International Journal of Computer Science and Engineering
ISSN: 2832-2754 (Online), Volume-2 Issue-6, Nov-Dec 2022, pp.1-4

A Survey On Assured Data Transmission

[1]R. Ramesh, [2]P. Vyshnavi, [3]M. Jaya Madhuri, [4]P.Sri Vasavi, [5]K.Keerthi, [6]N.Gayathri

[1]Professor, Department of CSE, KKR & KSR Institute of Technology and Sciences
[2,3,4,5] B.Tech Students, Department of CSE, KKR & KSR Institute of Technology and Sciences.

***Abstract* - Security plays an important role in our life as well as in the area of networking for transmission of data from one device to other device, because it is only responsible for securing all information which are passed through the computers network. There is tension between user data protection and rich computation in the cloud. Users want to maintain control of their data, but also want to benefit from rich services provided by application developers using that data. At present, there is little platform-level support and standardization for verifiable data protection in the cloud. On the other hand, user data protection while enabling rich computation is challenging. It requires specialized expertise and a lot of resources to build, which may not be readily available to most application developers. We argue that it is highly valuable to build in data protection solutions at the platform layer. In this project, we would be doing that and protect the data transmission. Storage-as-a-Service offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their sensitive data to be stored on remote servers. In this paper, we enable a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them.**

***Keywords*- CSP, Transmission, SAAS, Security.**

I. INTRODUCTION

About Cloud:

Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing. Whether you are running applications that share photos to millions of mobile users or you're supporting the critical operations of your business, a cloud services platform provides rapid access to flexible and low-cost IT resources. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right type and size of computing resources you need to power your newest bright idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use. Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the internet. A cloud services platform such as Amazon Web Services owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application. Cloud service providers are companies that establish public clouds, manage private clouds, or offer on- demand cloud computing components (also known as cloud computing services) like Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a- Service (SaaS). Cloud services can reduce business process costs when compared to on-premise IT.

Cloud data security is the combination of technology solutions, policies, and procedures that you implement to protect cloud-based applications and systems, along with the associated data and user access.

The core principles of information security and data governance—data confidentiality, integrity, and availability (known as the CIA triad)—also apply to the cloud:

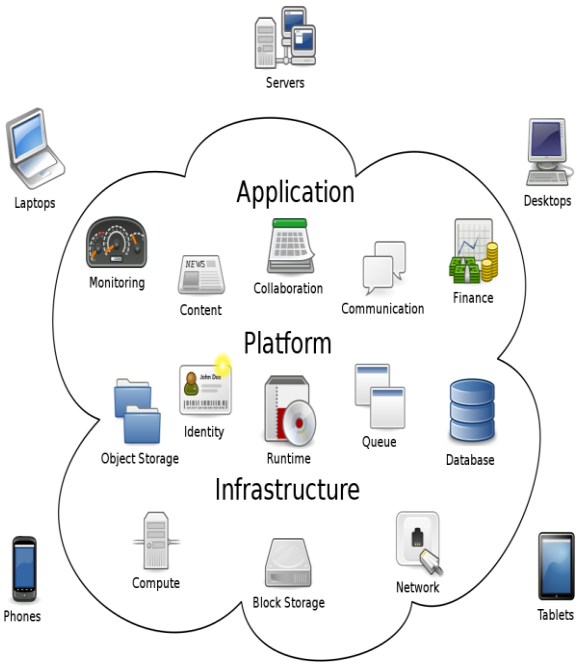
•Confidentiality:
protecting the data from unauthorized access and disclosure

•Integrity:
safeguard the data from unauthorized modification so it can be trusted

•Availability: ensuring the data is fully available and accessible when it's needed

Applications Of Cloud:

International Journal of Computer Science and Engineering
ISSN: 2832-2754 (Online), Volume-2 Issue-6, Nov-Dec 2022, pp.1-4



Applications Of Cloud:

1. Art applications
2. Business Applications
3. Data Storage and Backup Applications
4. Education applications
5. Entertainment Applications
6. Management Applications
7. Social Applications

III. LITERATURE REVIEW

The research papers help us to find the existing models and guide us to develop a new thesis by overcoming the problems which have been found out

Akansha Deshmukh et al. [1] proposed that data generated by the organizations is growing exponentially, data is stored in cloud by CSP's. The main aim is to provide data authentication, integrity and confidentiality using cryptographic algorithms.

