iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46518

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VIII Aug 2022- Available at www.ijraset.com

Data Integrity on the Cloud Computing using Algebraic Signature

Uma S[1], Mr. Jayaprakash D[2], Dr. Vasanthi R[3], Mrs. Subhashini S. M. C.[4]
Narasu's Sarathy Institute of Technology

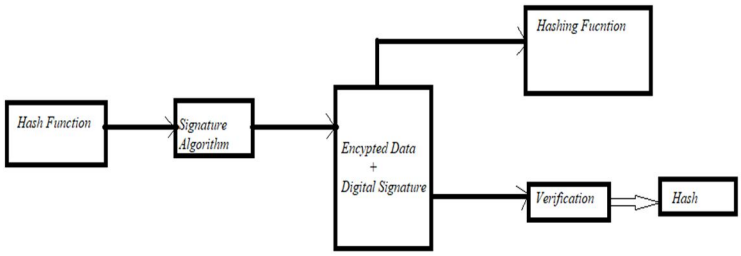
Abstract: ***The Trends of Cloud Computing, the cloud security work must be important because the huge number of data with specialized connections to distribute data processing among the various servers. Client stores their data on cloud server to maintain their data privacy and data security. The popular data security method which is called cryptography taking more time and space to encrypt and decrypt for data auditing processes. The existing method is Provable Data Possession which is dynamically operates the data and gives the high computation space and time complexity. So to avoid that complexity the proposed method is called as Algebraic Signature to used low computation performance time and low data space for large data set. It is based on data integrity method for providing good data security on the cloud for large organization also. This proposed method is used the Third Party Auditing method which is to provide large data file security with the Hashing technique using Algebraic Signature method. The conclusion of this paper is providing the data integrity and time efficiency of the process using TPA method also provides the dynamic operation.***

Keywords: Cloud Service Provider, Algebraic Signature, TPA and Hash technique.

I. INTRODUCTION

Cloud Computing is the famous method for server service provider and distributed processes. Cloud computing is used to make millions of data and its users into a single platform. The CSP is a large service provider for the big to small organizations where the data is stored. It is used to operating more effectively data storage and security and improving their large data set productivity to organizations. These are the tools and applications that are integrated into the cloud server that can be accessed from anywhere by the user. To improve the data integrity method, the cloud uses the Third party auditing method to protect the data files. Previously the Provable Data Possession method where used for the data integrity but this is used only for restricted data files only not widely. The Algebraic Signature method used for large dataset and provides better data integrity service to the user's own data. It is used to provide data authentication with effective method of TPA. Here every user will have separate user accounts methods to have their own data on the cloud server. Cloud computing is used as a huge group of servers with a large set of connections to distribute the data processing among the many servers. If they need to maintain their data on the cloud server it should safe and security manner and also to access the data in effective with time efficency.Today many of the people uses digital marketing and also uses large data processing on the web services. Mainly the user's data should be secure and timing efficiency on the cloud computing. In the cloud computing data integrity is the effective process to provide data security and deal with the dynamic operation. It is the protocol to make the data integrity for user's data and TPA provides to audit the user's data for both user and CSP. In this process cloud computing uses the three tier methods. That is CSP, TPA and data owner. Clients need to store their data on cloud servers to maintain their data without any data loss. CSP is the largest data operations of service providers where data is stored and provides applications to the organizations. For the data security here we used hashing function to provide data security using Signature algorithm. Here while doing hashing function the data will be provided to the signature algorithm and also it will process the data security with encrypted data.

Working function of Algebraic Digital Signature



©IJRASET: All Rights are Reserved

The main purpose of algebraic Signature is checking whether the remote data is stored completely on a cloud server. In this method we get instance of the signature object passing the signing algorithm and assign it with public key and finally pass the input this will return byte array. The Hashing function is used to define data files and it is used to explore the verification method by using the signature algorithm method in the format of algebraic expression. Then it will be process the data integrity by using digital signature to encrypt the data. Here the data will be the at verification level and hash function will be executed.

