Survey on Securing Data in Cloud at Various Fields

V. Sindhu[1] Dr. B.FathimaMary[2]
[1]M.Phil Scholar
[1,2]Department of Computer Science
[1,2]St. Joseph's College, Tiruchirappalli, Tamil Nadu, India

Abstract— Nowadays securing data in the cloud is a major challenge while transferring information in an open-source. Data is a collection of information and it can be stored in a storage area. Cloud is a temporary storage area used to store the information and it can be easily accessible by the users. Even though accessing data can be done easily but security is an important issue in the cloud storage area. In this survey paper, we discussed the security of data in the cloud in various fields. Therefore many techniques like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Hybrid Encryption and Decryption, Homomorphic encryption, and Symmetric & Asymmetric encryption and decryption are used to secure the data and its privacy.

Keywords: Security, Cloud Storage, Various Fields, Encryption, Decryption

I. INTRODUCTION

Cloud is a storage area used for storing a large amount of data to access the information that we need. Definition of cloud computing by U.S National Institute of Standards and Technology is given as follows, which was already given in the paper Data Security and Privacy in Cloud Storage Environments based on Cryptographic Mechanism, "Cloud computing is a model for enabling

Unambiguous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, application, and services) that can be rapidly provisional and released with minimal management effort or service provider interaction". While sharing a message in an open-source, an intruder can easily steal the message. So security is a major concern, to safeguarding the data while transferring. Cryptography is a method or art of secret writing which is used to send a message or information to the authorized person using private and public keys which was only known by the sender.

This method is used to secure the data from an unauthorized person. Cryptographic Mechanisms play a major role to secure the data. The original message is called plaintext and it will get encrypted with the help of the secret key, and the message is decrypted as cipher text and get back into an original form. Many algorithms and mechanisms are used to maintain confidentiality, Integrity, Scalability, Availability, and Authenticity of data in the cloud. Cloud can also provide the following services Software as a service (Saas), Platform as a service (Paas), and Infrastructure as a service (Iaas) based on their needs. Cloud can be classified into Private cloud, Public cloud, Managed Cloud, Community Cloud, and Hybrid cloud.

A. Issues in cloud security

Security is a major issue while storing or exchanging information in cloud storage. Because anyone can easily steal the information in an open-source. Data loss is another issue in cloud storage. Loss of data happens due to insecurity. Intruders hack or stole the information through an unsecured network. In data integrity, an unauthorized person can easily modify or delete the data. The information was fully modified by intruders, so automatically data loss will happen. Maintaining confidentiality is another issue in cloud security. A user can store their private or confidential data in the cloud which is unsecured. Because the insider threats can easily steal the data from the users. Data portability in the cloud is an issue while it is used in various platforms, and it should be varied from one user to another user. Because some operating systems will not support the other one.

II. LITERATURE REVIEW

In this literature review, we discussed about the security of data in cloud at various fields. Many fields like Medical, IT, Banking and Financial Sectors, E-learning and smart cities using a huge amount of data in database. They need more storage area to store the information. The following fields tells about that, how they use mechanisms and how to store the data inn cloud.

A. In Medical field

Health information of patients will be recorded as PHR (personal health records) contains data regarding to the health issues of patients, records related to employees and financial status of the management. In hospital, records are stored in a database. If it is unsecured, an unauthorised person can easily access the health record information of patients and also they stole the full information of hospital.
The following papers will discussed about the security measures for maintaining the health records of patients.

Thangapandian etal.(2018) proposed the concept that secure the data in health care monitoring using Diffie-Hellman algorithm with Quantum key, Non-Abelian encryption and decryption which is scalable, flexible, efficient communication and reduced time and cost. Limitation of this paper was, complexity will be increased.

Karim Abouel Mehdi et al.(2018)proposed the health care data security using Big Data, with the help of encryption techniques which provide the security and privacy of data. Limitation of this paper was, privacy methods need to be enhanced. Christian Esposito et al proposed cloud based data security and privacy in healthcare using block chain to monitor the health records using Electronic Health Record (EMR). In this paper security, privacy and integrity will be increased. Limitation of this paper was, only smaller size data will be used.

B. In IT field

IT companies stores information about employees, company details, salary details and project details, which are all stored in a database. It can be accessed easily based on their user

needs. Cloud provides the storage area to store the large amount of data. But an unauthorised person hacks the data information while it is transferred through unsecured channel. The following papers discussed about security challenges and how the data will protect from the unauthorized persons.

