IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Efficient Access Control for Cloud-Based User Data Storage and Sharing

SK. Pujitha[1], Chintala Harish[2], Ganesh Gangishetty[3], Chimmula Shruthi Reddy[4], Arpan Butti[5]
Assistant Professor, Department of CSE[1]
Students, Department of CSE[2,3,4,5]
Guru Nanak Institute of Technology, Hyderabad, Telangana, India

Abstract: *Cloud computing provides flexible data management and ubiquitous data access. However, the storage service provided by cloud server is not fully trusted by customers. Searchable encryption could simultaneously provide the functions of confidentiality protection and privacy-preserving data retrieval, which is a vital tool for secure storage. In this paper, we propose an efficient large universe regular language searchable encryption scheme for the cloud, which is privacy-preserving and secure against the off-line keyword guessing attack (KGA). A notable highlight of the proposal over other existing schemes is that it supports the regular language encryption and deterministic finite automata (DFA) based data retrieval. The large universe construction ensures the extend ability of the system, in which the symbol set does not need to be predefined. Multiple users are supported in the system, and the user could generate a DFA token using his own private key without interacting with the key generation center. Furthermore, the concrete scheme is efficient and formally proved secure in standard model. Extensive comparison and simulation show that this scheme has function and performance superior than other schemes*

Keywords: Cloud Computing, Searchable Encryption, Privacy-Preserving, Deterministic Finite Automata (DFA), Keyword Guessing Attack (KGA).

I. INTRODUCTION

Cloud storage is an emerging model of storage to provide scalable, elastic and pay-as-you-use service to cloud computing users. For individual usage, the subscribers enjoy the freedom to access to their data anywhere, anytime with any device. When cloud storage is utilized by a group of users, it allows team members to synchronize and manage all shared documents. Moreover, it also saves the user a lot of capital investment of expensive storage equipment's. Cloud delivers convenience to the customers and at the same time arouses many security and privacy problems. Since the data are physically stored on the multiple servers of the cloud service provider, the customers cannot fully in charge of their data. They worry about the privacy of the stored documents since the server may be intruded by hacker or the data could be misused by the internal staff for commercial purpose. The customers prefer to adopt the encryption technology to protect the data confidentiality, which meanwhile arouses another problem: how to execute data retrieval on the large volume of ciphertext. It is almost unimaginable to ask the cloud subscriber to download all of their stored information and then decrypt and search on the recovered plaintext documents. No customer could tolerate the huge transmission overhead and the waiting time for the data retrieval result.

Objective

In this paper, we propose an efficient large universe regular language searchable encryption scheme for the cloud, which is privacy-preserving and secure against the off-line keyword guessing attack (KGA). A notable highlight of the proposal over other existing schemes is that it supports the regular language encryption and deterministic finite automata (DFA) based data retrieval. Proposed a mobile architecture to realize remote-resident multimedia service secure access. The secure framework for business clouds was studied, which realizes that the cloud services are safe and secure and the large volume of data can be securely processed.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

II. LITERATURE SURVEY

R. S. R. K. Shree Krishna, J. S. J. Arora (2023) This study highlights the criticality of data security and access control in cloud computing to mitigate the risks associated with data breaches and unauthorized access. Key strategies discussed include encryption for data protection, robust authentication mechanisms, and access control models like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). Compliance with regulations such as GDPR and HIPAA is emphasized, along with the importance of continuous monitoring and auditing to detect security threats and ensure policy adherence. The research concludes that a comprehensive, multi-layered security approach fosters trust and protects sensitive information in cloud environments.

N. K. K. Shafique, R. M. K. A. Sayyed (2023) This paper explores access control mechanisms in cloud computing, highlighting the unique challenges posed by multitenancy, elasticity, and virtualization. The authors compare various access control schemes, examining their merits and limitations, while emphasizing the need for solutions tailored to the heterogeneous nature of cloud users. The study suggests future directions for enhancing access control solutions, particularly in securing big data storage.

L. P. A. P. M. G. R. Ramos, et al. (2023) The authors review traditional and modern access control mechanisms used to secure data in cloud environments. They emphasize the importance of encrypting stored data alongside providing access control to authorized users. The study also discusses deployment models (private, public, community, and hybrid clouds) and access control methods like identity-based systems, which play a crucial role in ensuring data security in cloud storage systems.

