IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 1, November 2022

Privacy—Preserving Media Sharing With Scalable Access Control and Secure Deduplication in Cloud Computing

Prof. Aditi Patil[1], Nikita S. Walunjkar[2], Shivani A. Dhamankar[3], Gaurav P. Patil[4], Vishal R. Boddula[5]

Professor, Department of Computer Engineering[1]

Students, Department of Computer Engineering[2,3,4,5]

SKN Sinhgad Institute of Technology and Science, Kusgaon (BK), Pune, Maharashtra, India

Abstract: *With the aim to save cloud storage space, safe deduplication algorithms have been developed. We will begin with AES encryption algorithm; it encrypts the messages using a message-derived key. In the result, we found out that identical plaintexts generate similar ciphertexts. AES encryption algorithm encompasses convergent encryption and provides precise security definitions, was proposed. Cloud computing is the advancement of sharing very large amounts of data via network. There are multiple approaches available for providing data security in the cloud storage space. Whereas present approaches are more closely tied to the ciphertext. So, we are suggesting a cloud-based data collection, sharing, and restricted dissemination plan that will preserve multi -owner privacy, in this paper. In this, the database owner will be able to securely share confidential data with a group of clients through the cloud.*

Keywords: Cloud Computing

I. INTRODUCTION

It is a network-based computer system with a very large storage space where only authorized users will be able to access the platform from anywhere and at any time using a good internet or network connection. Secure deduplication solutions have been proposed to preserve cloud storage space because of increasing development of media content.

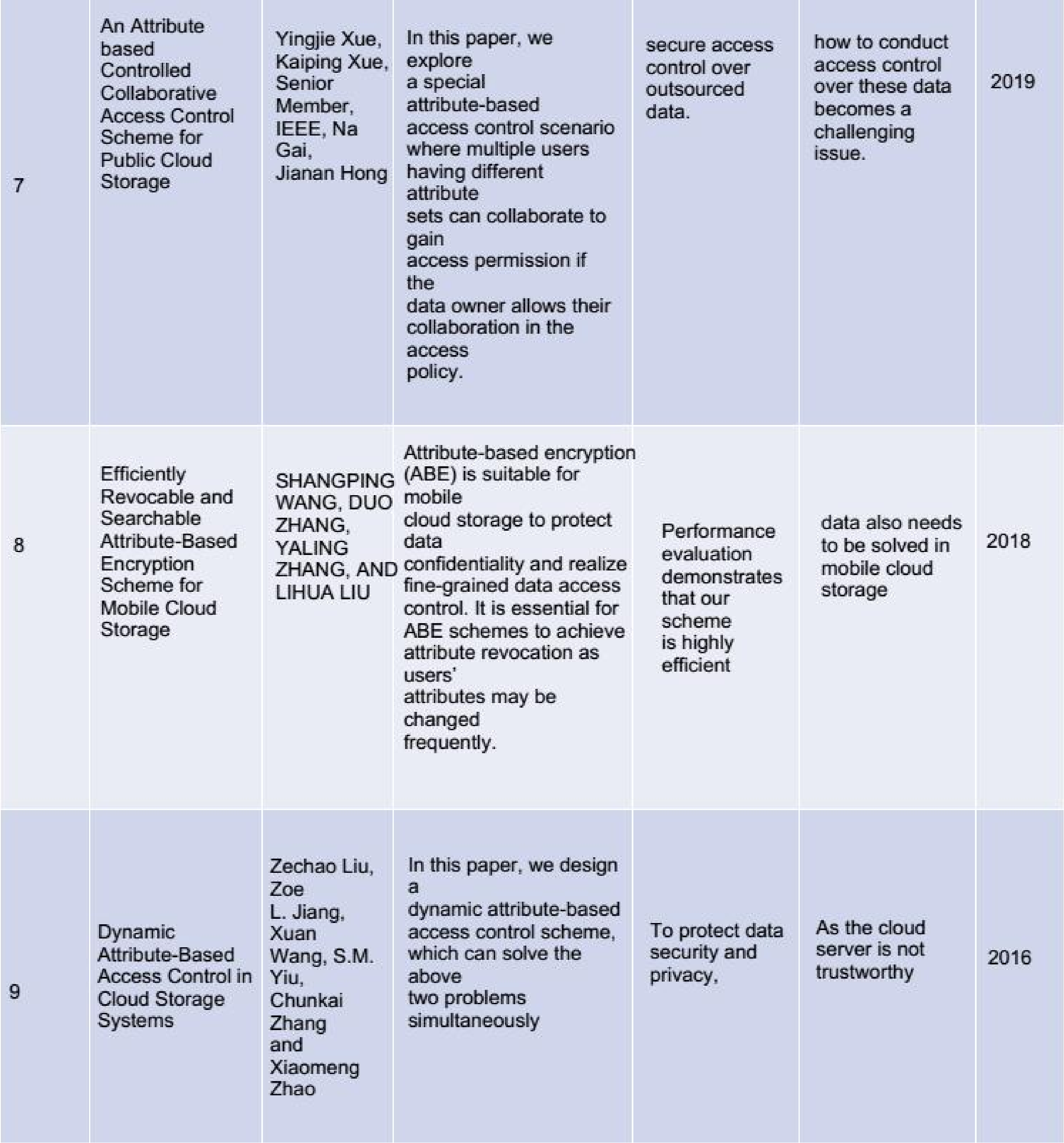
In the beginning, the AES encryption algorithm was established, which uses a message -derived key, for message encryption. In the result, we found out that identical plaintexts generate similar ciphertexts. AES encryption algorithm encompasses convergent encryption and provides thorough security, was proposed. It is the advancement of sharing huge amounts of data via network. There are multiple methods for delivering data security in the cloud. Whereas present approaches are more closely tied to the ciphertext. As a result, we propose that data should be gathered, shared, and distributed in a controlled environment. We need to create a plan that can protect the privacy of several owners, in the cloud. The owner of the data will be able to share this data here and store the data securely