Vishal et al.(2016) proposed to enhance the security of data in IT field with the help of AES Encryption and Decryption techniques which is rich in availability, confidentiality, integrity and security toprotect the information. Limitation of this paper was computational time will be increased.

C. In Banking and Financial field

In Banking sector and financial services, customer details, account and online transaction details are stored as data. Data can be easily altered or stole by an unauthorised person. So the data must need more security from the intruder. Abishek et al.(2018)proposed system security method for data security and privacy in Banking and financial services which reduces the cost and provides more security to data.

Sneha sakharkar et al.( )proposed a system for Banking and financial services using Homomorphic encryption and RSA algorithm, which provide the security in cloud using data mining techniques, which aims to propose the confidentiality, data privacy and security.

D. In E-learning:

E-learning enhances the learning process in digital learning aids to the users. We can easily get the ready materials anytime, anywhere. Large numbers of study materials and videos are available in many websites.

Sahaya Stalin Jose et al.(2018)proposed secure cloud data storage approach in e-learning systems using DES and Reed Solomon code for distributed data storage security to reduce the storage uploading time.

Neelakantan et al.( )proposed a e-learning , Virtual Lab cloud System which is more efficient for easy learning. Students can easily get the study material and gain more knowledge through e-learning.

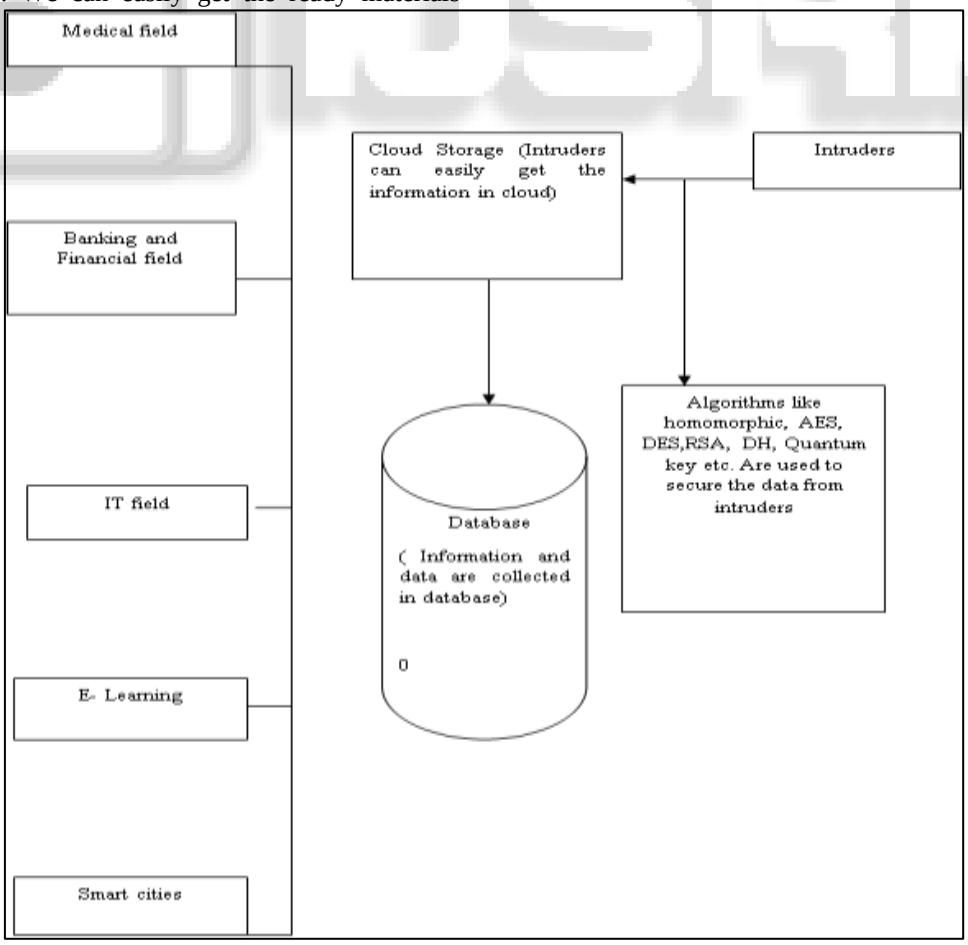
E. In Smart Cities:

Smart cities works based on IoT applications and sensors. For example a smart city includes Educational Institutions, Hospitals, Companies, Industries, Hotels and Many things. It contains large amount of data and storage.