H. M. Ali, A. H. S. Almazroi, F. A. Alzahrani (2022) This survey delves into various access control frameworks, such as RBAC and ABAC, highlighting their role in creating precise governance models. The authors also examine advanced techniques like Access Control Lists (ACLs), data encryption, and automated identity management. Emerging technologies, including machine learning and blockchain, are identified as promising solutions for improving scalability and compliance with regulations like GDPR and HIPAA. The study underscores the importance of robust access control frameworks in maintaining data integrity and user trust in cloud services.

T. Z. K. V. K. Satyanarayana, S. M. N. K. C. Ravi Kumar (2022) This paper introduces a two-factor data security protection mechanism involving a secret key and a unique personal security device. The system ensures that decryption is impossible without both factors. If the security device is lost or stolen, it can be revoked, rendering it ineffective for decryption. The authors demonstrate that their mechanism is both secure and practical, offering a significant improvement in data security for cloud storage systems.

S. Hu, H. Wang, S. J. Lee (2021) The authors present a comprehensive survey on Attribute-Based Access Control (ABAC), which enables fine-grained access control in cloud environments. Unlike traditional role-based models, ABAC uses attribute-based encryption (ABE) to secure data and restrict access effectively. The study highlights the challenges of implementing ABAC in mobile cloud scenarios due to resource limitations. The authors identify the need for further research in this area, emphasizing its potential to advance data security in dynamic cloud environments.

III. EXISTING SYSTEM

Cloud computing provides flexible data management and ubiquitous data access. However, the storage service provided by cloud server is not fully trusted by customers. Searchable encryption could simultaneously provide the functions of confidentiality protection and privacy-preserving data retrieval, which is a vital tool for secure storage.

Disadvantages of Existing System

- The user can only sign documents on that particular computer.
- The security of the private key depends entirely on the security of the computer

Proposed System

We propose an efficient large universe regular language searchable encryption scheme for the cloud, which is privacy-preserving and secure against the off-line keyword guessing attack (KGA). A notable highlight of the proposal over other existing schemes is that it supports the regular language encryption and deterministic finite automata (DFA) based data retrieval.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Advantages of Proposed System:

- An encrypting algorithm scrambles the message and it can only be unscrambled with a key created at the same time.
- Cipher algorithms are either symmetric or asymmetric for encryption security. For example: Symmetric - the exact same key is used to encrypt and decrypt data.