A. Converting Hash Signature HKEY into Segments

1) Pick any byte from HKEY

```
#Byte=char(HKEY,10);
```

2) Obtain its rank in [0:255] range expression

```
Rank=rank(HBYTE)
Rank=input(HBYTE,pi);
```

3) Use the Divide and conquer method function to split the ranks into segments from 1 to N.

```
Segment=1+mod(rank,N);
```

II. LITERATURE SURVEY

A. Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

The main purpose of this paper is to ensure security and the user's data is usually encrypted before it's outsourced to the cloud to avoid data losing. It is critical tasks for the CSP as the users expect the cloud to conduct a quick search and return the result without lose data. To overcome these problems, here proposes a ciphertext-policy attribute-based mechanism with keyword search and data sharing for encrypted cloud data.

B. Data Security and Privacy Production for Cloud Storage: A Survey

The new development trends called Internet of Things, digital Smart city, enterprises business digital transformation and world's digital economy are at the top of the tide. The fast growth of data storage pressure drives the rapid development of the entire data storage market on account of massive data generated. By providing data storage and Management, cloud storage system becomes an indispensable part of the new area. Currently the government, enterprise and individual users are actively migrating their data to the cloud. The good performance of cloud in the digital economy, enterprise digital transformation, Internet of Things and other fields, we confirm that cloud computing and cloud storage will be the mainstream.

C. A Verifiable Semantic Searching Scheme by Optimal Matching over Encrypted Data in Public Cloud

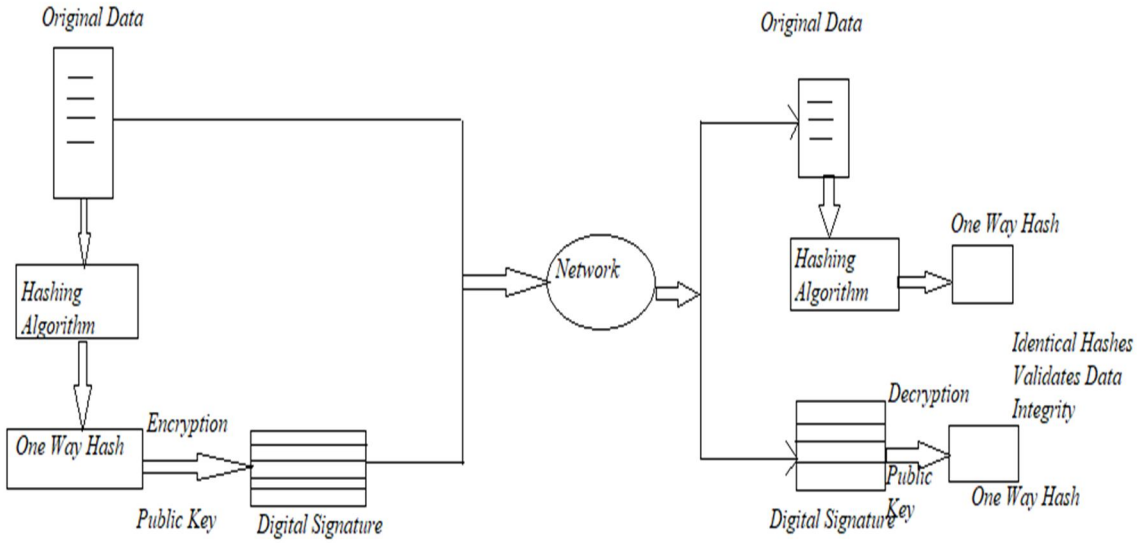
Semantic Searching over the encrypted data is a very crucial task. So to provide retrieval service to client data and search results and be flexible. This paper provides a secure verifiable semantic searching scheme. For semantic optimal matching on ciphertext, we formulate word transportation problems to calculate the minimum word transportation cost as the similarity between queries and documents and propose a secure transformation to transform word Transportation problems into Random Linear Programming problems to obtain the encrypted Minimum Word Transportation Cost. For verifiability the duality theorem of Linear Programming to design a verification mechanism using the intermediate data produced in the matching process to verify the correctness of search results.