DOI: 10.48175/568

II. LITERATURE SURVEY

Sr. No	Paper	Author	Description	Advantages	Diadvantages	year
1	Attribute-based st ttribute-based storage suppor age supporting secur ting secure deduplication of e deduplication of encrypted data in cloud.	Hui CUI, Robert H. DENG,Ying jiu LI,Guowei WU	Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with users possessing specific credentials (or attributes)	it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys.	the standard ABE system does not support secure deduplication	2017
2	Usage of DHS and De-duplicating Encrypted Data using ABE & ECC for Secured Cloud Environment.	N Sandeep Chaitanya, S Ramachandr a m	In our paper, we have used a deduplication technique with a secured data attribute based encryption using ECC (Elliptic Curve Cryptography) in multi cloud setting.	Compared to other systems we have designed data confidentiality with settings of access policy avoiding the share of decryption keys.	is choosing a few reasonable mists	2018
3	A Review on Attribute Based Encryption .	Nikhil Chaudhari1, Mohit Saini, Ashwin Kumar, Priya G	This paper presents an Attribute-Based access to the media within the cloud wherever it uses cipher-text policy Attribute-Based encryption (CP-ABE) technique to make associate access management	cloud storage providers are secure and cannot be hacked	some authorities could compel cloud storage suppliers to form public user secrets	2016

4	Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems.	RUI GUO , HUIXIAN SHI, QINGLAN ZHAO, AND DONG ZHENG	In this paper, to guarantee the validity of EHRs encapsulated in blockchain, we present attribute - based signature scheme with multiple authorities, in which a patient endorses a messageaccording to the attribute while disclosing no information other than the evidence that he has attested to it	The comparison shows the efficiency and properties between the proposed method	there are multiple authorities without a trusted single or central one to generate	2018
5	Privacy Preserving Attribute-Based Keyword Search in Shared Multi owner Se	Yinbin Miao, Ximeng Liu, Kim-Kwang Raymond Choo, Senior Member	In addition, due to privacy concerns on access policies, most existing schemes are vulnerable to off-line keyword-guessing attacks if the keyword space is of polynomial size.	We also evaluate their performance using real-world datasets	without incurring high computational and storage costs	2019
6	Revocable, Decentralized Multi-authority Access Control System	Ruqayah R. AlDahhan, Qi Shi, Gyu Myoung Lee, Kashif Kifayat	in this paper, we propose a new CP-ABE scheme that tackles most of the existing work's limitations and securely allows storing data on a public cloud storage system by employing multiple authorities which manage a joint set of attributes	securely allows storing data on a public cloud storage system by employing multiple authorities which manage a joint set of attributes.	this type of technique mainly supports storing data only on a private cloud storage system	2018



