IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Secure File Storage Using Hybrid Cryptography Algorithm

Ms. Renuka Durge , Dr. Vaishali Deshmukh
Dept of CSE
Prof. Ram Meghe Institute of Technology and Research ,Badnera.Amravati.

Abstract

The big data is stored on the web i.e cloud. So because of cloud storage, users can store their data on cloud. Cloud computing provides various services to the users like SaaS, PaaS, IaaS. Cloud storage does not require any maintenance cost and it provide high quality applications. But when the data and business application to a third party causes the security and privacy become a critical issues . In this proposed system the concept of cloud data storage security is used to overcome the shortcomings of traditional data protection algorithms and improving security by using enchanced encryption and decryption techniques, to better security for the cloud.This paper presents Hybrid (AES & MD5) encryption

***Keywords*-cloud computing, encryption, decryption, AES.**

I. Introduction

Basically the concept of cloud computing is invented due to the need of various services like networking , security, storage, and artificial intelligence also for standard applications. Cloud computing can be known as the program computing . one can use different applications & software from all over the world, which are provided by some service provider called as cloud. [1]

In the current world, big data or rather mega data has become an essential part of our daily life. People get to deal with huge amount of data every day because of the activities in their professional or personal life. All this data needs a lot of storage space and consistency in its availability all the time across various devices that the users use daily and connect to get their work done. However, the physical storage space has a limitation because of the cost involved and a few other factors like the device type or the technology they use to function[2]. Many companies have come up with a new, fast, and low-cost technology to overcome the challenges regarding storage and availability issues of data for the users which is commonly known as Cloud Computing to the world[3].

II. Literature survey

Since the early 2000s, quite a few enterprises were using the cloud technology to share their resources on-demand. It is only in the past few years that this technology has started gaining its popularity overall. People need to have access to the internet and the cloud domain of the company whose services they would like to use to store their data. During the last ten years, the development of the cloud computing was comparatively slower than what it is now. In 2006, traditional IT technology occupied 98% in the 29 million IT workloads worldwide with only 2% cloud computing occupancy. However, by 2016, the global market for public cloud and private cloud has increased up to 15% and 12% respectively, and the world's IT workload has increased to 160 million items [2].

We has emerged as a global leader in dataintensive computing that covers Artificial Intelligence (AI), the Internet of Things (IoT), Virtual Reality (VR), Online-to-Offline (O2O), Smart Cars and Online Payments. It has been predicted that in the coming years, the use of the cloud computing service will keep a stable growth rate of 30% annually [4]. For example, more and more financial service companies and organizations, like banks, non state- owned third-party funds and loan platforms, tax and revenue administration channels have shifted their offline services to cloud platforms to provide customers with more convenient and accurate services.

Health care systems and government agencies also have started to using cloud platform. As a result of this emerging trend in the those who are using the usage of the cloudbased services have the security issues related to cloud computing which becomes a massive challenge.

After the release of Cyberspace Security Law in June 2017, the National Cyberspace Security Strategy and other related laws, regulations, and policies in recent years, security, and trustworthiness have become key to enterpriselevel users' IT system building. For essential sectors and fields such as public communications, information services, energy, transportation, water conservancy, finance, public service and e-government, it is more critical to ensure a secure and reliable key information infrastructure.[5] These days, the most significant challenge for most of the organization is the constant increase in the number of online security threats and the rise in their complexity.

The whole process of monitoring and securing a system in an organization becomes more complicated because of the widespread use of various devices and platforms by employees to connect to the online world. Cybercriminals, on the other hand, are also becoming very professional and smarter by using more sophisticated and sometimes readily available online tools to execute attacks. This creates a massive gap between the overall security of an enterprise and the level of potential cyber threats. In addition to the security of the cyberspace, the security of the physical space is also paramount. In the last few years, insider threat has become one of the top reasons for an organization .

However, the operations team with the most considerable authority can easily access all the confidential information from their cloud product. Another security issue that most people ignore here is the use of the public wireless internet connection to access their vulnerable personal information. Most of the cities provide the free urban wireless networks. Shops and restaurants usually provide free open wireless connections to attract more customers. Most people do not even care if it is safe and secure or not before starting to use them. The public Wi-Fi connections allow people to have internet access without asking for any authentication. This means that all the information gets transmitted without any encryption[6]. The customers are likely to access the internet and use their Smart phones or devices to access their accounts with vulnerable data like banking or online payment systems. Hackers can easily hack the account of people to steal their payment authentication keys.

Also the issue with the network is the bandwidth, which is always very limited. It may be very likely for the users to lose connectivity in the middle of their financial transactions which could leave their private accounts more susceptible to potential attacks. Besides, both traditional and start-up financial companies are also using Application Programming Interface (API) to provide third-party services to their customers. Also, most people access their private information from different platforms across the Internet, and it needs very less effort from cybercriminals to eavesdrop and steal this information while data is being transmitted across various platforms and networks[7].

A. Data Security

The most critical issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. Data security issues are seen in (SaaS, PaaS, and IaaS) level and the primary challenge in cloud computing is data sharing. Cloud service providers use some data security techniques like encryption and decryption to access control to protect their data from and data loss.

Some cloud service providers not only apply encryption algorithms to the data stored on their server but they also encrypt the data during its transition on the network, as the data is in transmit is the most vulnerable to an attack. An advanced method in cryptography can be used to address the issue of confidentiality, and some system also monitor how much people have access to the data so that the need for users must be to take extra precautions to secure their data.