IV. SYSTEM ARCHITECTURE

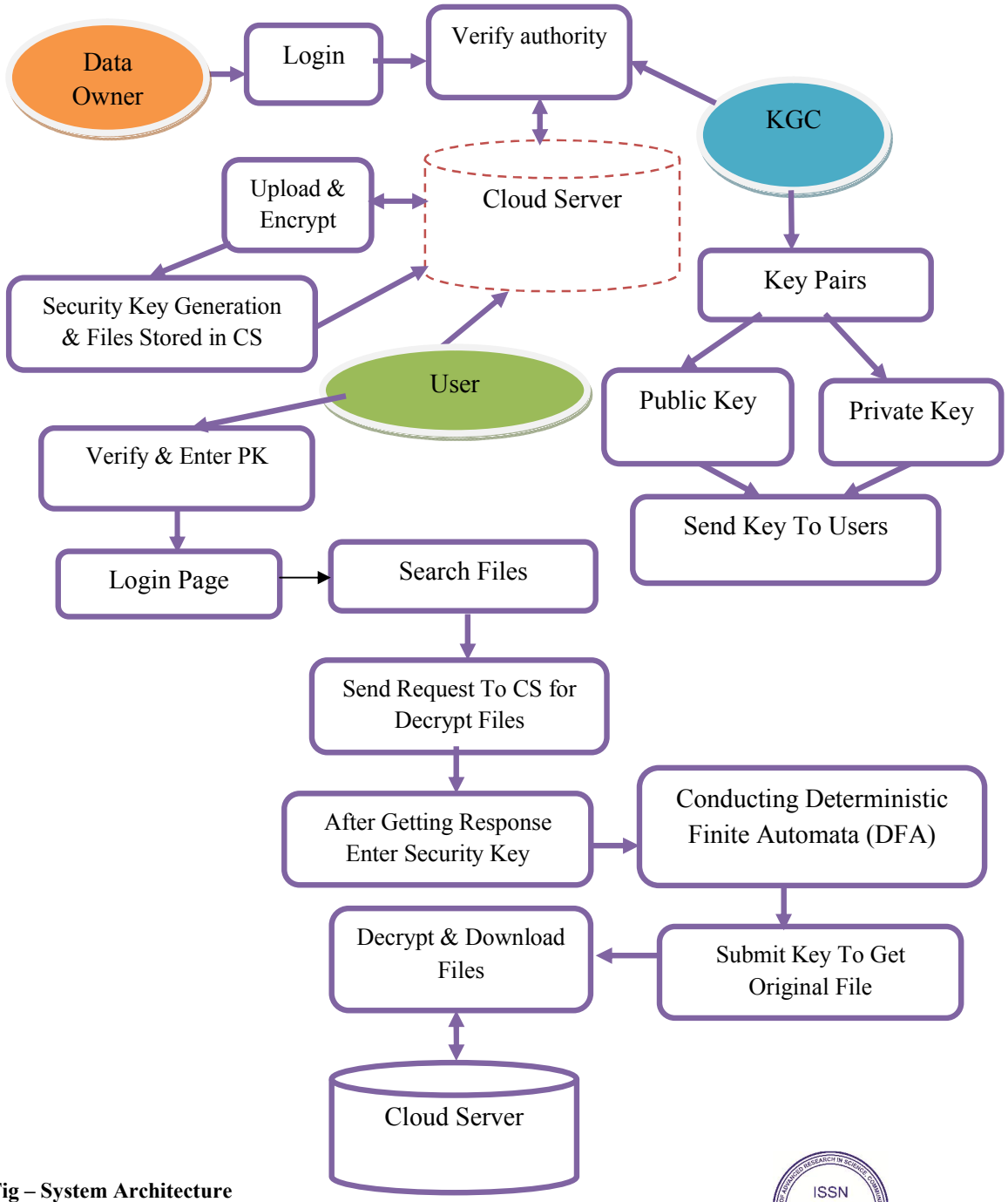


Fig – System Architecture

DOI: 10.48175/IJARSCT-22092

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Explanation:
KGC is the abbreviation of key generation center, who is fully trusted by all the entities in the system. KGC is responsible to generate the public parameter for the whole system. Meanwhile, KGC creates public/private key pair for each legal user in the system. The private key is sent to the user via a secret channel. Users' public keys are made public and maintained by KGC utilizing a secure management mechanism (such as PKI: public key infrastructure. Data Owner utilizes the cloud storage service to store the personal sensitive data. The data owner utilizes regular language to describe the file, and encrypts the regular language and the file, which are then outsourced to the cloud. Cloud Server provides cloud storage service for the users. The digital data are usually stored in logical pools and multiple physical servers. The cloud server is responsible to keep the data ubiquitously available and accessible by authorized users. Cloud server processes amazing data processing and computation ability. Cloud server responds on the search query from the data user and searches the match documents. Data user requests the cloud server to perform the test calculations over the encrypted data. The data user generates a search token utilizing his private key, which is sent to the cloud server to issue a query. The data user may utilize mobile device to generate the search token such that the related algorithms should be efficient and have low transmission overhead.

V. METHODOLOGIES

Modules Name:
This project having the following six modules:

- User Interface Design
- Key Generation Center
- Data Owner
- Cloud Server
- Data User

Module Explanation
User Interface Design
In this module we design the windows for the project. These pages are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

Key Generation Center:
KGC is the abbreviation of key generation center, in which all the entities of the system trust fully. KGC is responsible for generating the public parameter for the entire system. Meanwhile, KGC creates a pair of public / private keys for each legal user in the system. The private key is sent to the user through a secret channel. The public keys of the users are made public and Maintained by KGC using a secure management mechanism.