7	An Attribute based Controlled Collaborative Access Control Scheme for Public Cloud Storage	Yingjie Xue, Kaiping Xue, Senior Member, IEEE, Na Gai, Jianan Hong	In this paper, we explore a special attribute-based access control scenario where multiple users having different attribute sets can collaborate to gain access permission if the data owner allows their collaboration in the access policy.	secure access control over outsourced data.	how to conduct access control over these data becomes a challenging issue.	2019
8	Efficiently Revocable and Searchable Attribute-Based Encryption Scheme for Mobile Cloud Storage	SHANGPING WANG, DUO ZHANG, YALING ZHANG, AND LIHUA LIU	Attribute-based encryption (ABE) is suitable for mobile cloud storage to protect data confidentiality and realize fine-grained data access control. It is essential for ABE schemes to achieve attribute revocation as users' attributes may be changed frequently.	Performance evaluation demonstrates that our scheme is highly efficient	data also needs to be solved in mobile cloud storage	2018
9	Dynamic Attribute-Based Access Control in Cloud Storage Systems	Zechao Liu, Zoe L. Jiang, Xuan Wang, S.M. Yiu, Chunkai Zhang and Xiaomeng Zhao	In this paper, we design a dynamic attribute-based access control scheme, which can solve the above two problems simultaneously	To protect data security and privacy,	As the cloud server is not trustworthy	2016

III. PROPOSED SYSTEM

We are going to use the AES encryption algorithm for encryption and decryption in the suggested system, as well as data security and secure access management. The MD 5 algorithm will be used for avoid data duplication.