In cloud computing companies the maintenance staff working for the service providers may also act as an insider threat, especially the ones who have the authorized access to the database. They can access, modify and delete data from their customer's account causing severe damage to the reputation of the service provider. Eg. Aliyun has its system in which the machine for sensitive and private information storage and the maintenance devices are separated. As a result, even the internal operations and maintenance staff are not authorized to access all the data. Aliyun system also takes charge of the access command, which can be used for the surveillance of staff and user's ultra-right operations. Besides, nearly all the cloud computing companies provide supervision on the database. All the data on the cloud are stored in a database, including the user's business confidential data and government data. Except for essential data cryptography, Aliyun and Huawei provide database auditing to supervise all the operations on the database, which can help to trace back to the identity and behavior of a user according to their suspicious actions. Cipher machine, server clustering and load balancing can efficiently solve the problems with data when some of the servers are out of power or destroyed by natural disasters.

B. Network Security

To avoid the data loss or data misuse, many service providers use data encryption. Data transmitted in a network is divided into smaller parts using encryption before being transmitted to the cloud server.

Thus, it is essential to encrypt the data during transmitting on the network as the data can be easily attacked during that period. Many companies handle their clients by making them aware of the reason for the need to update their network transport protocol, and ask them to switch from HTTP to HTTPS, without changing the user's server configuration during the request and response exchange. SSL certificate as a controlling service also plays a vital role in system which also takes charge to access command that can be used for the surveillance of staff and user's ultra-right operations. Important role of SSL helps to establish an information highway to connect the client to the server. It provides client and user authentication and encrypts the transmitted data on the highway.

III. Proposed work

In this proposed work we mainly focuses on the following activites like:

a)Uploading the data on cloud such that even the administrator is unaware of the contents.

b)Downloading the data so that the integrity of data is maintained.

So that proper usage and sharing of the public, private and secret keys involved for encryption and decryption algorithm to safeguard data security in Cloud.

The system proposed have described a hybrid system where encryption algorithms are used in a predefined order on the same set of data one after the other to finally obtain an encrypted data form. This encrypted data or cipher text can be used to transfer such confidential data without the fear of being rigged. And to decrypt same data the exact reverse order of the encryption process is used in the encryption stage.

The encryption technology is the most safety techniques used in today's e-commerce and banking websites which are very importance. Information encryption technology can not only meet the security requirements of confidentiality of information, but also avoid the leakage of the important information which are of high security especially in the security (defence) and hospital, banking sectors. Therefore, encryption technology is the base of authentication technology, as well as many other security technologies that are used today. At present, in different areas of software systems, the most popular encryption algorithms are the AES encryption algorithm, the MD5 encryption algorithm, the SHA1 algorithm, etc. In connection with characteristics of different encryption algorithms, we define a simple initial encryption algorithm first in this survey, then use the AES encryption algorithm, finally, form a hybrid encryption algorithm together with MD5 encryption algorithm. The hybrid encryption algorithm has greatly improved the security of the encryption algorithm.

The exact reverse application of the sequence of the algorithms needs to be used to decrypt the cipher text, thus even if the algorithms used in this process are widely known, unless the sequence is known to the decrypting body, decryption is impossible.

Example process with explanation:

Algorithms to be used are AES and MD5.

Cipher algorithms were one of the most precluding algorithms of all the cipher algorithms. Most of them such as Caesar cipher, substitution cipher are inexistent today as they have fatal flaws or are too easy to decrypt. But the only possible way to crack these algorithms is if their output is known, because only then can the pattern be detected. But in hybrid system, the output of cipher algorithms are further encrypted by other algorithms and thus detection of pattern is impossible even if the attacker has the final cipher text. Mathematical cipher maybe or may not be used. But this may be used as a slight deterrent which would be producing output closest to the text and thus may act as a last step to lead the attacker haywire.

IV. Conclusion

Thus , we can conclude that the cloud sector is rapidly increasing, today's world cloud computing is very necessary for businesses and organizations for storing their large data, as the data is very vast and that has to be stored at some place, less space have to be there on computers, it will more expensive and time consuming. But still we are worried with security because we don't wants that someone else is using or misusing their data. So using enhanced security encryption technique data storage in cloud is more advantageous than traditional storage because of its availability, scalability, performance, portability and its functional requirements.

V. References

[1] Pratik Gaikwad, Prof. Swapnil Patil ,"Data Access Security in Cloud Computing : A Review", International Journal of Scientific & Engineering Research Volume 12, Issue 3, March-2021 .

[2] Sonali Chandel, "Enterprise Cloud : its Growth & security challenges in China", 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud).

[3] Nagarajan and K., & Sampath Kuma,"A Security Risk on Data Storage in Cloud based System –Survey",

[4] Sean Carlin, "University of Ulster, UKCloud Computing Security, International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011

[5]Naveen Kunnathuvalappil Hariharan, "Financial data security in cloud computing", International Journal of Engineering, Science and Mathematics. Vol. 10 Issue 1, January 2021.

[6] Sampath Kumar K," A Security Risk on Data Storage in Cloud based System –Survey", International Journal of Emerging Technologies 10(2): 195-199(2019) .

[7] Keke Gai,"SA-EAST: Security-Aware Efficient Data Transmission for ITS in Mobile Heterogeneous Cloud Computing", January 2017 ACM Transactions on Embedded Computing Systems 16(2):1-22

IJCRT