IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11634

DATA SECURITY AND PRIVACY PROTECTION FOR CLOUD STORAGE

N. Usha[1], N. Shabnam Sulthana[2], J. Vinothini[3]

Student, B.E. Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1,2]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[3]

Abstract: The development of cloud computing era with the explosive increase of unstructured records, cloud storage era gets more interest and better development. The cloud provider does not have pointers regarding the statistics and the cloud facts saved and maintained globally everywhere within the cloud. The privateness safety schemes are typically based totally mostly on encryption era. there are many privateness keeping strategies in the facet to prevent facts in cloud. We propose a three factors of storage framework primarily based on fog computing. The proposed framework can each take whole benefit of cloud storage and guard the privacy of data. here we're the use of Hash-Solomon code set of rules is designed to divide statistics into specific components. If the simplest facts aspect missing we lost the information records. on this framework we are using bucket idea based totally algorithms and secure the records data after which it could show the security and performance in our scheme. moreover, based on computational intelligence, this set of regulations can compute the distribution percent stored in cloud, fog, and local system. patron releases their utility on a hosting environment which can be accessed through network from diverse clients via application users.

Keywords: cloud Computing, Pointers, Hash-Solomon, privateness, Encryption, Fog Computing, Computational intelligence

I. INTRODUCTION

Cloud computing describes a kind of outsourcing of laptop services, just like the manner wherein electricity deliver is outsourced. customers can virtually use it. They do no longer need to worry in which the energy is from, how it's far made, or transported. each month, they pay for what they consumed. The idea behind cloud computing is similar: The consumer can honestly use storage, computing electricity, or particularly crafted development environments, without having to worry how those paintings internally. Cloud computing is normally net-based totally computing. it is a fashion of computing wherein associated abilities are provided “as a carrier”, permitting customers to get entry to era-enabled services from the internet ("within the cloud") without information of, or manipulate over the technologies in the back of these servers. Fog computing may be perceived both in huge cloud structures and huge records systems, making reference to the growing problems in accessing records objectively. The TSL framework can supply consumer a certain energy of management and effectively defend person’s privacy. Combining with the fog computing version, the 3 components of records can be stored inside the cloud server, the fog server and consumer’s local system consistent with the order from large too small.

1.1 OBJECTIVE

Cloud storage additionally causes a chain of comfy issues. whilst the use of cloud garage, customers do not truly control the bodily garage in their facts and it consequences inside the separation of possession and control of facts. so as to remedy the trouble of privacy protection in cloud garage, we propose a TLS framework based totally on fog computing model and layout a Hash-Solomon set of rules. The three parts of cloud storage shops in to the three exclusive parts of statistics elements. If the only statistics part lacking, we misplaced the facts, on this proposed framework the usage of the bucket concept primarily based algorithms.

1.2 SCOPE

- A three parts of privacy preserving Cloud garage Scheme primarily based on Computational Intelligence in Fog Computing.
- The privateness protection is our attention, some energetic attacks are beyond the scope of this paintings.
- The three parts of cloud storage shops in to the 3 extraordinary parts of facts elements.
- If the one information element lacking.
- we misplaced the information facts.
- On this proposed framework the usage of the bucket concept, based algorithms.
- We use BCH code algorithm. It’s excessive bendy.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11634

II. ANALYSIS

2.1 SYSTEM ANALYSIS

We design a three elements of garage framework based on fog computing. The proposed framework can each take full gain of cloud garage and guard the privateness of statistics. here we're using Hash-Solomon code algorithm is designed to divide facts into distinctive components. If the only records element lacking. we lost the facts data. on this framework we're using bucket concept, based algorithms and comfy the statistics information after which it can display the safety and efficiency in our scheme.

2.1.1 Problem Definition

The privateness problem is particularly significant amongst those safety problems. the security of outsourcing information is still a essential hassle of part computing statistics safety. Confidentiality, Integrity, Availability, Authentication and get right of entry to control, privateness requirement.

2.1.2 Existing System

Recent years witness the development of cloud computing generation. With the explosive boom of unstructured statistics, cloud storage era receives extra attention and better development. The pc era has evolved swiftly. Cloud computing has progressively matured thru so many human beings attempts. In current storage schema, the consumer's data is definitely saved in cloud servers. If the user lose their right of control on records and face privacy threat. The privateness protection schemes are normally based totally on encryption era. these varieties of techniques can't correctly withstand assault from the interior of cloud server.