Punam V.Maitri et al. [2] showed that cloud computing is useful in many fields for data storage purposes, there are n number of ways to provide data security, here symmetric key cryptography and steganography algorithms are used.

Dr.G.Jaspher et al. [3] proposed that cloud is a omnipresent computing technology, day by day cloud computing is enhancing so its security is important such as access control, storage, virtualization. Biometric based authentication is proposed. We try to implement a model using Microsoft Azure for using cloud services. The encryption and decryption algorithms, i.e., DES and RSA, were embedded in the code. We have used PHP for web page development and for encryption and decryption. To provide protection for business data we have BitGlass, which is a beta version and provides transparent protection. It aims to reduce the risk of data loss and maintains data visibility.

[4] Study and improved data storage in cloud computing using cryptography
The Due to security issues, information over the Internet is becoming important. We have suggested a method to protect critical file data. Cryptography algorithms are an efficient way to encrypt sensitive data. It is a retrieval and transmission system that is readable only by intended users. The low cost and data usability of cloud computing is advantageous. Cloud storage has many advantages at low cost and data connectivity through the Internet. Ensured cloud data security is an important aspect in the cloud computing community, as customers often store confidential information with cloud storage services, but such providers are not trustworthy.

[5] ENABLING DATA INTEGRITY PROTECTION IN CLOUD STORAGE USING CRYPTOGRAPHY
Cryptography is one of the most important security technologies which used to secure the data transmission and the data itself. As the time and challenge growth, the cryptography also grows up with variety of encryption techniques and algorithms. It protects against unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key. Crypto cloud computing is a new secure cloud computing architecture.

[6] Security enhancement using blockchain based modified infinite chaotic elliptic cryptography in cloud. This paper develops a blockchain-based modified infinite chaotic elliptic cryptography (MICEC) to improve and tighten the security in the cloud. It contains three stages: protection of authentication, ownership protection, and identity mapping validation. At first, MICEC is employed for an authentication process that combines the infinite elliptic curve cryptography and modified chaotic neural network for pair of key generation and data encryption.

[7] Security protocol for data Transmission
In this paper we will present a protocol that help to secure data access during transmission. Accordingly, users can send their data to the cloud safely and quickly. Thereby, encourage the users to take the full advantage of the cloud computing services. We used in this paper a private and public key scheme to verify data confidentiality.

ISSN: 2832-2754 (Online), Volume-2 Issue-6, Nov-Dec 2022, pp.1-4

Additionally, we used a hash function to verify data integrity. Finally, data authenticity and non-repudiation have been verified by applying the digital signature mechanism.

[8] Data Transmission in clouds using Heed and Energy efficient routing Algorithm
Cloud Computing is a field of computer science in which user can access resources remotely through a browser. Cloud Computing increases the speed of accessing the services in very less cost without actually deploying them. It decreases the time from implementing the software to actually deploying it. Cloud Computing users can access resources on demand. Cloud provides the on-demand services, virtualization, and open source. The data owner can store and access the data from the cloud with the help of the cloud service provider. In large organizations, the data which is stored on the cloud is accessed by the many users of the same organization.

[9] Secure data Transmission in cloud using Code Verification
This paper describes about the use of code verification and use of code certificate in order to perform secure and trusted sharing of data transmission.

[10] Multi level Authentication for secure data transmission using RKGM to cloud
In this paper we propose a multilevel based authentication for secure data transfer over cloud. The proposed system has three modules first module defines how multilevel authentication is processed, second level determines how encryption is administered and final module deals with decryption process. To avoid the unauthorized access into the server a novel multilevel authentication is developed. In the proposed system data security is enhanced with the help of random key generation algorithm (RKGM).
[11] Homomorphic technique for secure data transmission in cloud computing
The architecture of cloud computing is one in which there is no existence of central manager which results in various breaks occurred in the network. To guarantee the transmission of data from the source to the destination, two types of cryptographic schemes are introduced, i.e., the fully homomorphism and fully disk encryption are familiarized. The completely homomorphic cryptography scheme is safer and lighter than fully disk encryption. In the paper, an improvement of completely homomorphic cryptography is planned using elliptic curve cryptography and OTP generation.

[12] Efficient and secure data transmission approach in cloud MANET -IoT integrated Framework. Our purpose in this research would be to establish a communication system among IoT nodes in such an embedded Cloud and MANET structure. The main goal of this research is to create an efficient and secure approach for communication in Cloud-MANET-IoT integrated framework. This approach is implemented and tested.