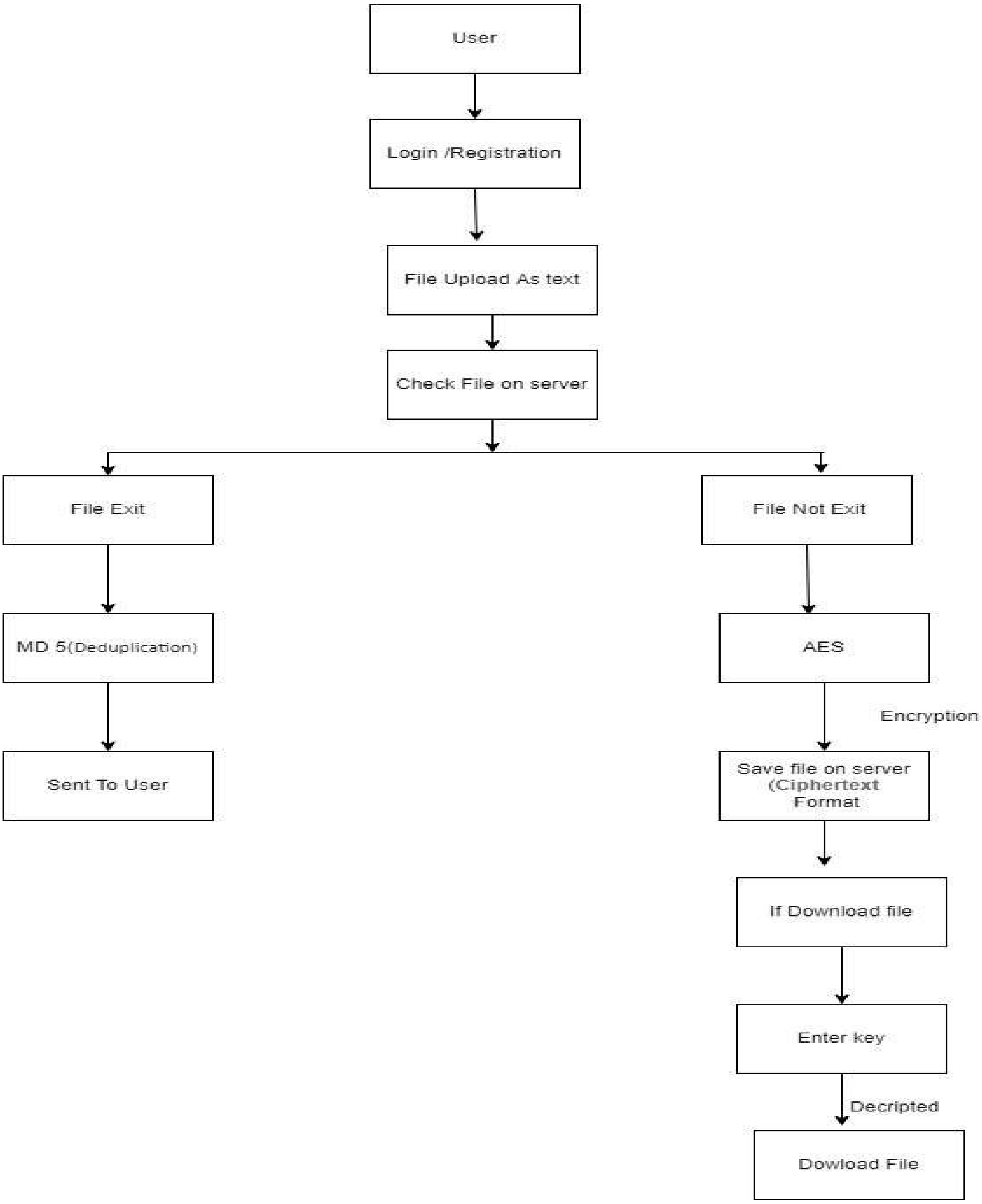


Figure 1: The System Architecture.

IV. ALGORITHM

AES algorithm is a symmetrical block cypher method which accepts plain text in format of 128-bit blocks and converts it into ciphertext using keys of 128, 192, and 256 bits. The AES algorithm is a worldwide standard because it is considered one of the most secure algorithms. The Advanced Encryption Standard (AES) algorithm is a symmetric block cypher that the United States government has chosen with aim to safeguard confidential data. AES algorithm is used to encrypt sensitive data in software and hardware all over the planet. It is very critical for government computer security, cybersecurity, and data security.

MD5: The MD5 message-digest technique produces a 128-bit hash value and it is cryptographically broken but still used frequently. Even though MD5 was created with the aim of being used as a cryptographic hash function, it has been discovered to have multiple flaws. Java is an object-oriented programming language with a high level of abstraction and as few implementation dependencies as possible. Java applications are normally compiled to bytecode, which can execute on any Java virtual machine, regardless of the computer architecture.

V. CONCLUSION

1. Deduplication is an Important technique to save the storage
2. Space and network bandwidth ,Which eliminates duplicate copies of identical data

REFERENCES

[1]. Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, “Secure, efficient and revocable multi-authority access
[2]. control system in cloud storage,” Computers Security, vol. 59, pp. 45–59, 2016.
[3]. J. Li, H. Yan, and Y. Zhang, “Certificateless public integrity checking of group shared data on cloud storage,” IEEE Transactions on Services Computing, pp. 1–12, 2018.
[4]. J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, “Flexible and fine-grained attribute-based data storage in cloud
[5]. computing,” IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785–796, Sept 2017.
[6]. J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, “User collision avoidance cp-abe with efficient attribute
[7]. revocation for cloud storage,” IEEE Systems Journal, pp. 1–11, 2017.
[8]. H. Wang, Z. Zheng, L. Wu, and P. Li, “New directly revocable attribute-based encryption scheme and its application in cloud storage environment,” Cluster Computing, vol. 20, no. 3, pp. 2385–2392, Sep 2017. [Online].
[9]. T. Taleb, A. Ksentini, M. Chen, and R. Jantti, “Coping with Emerging Mobile Social Media Applications Through Dynamic Service Function Chaining,” IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 2859–2871, Apr. 2016.
[10]. K. Yang, Z. Liu, X. Jia, and X. S. Shen, “Time-Domain Attribute Based Access Control for Cloud-Based
[11]. Video Content Sharing: A Cryptographic Approach,” College Short Form Name, Department of
[12]. Computer Engineering 2021 44 IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 940–950, May 2016
[13]. M. J. Atallah, K. B. Frikken, and M. Blanton, “Dynamic and Efficient Key Management for Access Hierarchies,” in Proceedings of the 12th ACM Conference on Computer and Communications Security, 2005, pp. 190–202.
[14]. C. Ma, Z. Yan, and C. W. Chen, “Scalable Access Control for Privacy-Aware Media Sharing,” IEEE
[15]. Transactions on Multimedia, vol. 21, no. 1, pp. 173–183, Jan. 2019.
[16]. H. Cui, R. H. Deng, Y. Li, and G. Wu, “Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud Transactions on Big Data, pp. 1–1, 2019.

DOI: 10.48175/568