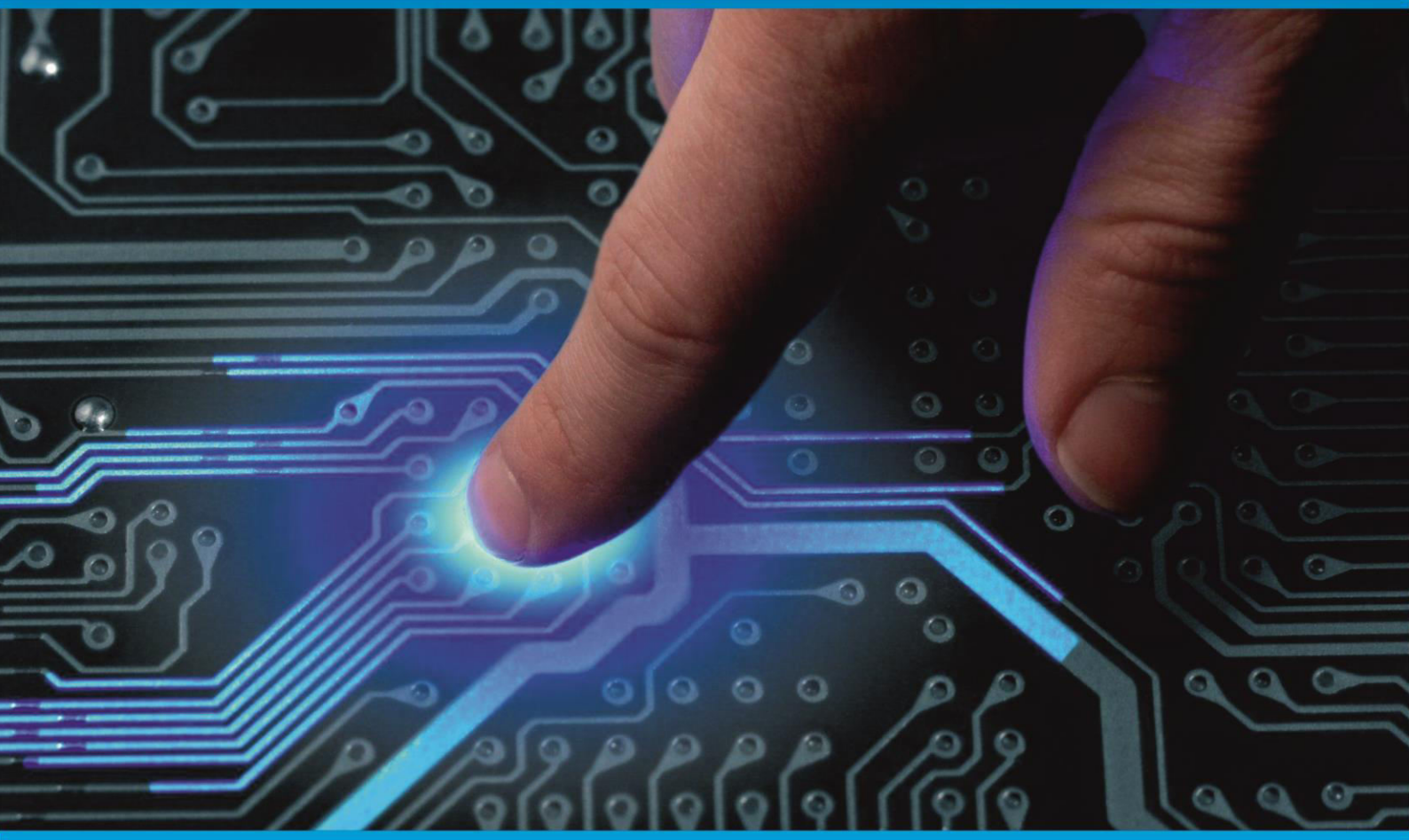
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 2, February 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902017 |

Securing the Cloud a Review of Cloud Computing Security Implications and Best Practices