[13] An innovative DNA cryptography technique for secure data transmission
In this paper, a new DNA cryptography technique is proposed using Symmetric Key Exchange. It is used to protect data from intruders while data travel through an insecure channel. When symmetric key is used, intruders are unable to generate a crack key, thus protecting the data. If the key is not known, it is impossible to decrypt data even when data are sent through an insecure channel. XOR operation with one-time- pad DNA sequence is used as the encryption technique.

[14] Quantum cryptography: The ultimate solution for secure data transmission
Today, Quantum Cryptography is rapidly moving out of the lab and into the telecommunications mainstream offering commercial quantum cryptography and key distribution systems based solely on quantum first principles. The question is: could Quantum Cryptography be the ultimate solution to secure data transmission? This paper presents some recent developments in the field and investigates the guarantees offered by the proposed protocols.

[15] A Multi-layer cryptosystem for secure data transmission using PRNG.
In our proposed system, Colour Image has been used for embedding the secrete message. In the proposed technique mostly used random binary digit from multiple pixels instead of LSB technique after converting the stego image into a binary form. Before embedding the secret messages, the Robust Cryptography Algorithm Advanced Encryption Standard (AES) & Pseudorandom Number Generator (PRNG) has been used to encrypting the secret message and secure the confidential data from the unauthorized access.

IV. REVIEW FINDINGS

• Based on the above reviews we are able to find the problems in the existing systems and feature that are to be improved in to the proposed system.
• The reviews helped us lot about the technologies not only the technologies and how the cloud is reaching in various applications.
• From the reviews we realized how important the cloud is and how important the data must be secured and transmitted.

ISSN: 2832-2754 (Online), Volume-2 Issue-6, Nov-Dec 2022, pp.1-4

• Cryptography is not only encrypting and decrypting but also the data must be transmitted from sender to receiver correctly without any attacks.

V. CONCLUSION

In this project, we investigated the problem of data security in cloud data transmission, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme. In the data transmission proposed, method transferred data is encrypted in the upper-layer on top of the transport layer. Thus, the scheme for the performance improvement can be applied without modifying the implementation of IP layer, and efficient secure communications by pre-processing of encryption in the upper- layer are realized. We have applied over to the data at the background using the encryption algorithms. The hashing can be used for effective storing and transmitting without altering data

VI. REFERENCES

[1]https://books.aijr.org/index.php/press/catalog/download/8/3/66-1?inline=1

[2]https://www.researchgate.net/publication/325889056_Secure_Cloud_Using_Cryptography

[3]ttps://www.researchgate.net/publication/325889056_Secure_Cloud_Using_Cryptography

[4]https://aip.scitation.org/doi/10.1063/5.0057961

[5]https://www.researchgate.net/publication/314509549_ENABLING_DATA_INTEGRITY_PROTECTION_IN_CLOUD_STORAGE_USING_CRYPTOGRAPHY

[6]https://www.researchgate.net/publication/364333035_Security_enhancement_using_blockchain_based_modified_infinite_chaotic_elliptic_cryptography_in_cloud

[7]https://www.researchgate.net/publication/323659837_Security_Protocol_for_Data_Transmission_in_Cloud_Computing

[8]https://www.researchgate.net/publication/358796903_Data_Transmission_in_Clouds_using_Heed_and_Energy_Efficient_Routing_Algorithm

[9]https://www.researchgate.net/publication/321697864_Secure_data_transmission_in_CLOUD_using_code_verification

[10]https://www.researchgate.net/publication/342766288_Multilevel_authentication_for_secure_data_transmission_using_RKGM_to_cloud

[11]https://www.researchgate.net/publication/331064065_Homomorphic_Technique_for_Secure_Data_Transmission_in_Cloud_Computing

[12]https://www.researchgate.net/publication/282969924_A_study_on_high_secure_and_efficient_MANET_routing_scheme

[13]https://www.researchgate.net/publication/306044176_An_innovative_DNA_cryptography_technique_for_secure_data_transmission

[14]https://www.researchgate.net/publication/228382926_Quantum_Cryptography_The_Ultimate_Solution_to_Secure_Data_Transmission

[15]https://www.researchgate.net/publication/348694305_A_Multilayer_Cryptosystem_for_Secure_Data_Transmission_using_PRNG