Cloud Computing Security Issues Using Encryption Techniques

S.Kanimozhi

M. Phil Research Scholar, D. B. Jain College (Autonomous), Thoraipakkam,

Chennai, India.

E-mail:nevathasivakumar10@gmail.com

Karthik. M

Assistant Professor, D. B. Jain College (Autonomous), Thoraipakkam,

Chennai, India.

E-mail:karthikmohan2006@gmail.com

ABSTRACT: Cloud cryptography is a rising technology for providing computing resources and storage to the users. Its eliminates the need of maintaining costly computing facilities by companies and many other institutions. But the acceptance of cloud computing applies only if the security is ensured clients data is placed on the secure model in the cloud. In cloud can single encryption scheme rather it makes use of different encryption scheme rather it makes use of different encryption schemes for the encryption of the cloud data and convert the data to unreadable format and later on decryption using some unique key. Numerous encryption techniques by now are available for the protection of the data in the various application. So the cryptographic techniques within the cloud will ensure the data security and integrity which is mostly required in cloud atmosphere. The security issues such as confidentiality and integrity of data in data security are essential in the cloud. This paper is mainly focused on security issues and cryptographic techniques. In today's cloud and several cryptographic techniques that can be used to improve the security in cloud environment.

Keywords: Cloud Computing, Security Issues, Cryptography Techniques, Encryption.

I. INTRODUCTION

Cloud computing is one of the most popular technology that permit get admission to to information and computer resources from anywhere that a network connection is to be had. Cloud computing offers a shared pool of resources inclusive of facts storage space, networks, computer processing energy. The cloud is a cryptographic techniques of resources that which maintain and manages itself. Cloud computing is the quickest growing era, offers various services over the net. It can serve many centres to the enterprise inclusive of sources, infrastructure, platform and so forth., by using paying amount on demand basis over the network with the capability of increase or lower the necessities. Cloud computing can enhance the supply of IT networks and thus provide the capacity for fee reduction via optimized and green computing. Cloud also includes the primary chance inclusive of safety, facts integrity, community dependency and centralization. As the safety isn't provided in cloud many corporations adopt their particular security shape.

There is no higher manner to comfy important facts than thru cryptography specifically while that records is saved inside the cloud. Ralph Spencer Poore, an records security with a long time of experience in cryptography, is a proponent of employing cryptographic security in cloud computing. Cloud encryption the maximum trusted protection technology these days. While those experts agree that encryption in the handiest technique to facts safety in the cloud, It may be difficult. There are such a lot of types of encryption offerings available in online market place. All varieties of companies, from small to big companies, locate these offerings promising but they may be complicated and complicated.

II. CLOUD DATA ENCRYPTION CHALLENGES

The demanding situations of cloud clients and cloud provider companies face in terms of facts encryption. There are as follows:

1.Cloud Platform Differences:

Differences in cloud systems pose headaches in records encryption. There are 3 models with regards to the cloud platform and these are Infrastructure as a Service(IaaS), Platform as a Service(PaaS), and Software as a Service(SaaS). Each of these models gives protection answers and perform one-of-a-kind responsibilities to offer protection to a giant quantity of records. Because of the differences among these models pose, there are complexities within the encryption procedures. As a outcomes, an organisation's cloud carrier provider will find it hard to preserve and carry out numerous encryption strategies.

2. Key Management Complexity:

Dealing with information encryption, key management is the most complicated issue of any protection system and network. Key management is the technique of safeguarding encryption keys from loss, unauthorized access, and corruption. However, key management is commonly the predominant reason encryption is not being carried out by organizations.

3. Diversity of Encryption Architectural Approaches:

There are lot of architectural tactics for encryption inside the cloud, including utility stage, record system primarily based, agent-primarily based, and garage tool stage approaches, According to the Cloud Standards Customer Council. These approaches have their personal features based totally at the control of encryption keys and their overall performance.

4. Compliance Regulations in Different Locations or Countries:

One of the cloud problems in the use of encryption is the style of compliance rules in one-of-a-kind territories. Thus, information encryption isn't straight forward and is going via numerous techniques earlier than its receives done. For instance, if a enterprise is needed to complete with guidelines in different international locations may perform records evaluation first. In outcomes, the cloud garage company will to transport probably to locate it hard to control and perform encryption on that scenario.