Yogesh khanna, Dr. Saroj Hirnwal

M.Tech. (Research Scholar ,C.S.), R.I.E.T, Jaipur, India

Principal and Head, R.I.E.T, Jaipur, India

ABSTRACT: Searchable Symmetric encryption has been generally used in a cloud storage. It allows cloud services to straight search over the encrypted data. Most verifiable SSE scheme only enables verifiability for single user model. So, we recommend a GSSE, a generic verifiable SSE framework to ensure search result honestyorbrilliance across multiple users GSSE provides verifiability for any SSE scheme and it provisions data updates. It ensures both the freshness and integrity of search out comesathwartm any users and data owner. GSSE is a generic verifiable SSE scheme that can work with three party models. Data tenants provide services to many businesses and companies, and they insist on improving data security standards by following a covered method, including following: data encryption, key organization, strong admission controls, or security intellect.

I. INTRODUCTION

Cloud computing is a distributed community that provides calculating or storage space as services to end users. The architecture / model of cloud computing is that all servers, networks, presentations or other basics connected to the facts center are accessible to the end users. Cloud computing is upward in attention of technology and business organizations, but this is useful for solving social problems. It can also be beneficial. Cloud computing refers to online operation, configuration or access to applications. It provides online data storage, infrastructure or submissions.

Cloud computing allows individuals and businesses to shift the burden by managing large amounts of data or performance processes that require computing for powerful servers. Due to the growing approval of cloud figuring, more or more data proprietors are being encouraged to subcontract their data to cloud attendants in order to provide great convenience and reduce data management costs. Data tenants provide services to many businesses and companies, and they insist on improving data security standards by following a covered method, including following: data encryption, key organization, strong admission controls, or security intellect.

II. CLOUD COMPUTING

In recent days, Cloud storage has become good entrant for organizations that suffer from resource limitation. Cloud computing is a procedure that surveys internet founded computing. The cloud computing method is used to lessen data organisation cost or time. In addition, cloud computing is used to store data that can be retrieved in remote areas. The most challenging task in the cloud is to ensure availability, integrity, and secure file transfer.

The motivation for cloud computing was needed for complex intensive application run by large scale organization like governments. Those organizations require more computational, network and storage resources then a single computer. Using cloud computing data possessors diffuse data concluded cloud servers to individual users. The use of cloud computing procedure affects the security of the transmission of data.The encryption or decryption procedures to transmit data safely through the cloud servers Data owners encrypt data using encryption algorithms or forward the data to the cloud servers. After encryption, the data is diffused to cloud attendants where data cannot be accessed directly and diffused to the individual users using precise searching technique.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902017 |

Figure 1 : Accesses of statistics among network and Cloud

Figure 1 above defines a scenario where a local area network is related to Cloud system. Some of network data is decomposed from local system or placed in Cloud, but key data is found in local network itself. Cloud provider has no privileges to physically access data in local network. However, cloud wants to admission certain information in local system through the visit. Unauthorized access to local network capitals is possible. It defines a distinctive problem in network security,

Important Security issues in the Cloud

Although virtualization or cloud calculating provide a wide variety of dynamic resources, security risks are usually considered as huge problems in the cloud, causing users to resist themselves when using cloud computing technology. Some cloud security issues are conversed below:

Integrity: Integrity ensures that the data stored in the scheme can correctly represent the expected data and that it can be modified by unauthorized personnel. When an submission is running on the server, backup routine will be arranged to be secure in case of data loss. In general, data is regularly backed up to any portable media and then stored in a remote location

Availability: Being able to verify that data sharing properties are inaccessible due to misconduct. It's just a simple idea, when users try to accept it can be open. It is very important in the mission testing system. The existence of these systems is essential for companies to develop a continuous business plan (BCP) for them to be reorganized. [1].