ALGORITHM USED

AES algorithm - The AES encryption algorithm is a symmetric block cipher algorithm that has a block size of 128bits. It converts these individual blocks using keys of 128, 192, and 256 bits. When, it encrypts these blocks, it joins them together to create the ciphertext. It's supported by a substitution-permutation network, also mentioned as an SP network. It consists of a series of operations, including replacing the inputs with specific outputs and bit shuffling.

DISADVANTAGES

- Changes in the understanding of risk as a result of extending the data center into the cloud.
- Low latency and location awareness.

2.1.3 Proposed system

The framework can take complete of cloud garage and guard the privateness of information. the cloud computing has attracted amazing attention from different sector of society. The 3 parts of cloud garage shops in to the 3 exclusive elements of records components. If the only statistics component missing, we misplaced the information facts. in this proposed framework the usage of the bucket idea-based algorithms.

ALGORITHM USED

BCH code algorithm - The Bose–Chaudhuri–Hocquenghem codes (BCH codes) form a class of cyclic error-correcting codes that are constructed using polynomials over a finite field, the key features of BCH codes is that during code design, there is a precise control over the number of symbol errors correctable by the code. In particular, it is possible to design binary BCH codes that can correct multiple bit errors.

Hash-Solomon algorithm - Hash-Solomon code algorithm is designed to divide data into different parts. using,Hash-Solomon code will produce a portion of redundant data blocks which will be used in decoding procedure. Increasing the number of redundant blocks can increase the reliability of the storage, but it also results in additional data storage.

Secure hashing algorithm - SHA stands for secure hashing algorithm. A hashing algorithm shortens the input smaller form that cannot be understood by using bitwise operations, modular additions,and, compression functions. Hashing is similar to encryption, the only difference between hashing and encryption is that hashing is one-way, meaning once the data is hashed,

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11634

the resulting hash. digest cannot be cracked. SHA works in such a way even if a single character of the message changed, then it will generate different hash.

ADVANTAGES

- In our machine we the use of a bucket concept so reduce the facts wastages and reduce the manner timings.
- we are the usage of a BCH (Bose–Chaudhuri–Hocquenghem) code algorithm. It's high bendy.
- BCH code are used in lots of communications application and coffee amount of redundancy.