Farahat et al.(2019) proposed a article Data security and Challenges in smart citites using Encryption and Decryption techniques using IoT. Limitation of this paper was low cost authentication and also security is challenge for data storage.

Somnath et al.( )proposed a system for smart cities using sensors to measure the temperature, Pressure, humidity for more crop yield, to gain quality and productivity for crops.

III. BLOCK DIAGRAM FOR THIS SURVEY



IV. TABLE

Various Fields	Techniques	Advantages	Drawbacks
Medical Field	Quantum Key Encryption & Decryption and Non-Abelian Encryption & Decryption	Scalability Flexibility Reduced the time and cost	Complexity increased
IT	Advanced Encryption Standard	Availability Confidentiality High Security	Computational Time Increased
Banking and Financial sectors	Symmetric key Encryption, Homomorphic Encryption	Low cost Security Confidentiality	Enhances security level
E-learning	DES and Reed Solomon code	Availability Flexible Storage uploading time is low	Needs more security
Smart Cities	Encryption and Decryption technique	Authentication Low cost	But security is a challenge. Needs more security

The following table describes the data security and its mechanisms in various fields.

V. CONCLUSION

This survey paper covers the overview of securing the data in the cloud in various fields. Even though there are many algorithm and mechanisms provides more security, integrity, availability, and privacy. Sometimes the complexity is increased, data loss and data leakage will happen, hackers can easily modify or alter the data information. Because of these above issues, in our future work, we will enhance the security level, data privacy, and data loss in cloud storage. The future enhancement will help many cloud users to secure their data information from the intruders.

REFERENCE

[1] M. Thangapandiyan, P.M. Rubesh Anand and K. Sakthidasan, International conference on commerce and signal processing, April 2018, India.
[2] Vishal R. Pancholi and Dr. Bhadresh P. Patel IJIRST|vol 2|Issue 09|Feb 2016|ISSN (online), Enhancement of Cloud Computing Security with Secure Data Storage using AES.
[3] Bih-Hwang Lee, Ervin Kusuma Devi, Mohammed Farid Wajdi, "Data Security in Cloud Computing Using HEROKU Cloud", The 27th wireless and optical communications conferences(WOCC 2018),
[4] Zheng Yan, Robert H.Deng and Vijay Varadharajan, "Cryptography and Data Security in Cloud computing", Institutional knowledge at Singapore Management University, 2017.
[5] Shweta Kaushik, Charu Gandhi, "Cloud Data Security with Hybrid Symmetric Encryption", (ICCTICT), 2016.
[6] John Harauz, Lori M. Kaufman, Bruce Potter "Data security in the world of cloud computing", 2009.
[7] Saira Varghese, S. Maria Celestian Vigila, "A Comparative Analysis on Cloud Data Security",(GCCT 2015).
[8] Nesrine Kaaniche, Maryline Laurent, "Data Security and Privacy presentation in Cloud Storage Environments based on Cryptographic Mechanisms", 2017.
[9] Dr. L.Arockiam, S. Monikandan, " Data Security and Privacy in Cloud Storage Using hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol.2, Issue 8, 2013.
[10] Karim Abouelmehdi, Abderrahim Beni Hessane and Hayat Khaloufi, "Big Healthcare Data Preserving Security and Privacy", 2018.
[11] Pradeep Senwal, Mahesh Kumar Sharma, "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing", 2017.
[12] Abhishek Mahalle, Jianming yong, Xiaohi Tao and Jun Shen, "Data Privacy and System Security for Banking and Financial Services Industry based on cloud computing Infrastructure", IEEE, 2018.
[13] I.S. Farahat, A.s.Tolba, Mohamed Elhoseny and Waleed Eladrosy, "Data Security and Challenges in Smart Cities", Springer Nature Switzerland AG 2019.
[14] G. Sahaya Stalin Jose, C. Seldev Christopher, "Secure Cloud data storage approach in e-learning systems", Springer Nature 2018.
[15] M. Geetha, K. Akila, "Cryptography Optimization Algorithms", IJETIE, vol 5, Issue 1, 2019