Confidentiality: Confidentiality confirms that data is not leaked to unlawful persons. Loss of confidentiality occurs when anyone who has unauthorized access to the data can view or read the data. Confidentiality may be lost physically or electronically. The loss of intimacy occurs through social engineering. When the client and server do not encrypt their communications, electronic loss of privacy occurs

III. METHODOLOGY

Advanced Encryption Standard (AES) is a symmetric block digit selected by US Government to defend confidential material or realised in software or hardware worldwide to encrypt complex facts.

AES function

The collection procedure for this new symmetric key algorithm is completely open to public review or reference. This ensures a thorough and translucent study of acquiesced design.

NIST specifies that new innovative encryption typical algorithm should be a block digit that can process 128-bit blocks using 128, 192, and 256-bit keys; other standards selected as next progressive encryption normal algorithm include:

• **Security:** Compared to other submitted passwords, the competitive algorithm must be judged based on the anti-attack capability of the competitive algorithm, although the security strength is measured most significant factor in competition.

• **Costs:** Expected to be unrestricted on a global, non-exclusive or royalty-free basis The candidate algorithm is evaluated in terms of calculation or storage efficiency.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902017 |

• **Implementation:** The algorithm or employment features to be estimated include flexibility of algorithms, the applicability of algorithm in hardware or software; overall, the application is relatively simple.

IV. PROPOSED SYSTEM

The data owner first citations keywords of each articleor builds a keyword directory. He/she encrypts papers as well as keyword index. The data owner subcontracts the scrambled papers as well as encrypted keyword directory to cloud. Data users get every result, proof or public confirmation key, o they or others can even verify freshness, validity and integrity of search results without decryption. The advantages of cloudity parity services provide a secure return on investment, but the disadvantages are far greater. Compared to traditional computer technology, cloud computing offers various advantages. Cloud computing provides its customers with supercomputing capabilities and high-end devices at affordable prices

Advantages

- It support multi-user model.
- Effectual Search Result.
- Prevents data freshness attacks or data veracity attacks.
- It provides High Security.
- Files can be easily updated.
- We have planned a scheme GSSE to confirm freshness, authenticity, and extensiveness of inquiry answers from regularly efficient folders that were presented on untrusted servers

