.

Drawbacks:

1. Existing mitigation strategies does not support traceability.

2. Verification of the data considering time and size of the signature(passwords) linearly increase with number of users increasing in the cloud.

3. Data freshness while still preserving identity privacy.

4. TPA(Third party auditing) can learn the original data during public auditing.

MITIGATION METHOD FOR ERROR CONTROL OF DATA STORAGE IN CLOUD:

considering research work we have solution for supporting both the data and also user’s traceability based on signature and to perform multiple auditing tasks at the same time by using the aggregate signature.TPA gives a detailed information on data error location to the cloud. Users send an auditing request to TPA, after receiving a request TPA send a auditing challenge to the cloud server. The Cloud server is responsible for generating the proof based on verification signature and pass the auditing proof to TPA. TPA validates the proof and sends the auditing report to the user.

Steps for mechanism of the method

1) Creation of key

2) Generating signature or password

3) Dynamic data

4) Traceability

5) Data error location to resolve

CHALLENGES FACED:

1)Intially our selection of topic is a broad topic in which we are not in to a narrow or specific.

2)we have failed in expressing our views regard our research.

3)Finally we have used systematic literature review and gathered information,analysed for proposing new mitigation strategy.

Hence these are the some of the challenges we faced.

CONCLUSION:

Cloud computing is a technology in which all services are available to users.Its demands are increasing day by day.The security issues of the data in cloud computing are having obstacles.There is a scope to do research on data security issues in cloud computing.T.P.A is one of the security issue that can be used for data storage in cloud computing.There are many encryption tecniques for data security in cloud computing.Still there is a need to find advanced methods(mitigation strategies) regarding data security.Hence there is a lot work to be done on data security issues.