III. SYSTEM DESIGN

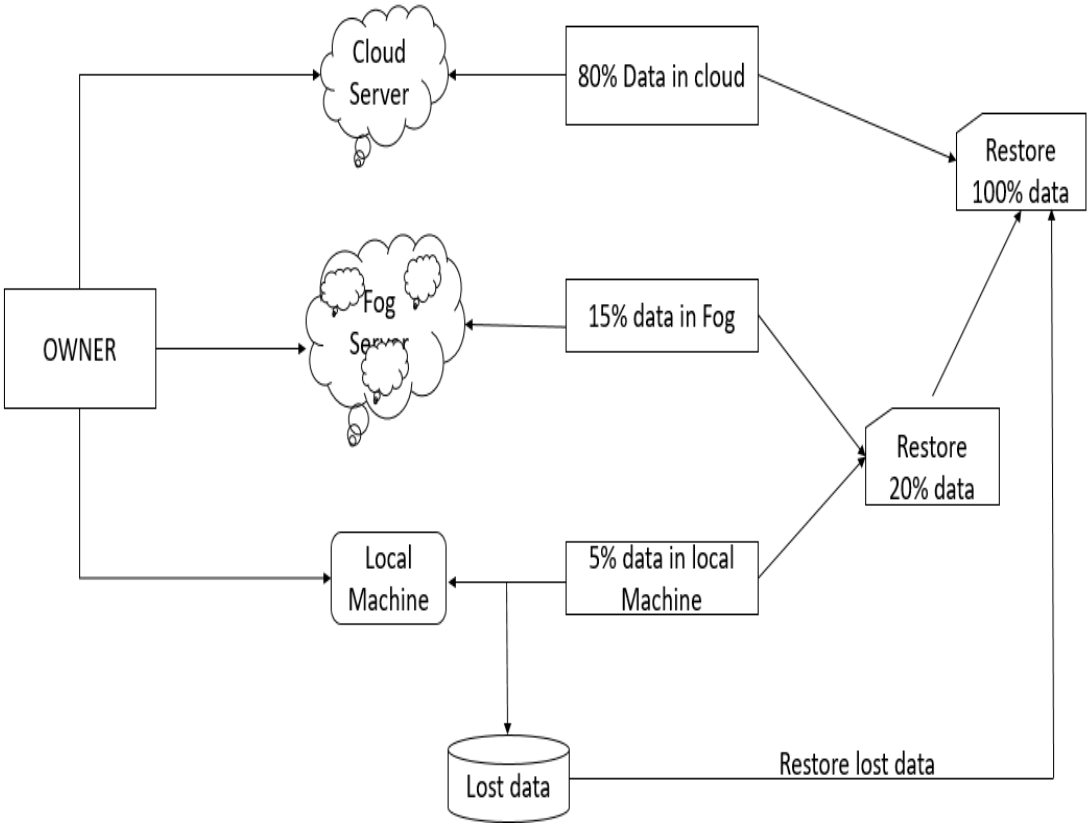

Figure 1. Over all Architecture Design

IV. MODULES

4.1 Login module
4.2 Registration module
4.3 Storage scheme
4.4 Recovery scheme

4.1 LOGIN MODULE:

This is the first interest that opens when person open the website. user wishes to provide a accurate contact variety and password, which person enters at the same time as registering, so one can login into the internet site. If information supplied with the aid of the person fits with the records in the database table, then user effectively login into the website else message of login failed is displayed and person need to reenter accurate statistics. A link to the check in interest is also supplied for registration of recent users.

4.2 REGISTRATION MODULE:

A new person who wants to access the webpage desires to sign up first earlier than login. with the aid of clicking on sign up button in login interest, the sign in interest receives open. a brand new user registers by way of getting into full call, password

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.11634

and phone quantity. A consumer wishes to enter password again in verify password textbox for confirmation. while consumer enters the data in all textboxes, on the press of signup button, the facts is transferred to database and user is directed to login interest once more. Registered person then wishes to login to be able to get entry to the website. Validations are implemented on all of the textboxes for correct functioning of the website. Like statistics in each textbox is must this is every textbox, both its far of name, touch, password or affirm password, will now not be empty even as registering. If this type of textbox is empty app will provide message of records is ought to in every textbox..also facts in password and verify password fields have to in shape for a success registration. some other validation is contact quantity have to be legitimate one that is of 10 digits. If such a validation is violated then registration might be unsuccessful after which consumer needs to sign up again. Message that website will display when one of the subject is empty. If all such information is correct person will be directed to login hobby for login into the webpage.

4.3 STORAGE SCHEME:

In this module, person can store their documents into three one-of-a-kind garage server. The records owner has no longer control over the facts after it is uploaded on cloud. on this module, the unique statistics get encrypted into three distinctive layers. The statistics in each layer can be encrypted by the use of exclusive cryptographic set of rules and encryption key earlier than storing them inside the Cloud.

4.4 RECOVERY SCHEME:

In this Module, person can get better their files from 3 special garage server this is Cloud server, Fog server and nearby machine. right here we're the usage of Hash-Solomon code set of rules is designed to divide information into exceptional parts. If the one information element lacking ,we lost the data records

V. RESULTS AND DISCUSSION

In this paper, we recommend a three-layer garage framework based totally on fog computing. The proposed framework can each take complete benefit of cloud storage and shield the privacy of information. besides,Hash-Solomon code algorithm is designed to divide statistics into distinct components. Then, we can positioned,a small a part of information in nearby machine and fog server so that you can shield the privacy. moreover, based totally on computational intelligence, this algorithm can compute the distribution proportion saved in cloud, fog, and local machine, respectively. through the theoretical protection analysis and experimental assessment, the feasibility of our scheme has been established, that's honestly a powerful supplement to present cloud storage scheme.

VI. CONCLUSION

The improvement of cloud computing brings us a lot of benefits. Cloud garage is a convenient technology which facilitates customers to extend their garage capacity. but, cloud garage additionally reasons a sequence of comfortable troubles. whilst the use of cloud garage, users do not simply control the physical garage of their data and it results. In order to clear up the trouble of privacy safety in cloud garage, we suggest a TLS framework based on fog computing version and layout a BCH Code set of rules. thru the theoretical protection evaluation, the scheme is proved to be feasible. via allocating the ratio of data blocks stored in exceptional servers reasonably, we can make sure the privacy of information in each server. On some other hand, cracking the encoding matrix is not possible theoretically. except, the usage of hash transformation can shield the fragmentary records.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.UTURE
[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.
[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, “Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments,” in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.
[4] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacy-preserving datastorage service in public cloud,” J. Comput. Res. Develop., vol. 51, no. 7,pp. 1397–1409, 2014.
[5] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, “Efficient data collectionin sensor-cloud system with multiple mobile sinks,” in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.