5. The Challenge of Responsibility:

The most chargeable for protective cloud records are cloud carrier providers, observed by using cloud consumers. Because of the challenges are whoever takes the responsibility of facts encryption will need to overcome and control all of them. Instances of this demanding situations may be an upsurge in economic fees and complex verbal exchange and collaboration among each the cloud carrier provider and the cloud client.

2.1 Security problems to don't forget whilst the cloud data is Encrypting:

According to Gartner, agencies must prepare a information securing plan first in terms of cloud encryption. If companies fail to accomplish that, it may bring about more complexities and economic troubles. There are some cloud garage protection issues and risks to when the businesses save and encrypt their records within the cloud.

Fig: 1 Cloud Security of Different Sectors

The largest troubles cloud safety is the password or the security key. If the assigned password is lost at some point of the system of encryption inside the cloud, there's no manner to salvage the information. Another issue approximately passwords or spouse's name. The less difficult security keys to bet and the records may be breached.

The encryptions guarantees that encoded records can't be worried and stolen due to its complicated strategies and techniques. However, there's no perfect answer of statistics security. The companies sees the encryption to have many resources required that's why it's reviewed as the handiest solution. Its complexity creates this fake feel of safety.

Another safety issue to recollect while encryption cloud data is that its calls for co-operation. For instances, if a member of the corporation stocks a file that desires secrecy to another member, this record have to be continually encrypted when sending the message. However, both of the contributors, would possibly discover it time-ingesting and dull to encode and decode that records encryption calls for co-operation and this can be difficult to all events involved.

III. COMMON CLOUD ENCRYPTION MISTAKES

Organizations and protection specialists see cloud encryption sturdy and perfectly secure. But the question is why organizations are or even the government still get hacked and breached? Here are the a number of the errors companies make whilst encrypting cloud records:

1.Believing that complying to regulations manner complete protection:

This is a misconception. It is proper that rules just like the HIPA-A(Health Insurance Portability and Accountability Act of 1996), CJIS(Criminal Justice Information Services), PCI DSS(The Payment Card Industry Data Security Standard), amongst others entail and require any agency to protect all touchy data.

2.Reliance on Low-Level Encryption:

Low-Level Encryption is considered as a one-click on solution to Data Breach Prevention. Examples of this are disk and record encryption. For instances, while the server is off, disk encryption only works during that point. The working device will decrypt data when the server is grew to become on and the facts can be handy to all users which might be logged in. Reliance on low-degree encryption is as very easy as one click, however attracters can be relaxed at breaches too.

3.Assuming that Software Developers have Full Expertise:

Software builders and engineers are generally no longer specialists in safety. Experts are commonly at the IT discipline and they may be pen testers, CISOs, and machine administrators. Organizations relay on software

builders encompass unprotected encryption keys, unprotected key keep, susceptible crypto, the usage of old libraries, and the usage of one key for the whole lot.

4.Dependence on cloud carriers when its involves records security:

Because statistics breaches have been growing over time, extra than technology businesses offer cloud garage services. Tech giants like google, Microsoft, and Amazon spend hundreds of thousands of greenbacks to be the maximum comfy cloud in the cyber security industry.

5.Incorrect Key Management:

Getting key control wrong is the biggest mistake an corporation can make. Even if the records is encrypted the proper manner, fallacious dealing with of key management ought to cause statistics breaches. Key control failures encompass fetching the key insecurely, leaving the important thing unprotected with some other layer of the encryption key using the identical key and never converting it.

IV. CONCLUSION AND FUTURE WORK

Cloud computing is global rising, subsequent era within the field of information generation. It has numerous benefits however a few demanding situations are nonetheless existing on this generation. Security is the maximum difficult difficulty, offers with security issues to don't forget when encryption of cloud information, common place cloud encryption errors and many others.

REFERENCES:

[1] Security in Cloud Computing Using Cryptographic Techniques. Deepanshi Nanda, Sonia Sharma IJCST Vol 8. Issue 2, April-June 2017, ISSN: 0976 8491.

[2] Cryptography within the Cloud Security.

[3] Challenges with the Cloud Encryption.

[4] Security and Privacy Issues in Cloud Environment.

[5] Cryptography Based Security for Cloud Computing System.