D. TPA Auditing scheme for Cloud Storage

Cloud Computing is the service provider by Cloud Servers in which data is maintained, managed, backed up remotely and available to users data over a large network. The user is concerned about the security of data stored in the cloud as the user's data can be attacked or modified or leaked by outside attackers. Therefore the concept called data auditing is introduced which checks the integrity of user's data with the help of an entity called TPA. The main purpose of this concept is to develop an integrity auditing scheme which is secure, efficient to use and possesses the capabilities such as privacy preserving, public auditing and maintaining the user's data integrity along with confidentiality. Thus the TPA auditing scheme has been developed by considering all these requirements. It consists of three entities which are Data Owner, TPA and Cloud Server. The auditing scheme makes use of AES algorithm for encryption, SHA-2 for Integrity check and RSA signature for digital signature calculation.

©IJRASET: All Rights are Reserved

III. SYSTEM ARCHITECTURE



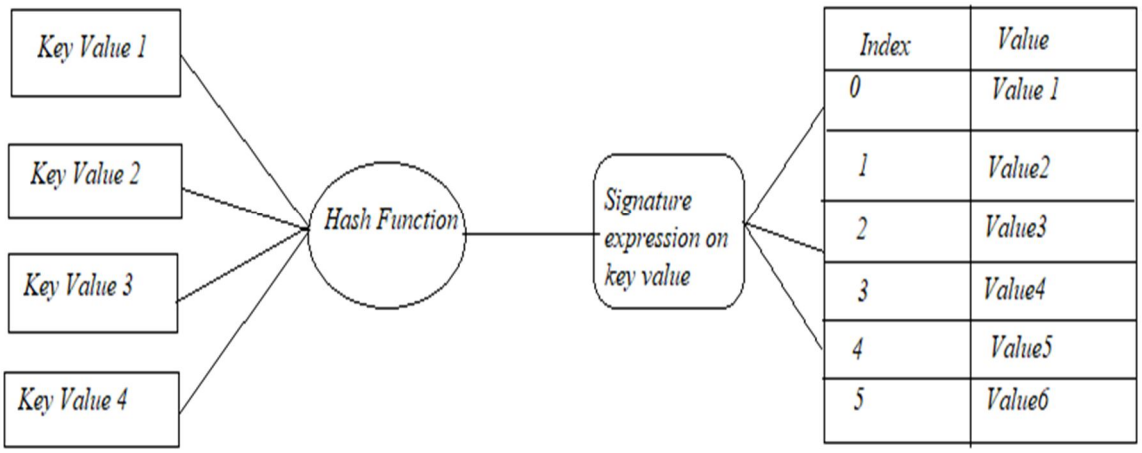
IV. EXISTING SYSTEM

In the existing system the Provable Data Possession is used to give the integrity to the data. This method is used for public data integrity so the process speed is low and also it is doing for only specific method or concept. But we need to give data integrity for all the data. In this PDP method, the data is organized through the linked list on the given operation. Here also we used to gives the dynamic operation of the data process method on PDP.In this data integrity is given to the entire user's data randomly. So that the data process speed will in very slow. The data is processing in sequential method, so that the data integrity can be give to particular data only. Nowadays the cloud server handling many data transaction method for large data set. So that the data can be handled in every minute which is very carefully. The existing method that is PDP will not be the best solution. We need to handle the large data transactions and methods to have effective data integrity.

V. PROPOSED METHODOLOGY

In the proposed method we will use the Third Party Auditing method to handle the large set of data transaction on the Cloud Computing. In This method we need to have three entities which is owner, TPA and CSP.The data transaction method is handling data in large size and the data should process in efficient method and also dynamic data operation like insertion, updating and deletion of data file. In the digital world everything is depends on digital platform. Examples are digital marketing, digital economics and digital news world. So these digital methods can handle only with the large data sets or data files for the large operations or transactions. For these large transactions we need to have the better security methods to deal with large data file sets transactions of data owner, whether it may be the single user or Big Organizations. These security methods can be handled using cryptography method or digital signature methods. In the existing system there are PDP method used for data integrity in the linked list method. The PDP method can be used only for the limited data and used in public data sets. But the proposed method is used for the efficient data integrity and methods which is used for data owner. Commonly the hashing technique is used to convert the key values into the index of an array. Here we will apply the algebraic method to provide the data integrity method. In this method the value has been taken as key value and processing with the hash function to convert into the actual value. Then the converted value should be process with digital signature which is applying expression to data for data integrity. So here the data will be protect without using external security method. This algebraic method can evaluate the data with expression like a0, a1, a2, a3…….a_n. This data can be handling over the single word content like $\sum a_i$. In This a_i will carry all the data from a0, a1……..a_n with the single a_i. By this we can reduce the time of data transfer method and also we can make easy of data transaction over the large data set.