Data Owner:
Data Owner utilizes the cloud storage service to store the personal sensitive data. The data owner utilizes regular language to describe the file, and encrypts the file, which are then outsourced to the cloud

Cloud Server:
Cloud Server provides cloud storage service for the users. The digital data are usually stored in logical pools and multiple physical servers. The cloud server is responsible to keep the data ubiquitously available and accessible by authorized users. Cloud server processes amazing data processing and computation ability. Cloud server responds on the search query from the data user and searches the match documents.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Data User:

Data user requests the cloud server to perform the test calculations over the encrypted data. The data user generates a search token utilizing his private key, which is sent to the cloud server to issue a query. The data user may utilize mobile device to generate the search token such that the related algorithms should be efficient and have low transmission overhead.

VI. IMPLEMENTATION

General

Algorithm Used

Search Encryption Algorithm.

Searchable encryption technology not only exerts encryption protection of the data, but also supports efficient search function without undermining the data privacy. The data user generates a token of the content that he wants to search using his private key. Receiving the token, the cloud server searches on the encrypted data without decrypting the ciphertext. The most important point is that the server learns nothing about the plaintext of the encrypted data or the searched content during the data retrieval procedure. However, most of the available searchable encryption schemes only support some basic search patterns, such as single keyword search, conjunctive keyword search and Boolean search. Since the cloud computing is a fierce competition industry, it is of vital importance to provide good user experience. It is urgent to design novel searchable encryption schemes with expressive search pattern for cloud storage.

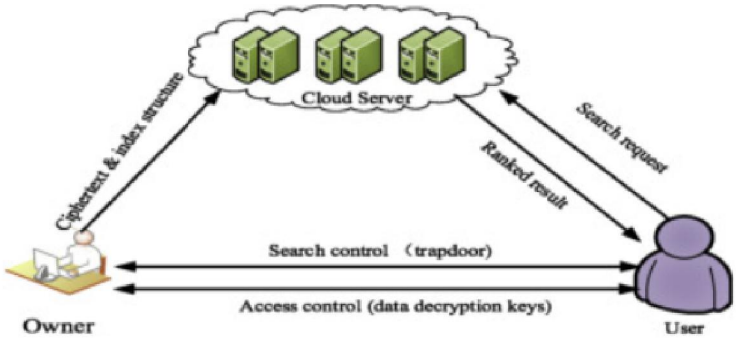
Searchable encryption [6,8–11,15] is a basic tool in PKS to construct the secure index and can be categorized into Symmetric searchable encryption (SSE) and Asymmetric searchable encryption (ASE). Most searchable encryption schemes cannot hide data access and search patterns. In addition, they only support exact match in the context of keyword search. As a result, one of the main contributions in the existing PKS schemes is to construct a secure index that support similar keyword search. Detailed survey of existing searchable encryption schemes is provided in Ref. [16]. In this section, we briefly describe the basic structure of searchable encryption in symmetric and asymmetric settings. We emphasize that all the following structures of symmetric and asymmetric encryption schemes are standard definitions and our goal is to highlight the key ideas behind each one.

The symmetric searchable encryption (SSE) scheme involves three different entities: data owner, data user, and remote server. In this setting, the data owner encrypts his/her own document collection and uploads the encrypted collection to a remote third-party server so that only the legitimate users, holding the secret key, can retrieve the documents based on a given keyword or a set of keywords. Under SSE, only the data owner can contribute searchable contents, and the data owner and the user share the same secret key. Generally, the definition of any SSE scheme.

Searchable encryption schemes follow the security definitions. More specifically, data confidentiality and keyword privacy must be achieved. For efficiency purpose, it is required that nothing should be leaked from the outsourced encrypted document collection and index beyond the search pattern and access patterns of the user queries. The access pattern refers to the outcome of the search result, that is, which documents contain the keyword, whereas the search pattern refers to the possibility of inferring whether two queries were performed for the same keyword and any information derived thereafter from this statement.