Flow Diagram

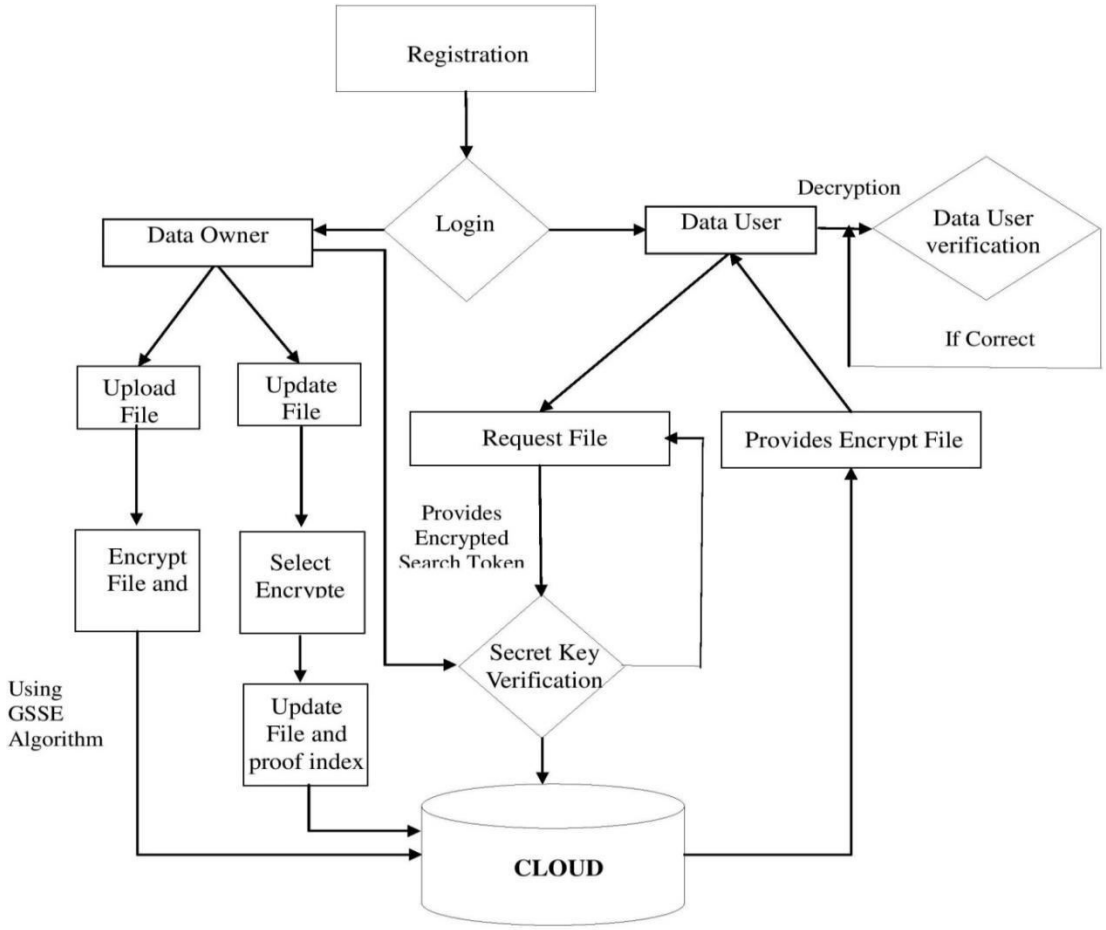


Fig 2 : flow diagram for cloud data secure processing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902017 |

V. CONCLUSION

Even cloud computing offers many benefits to users, but due to safety issues, many users are still reluctant to use it or service providers may also encounter unauthorized access issues. Therefore, we propose a new framework by combining encryption and disguise technologies to address issues related to users and service providers. Before sending data via Cloud encryption, it can provide security for data converted in the network so that the users can ensure the discretion of their data. We suggest a secure storing server that can track user keys and hash values for documents uploaded by the server. For cloud providers, an effective disguise technique is proposed through which the client's secret information (such as passwords, contact information, etc.) is not controlled by a third party.

REFERENCES

1. Vahid Ashktorab and Seyed Reza Taghizadeh, Security Threats and Countermeasures in Cloud Computing, International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 1, Issue 2, October 2018.
2. Cloud Security Alliances, Top Threats to Cloud Computing V1.0‖, Cloud Security Alliances, Version 1, Page No. 3, March 2017.
3. Wiiliam R Claycomb and Alex Nicoll, Insider Threats to New Research Challenges‖, CERT. Wayne A. Janssen, Cloud Hooks: Security and Privacy Issues in Cloud Computing , 44th Hawaii International Conference on System Sciences, January 2015
4. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zahria, A view of Cloud Computing‖, Communications of the ACM, Volume 53, Issue 4, April 2016
5. E. Kirda, C. Kruegel and G. Vigna, Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis‖, Proceeding of the Network and Distributed System. 2014
6. Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Zhuolin Yang and Jianyong Chen,Virtualization Security for Cloud Computing Services‖, International Conference on Cloud and Service Computing, December 2011.
7. Albert B Jeng, Chien Chen Tseng, Der-Feng Tseng and Jiunn-Chin Wang, —A Study of CAPTCHA and its Application to user Authentication‖, Proceeding of 2nd International Conference on Computational Collective Intelligence: Technologies and Applications, 2010
8. A. Liu, Y. Yuan and A Stavrou, ‖SQLProb: A Proxybased Architecture toward Preventing SQL Injection Attacks‖, SAC, March 2009.
9. D. Gollmann, —Securing Web Applications‖, Information Security Technical Report, Volume 13, Issue 1, 2008 153 [11] Mike Ter Louw and Venkatakrishnan V.N. BluePrint: Robust Prevention of Cross-Site Scripting Attacks for Existing Browsers‖, 30th IEEE Symposium on Security and Privacy, May 2009

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details