Diagram for Hash Function with Signature



A. Pseudo code for uploading a file into Cloud Server

Encrypting file(x)

- Algorithm to encrypt file onto cloud storage to transform Clair text in file X into Cipher text in file X.

```
Phase1: Encrypt Clair text with CSL algorithm.
For Y (1) to number of block(X) do
{
        Y=ENC_CSL(Y, K)
}
        Send_to _cloud ('X')
        Phase2: Generate Hash with BLANE3 Algorithm
        For k (1) to SizeOf (k) do
        {
                K=Hash_BlakE3 (K)
        }
        Store_in_Server (k)
```

B. Applying Hash Function on File:

- Concatenating all the key components, for example the input file as variable TRANS:
  CONCAT=catx(':',ID,KEY);
- Pass the result to hash function MD5 to obtain its signature, HKEY:
  length HKEY $lb;
  HKEY=MD5(CONCAT);
- We can also use Single Exprssion:
  HKEY=put(MD5(catx(':',ID,KEY)$lb));
- Hash Signature HKEY for sample File TRANS:

```
data vTransmap/view=vransMap;
set Trans;
CONCAT=catx(":",ID,KEY);
Format HKEY $hex32;
*length=16;
HKEY=MD5(CONCAT);
Keep ID KEY HKEY;
Run;
```

VI. COCLUSION AND FUTURE ENHANCEMENT

Thus the user's data can get the integrity from anywhere and it can get protected by using hashing technique with the signature. Here we can provide complete security for the user's data by using algebraic signature method and also from the Cloud Computing the data can get arranged according to the user's requirement. In the PDP method we can provide only the particular data. But in this algebraic signature method we can get data integrity for the large set of data and also with public mode. The data can be organization, government sectors and also for the individual data. In future we will apply for the divide and conquer algorithm for the big data dealing like online shopping-Commerce and also for government sectors. If we use this algorithm method we can handle the large data set without confusing the information searching on the cloud computing. Moreover we can apply for the Big Data concept also for the large set of data and files. Here we mentioned the Files as the data because we will handle by using the algebraic method.

REFERENCES

[1] Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski and L. Fang, "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 2787-2800, 1 Nov.-Dec. 2021, doi: 10.1109/TDSC.2020.2963978.

[2] P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

[3] W. Yang and Y. Zhu, "A Verifiable Semantic Searching Scheme by Optimal Matching Over Encrypted Data in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 100-115, 2021, doi: 10.1109/TIFS.2020.3001728.

[4] SmitaChaudhari and Gandharba Swain, "Efficient and Secure Group based Collusion Resistant Public Auditing Scheme for Cloud Storage" International Journal of Advanced Computer Science and Applications(IJACSA), 12(3), 2021. http://dx.doi.org/10.14569/IJACSA.2021.0120356

[5] SEzhilArasu, B Gowri, and S Ananthi. Privacy-Preserving Public Auditing in cloud using HMAC Algorithm. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277, 3878, 2013.