Most existing works related to searchable encryption schemes assume the semi-honest adversary model. In the semi-honest model (also referred to as honest-but-curious), the adversary (e.g., cloud) is assumed to follow the prescribed steps of the protocol (i.e., executes all searching operations and returns all search results honestly), but may attempt to learn extra information from the protocol transcript [24,25]. For example, an adversary may try to learn and infer the underlying plaintext information of the encrypted document collection or searchable index.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

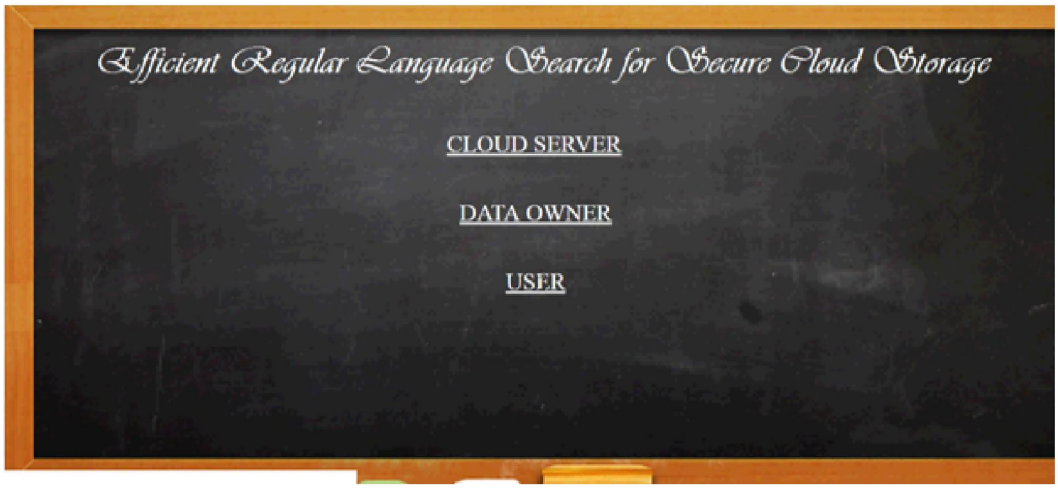


Experimental Results

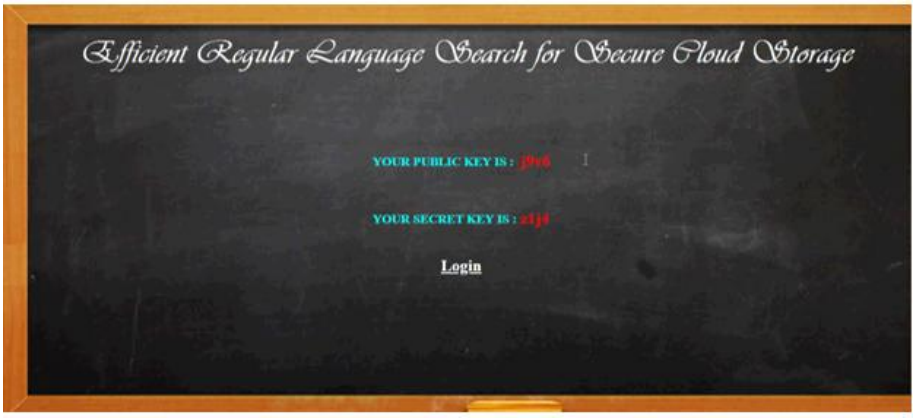
General:

This project is implements like web application using COREJAVA and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.

VII. OUTPUT SCREENS



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024



DOI: 10.48175/IJARSCT-22092

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

VIII. CONCLUSION

In this paper, we introduce a large universe searchable encryption scheme to protect the security of cloud storage system, which realizes regular language encryption and DFA search function. The cloud service provider could test whether the encrypted regular language in the encrypted ciphertext is acceptable by the DFA embedded in the submitted search token. In the test procedure, no plaintext of the regular language or the DFA will be leaked to the cloud server. We also put forth a concrete construction with lightweight encryption and token generation algorithms. An example is given to show how the system works. The proposed scheme is privacy-preserving and indistinguishable against KGA, which are proved in standard model. The comparison and experiment result confirm the low transmission and computation overhead of the scheme.

IX. FUTURE ENHANCEMENT

We do know the encryption was shared key, symmetric stuff; but we don't know exactly how it works which limits the practical applications. However, encryption built on machine learning alone is impressive enough to make us wonder where else encryption might go in the future. Any security model, cryptographic or otherwise, is conceptually an arms race between the adversaries that wish to subvert the technology and those that rely on the technology to secure their information.

REFERENCES

[1]. Erl T, Cope R, Naserpour A. Cloud computing design patterns[M]. Prentice Hall Press, 2015.
[2]. Li Z, Dai Y, Chen G, et al. Toward network-level efficiency for cloud storage services[M]//Content Distribution for Mobile Internet: A Cloud-based Approach. Springer Singapore, 2016: 167-196.
[3]. Sookhak M, Gani A, KhanMK, et al. Dynamic remote data auditing for securing big data storage in cloud computing[J]. Information Sciences, 2017, 380: 101-116.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

[4]. Zhang Q, Yang L T, Chen Z, Li P. Privacy-preserving double projection deep computation model with crowd sourcing on cloud for big data feature learning[J]. IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.

[5]. Zhang Q, Yang L T, Chen Z, Li P. PPHOPCM: Privacy-preserving High-order Possibilistic c-Means Algorithm for Big Data Clustering with Cloud Computing[J]. IEEE Transactions on Big Data, 2017, DOI: 10.1109/TBDATA.2017.2701816.

[6]. Liu J K, Liang K, Susilo W, et al. Two-factor data security protection mechanism for cloud storage system[J]. IEEE Transactions on Computers, 2016, 65(6): 1992-2004.

[7]. Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data[C]//Theory of Cryptography Conference. Springer Berlin Heidelberg, 2007: 535-554.

[8]. Q. Zheng, S. Xu, and G. Ateniese. VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In INFOCOM, pp. 522C530. IEEE, 2014.

[9]. Liang K, Huang X, Guo F, et al. Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(10): 2365-2376.

[10]. Chang V, Ramachandran M. Towards achieving data security with the cloud computing adoption framework [J]. IEEE Transactions on Services Computing, 2016, 9(1): 138-151.

[11]. Zheng X H, Chen N, Chen Z, et al. Mobile cloud based framework for remote-resident multimedia discovery and access[J]. Journal of Internet Technology, 2014, 15(6): 1043-1050.

[12]. Chang V, Kuo Y H, Ramachandran M. Cloud computing adoption framework: A security framework for business clouds [J]. Future Generation Computer Systems, 2016, 57: 24-41.

[13]. Barsoum A. Provable data possession in single cloud server: A survey, classification and comparative study[J]. International Journal of Computer Applications, 2015, 123(9).

[14]. Wang H. Identity-based distributed provable data possession in multicolour storage[J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-340.

[15]. J, Tan X, Chen X, et al. Opor: Enabling proof of irretrievability in cloud computing with resource-constrained devices[J]. IEEE Transactions on cloud computing, 2015, 3(2): 195-205.

[16]. Tiwari D, Gangadharan G R. A novel secure cloud storage architecture combining proof of retrievability and revocation[C]//Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on. IEEE, 2015: 438-445.

[17]. Omote K, Thao T P. MD-POR: multisource and direct repair for network coding-based proof of retrievability[J]. International Journal of Distributed Sensor Networks, 2015, 2015: 3.

[18]. Hopcroft JE, Motwani R, Ullman JD. Automata theory, languages, and computation. International Edition 24 (2006).

[19]. Lucas SM, Reynolds TJ. Learning deterministic finite automata with a smart state labeling evolutionary algorithm. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2005 Jul;27(7):1063-74.

[20]. Kobayashi K, Imura JI. Deterministic finite automata representation for model predictive control of hybrid systems. Journal of Process Control. 2012 Oct 31;22(9):1670-80.

[21]. de Parga MV, Garcła P, Lpez D. A polynomial double reversal minimization algorithm for deterministic finite automata. Theoretical Computer Science. 2013 May 27;487:17-22.

[22]. Sarkar P, Kar C. Adaptive E-learning using Deterministic Finite Automata[J]. International Journal of Computer Applications, 2014, 97(21).

[23]. Fernau H, Heggernes P, Villanger Y. A multi-parameter analysis of hard problems on deterministic finite automata[J]. Journal of Computer and System Sciences, 2015, 81(4): 747-765.