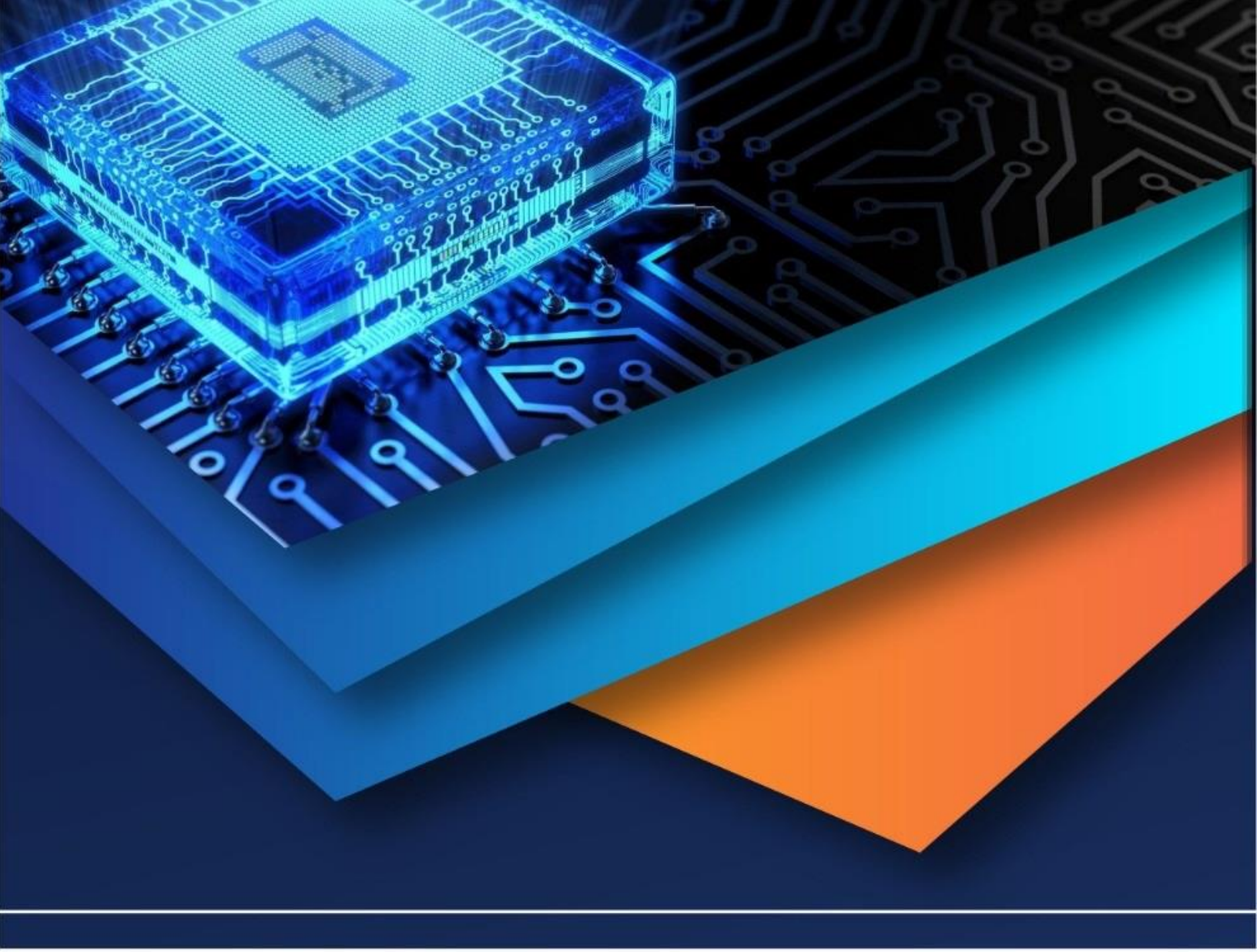
[6] Abbdal, Salah H., Hai Jin, DeqingZou and Ali A. Yassen. "Secure Third Party Auditor for Ensuring Data Integrity in Cloud Storage." 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (2014): 510-517.

[7] Li, Ling et al. "Study on the third-party audit in cloud storage service." 2011 International Conference on Cloud and Service Computing (2011): 220-227.

[8] W. Li, X. Li, J. Gao and H. Wang, "Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments" in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 03, pp. 1276-1290, 2021.doi: 10.1109/TDSC.2019.2909890

[9] A. d. Santos, T. I. Syed, M. C. Naldi, R. J. G. B. Campello and J. Sander, "Hierarchical Density-Based Clustering Using MapReduce," in IEEE Transactions on Big Data, vol. 7, no. 1, pp. 102-114, 1 March 2021, doi:10.1109/TBDATA.2019.2907624.

[10] K. Gai, M. Qiu and H. Zhao, "Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing," in IEEE Transactions on Big Data, vol. 7, no. 4, pp. 678-688, 1 Oct. 2021, doi:1109/TBDATA.2017.2705807.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)