IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

Attribute Based Database Management in Secured Cloud Storage

Mahalakshmi B , Sarumathi S , Yuvasree N, Dr.R.Sugumar

UG student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

UG student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

UG student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

Professor & HOD, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: This system proposed an improve data security protection mechanism for cloud using two components. In this system sender sends an encrypted message to a receiver with the help of cloud system. The sender requires knowing identity of receiver but no need of other information such as certificate or public key. To decrypt the cipher text, receiver needs two parts. The first thing is a unique personal security device or some hardware device connected to the computer system. Second one is private key or secrete key stored in the computer. Without having these two things cipher text never decrypted. The important thing is the security device lost or stolen, then cipher text cannot be decrypted and hardware device is revoked or cancelled to decrypt cipher text. We initiate a multi-parameter analysis of two well-known NP-hard problems on deterministic finite automata (DFAs): the problem of finding a short synchronizing word, and that of finding a DFA on few states consistent with a given sample of the intended language and its complement. For both problems, we study natural parameterizations and classify them with the tools provided by Parameterized Complexity. Somewhat surprisingly, in both cases, rather simple FPT algorithms can be shown to be optimal, mostly assuming the (Strong) Exponential Time Hypothesis.

KEYWORDS: Encrypt, Decrypt, cipher, Serilalization.

I. INTRODUCTION

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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

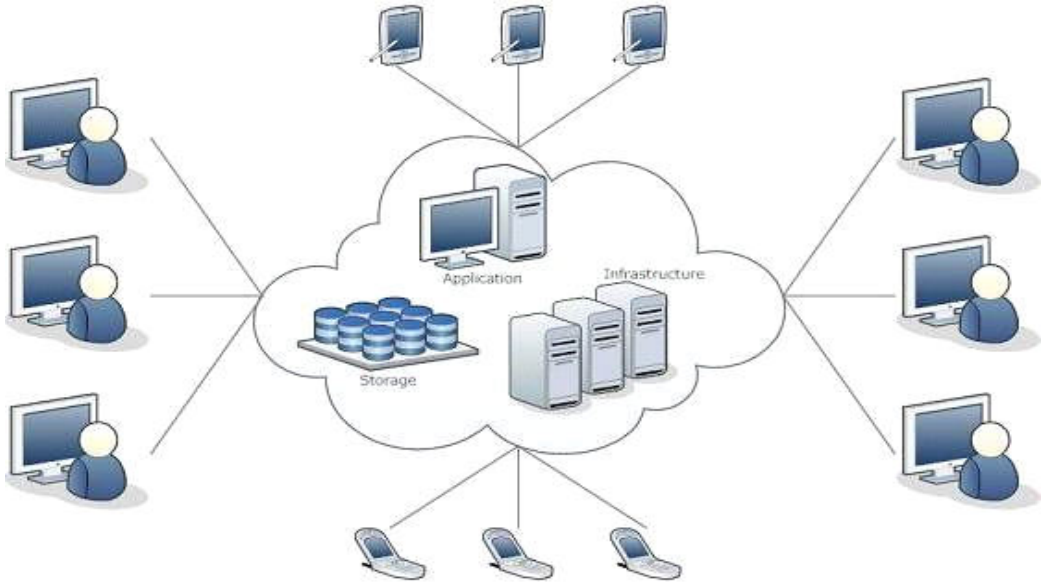

Fig.1.1

II. LITERATURE SURVEY

A.Project Title: Priya J. Khindre, Shital Y. Gaikwad, Two-Factor Data Security Protection Mechanism for Cloud Storage System Year of Publishing: 2017

This system proposed an improve data security protection mechanism for cloud using two components. In this system sender sends an encrypted message to a receiver with the help of cloud system. The sender requires knowing identity of receiver but no need of other information such as certificate or public key. To decrypt the cipher text, receiver needs two parts. The first thing is a unique personal security device or some hardware device connected to the computer system. Second one is private key or secrete key stored in the computer. Without having these two things cipher text never decrypted. The important thing is the security device lost or stolen, then cipher text cannot be decrypted and hardware device is revoked or cancelled to decrypt cipher text.

B.Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack, Peng Xu and Hai Jin

A lot of interest has been drawn recently into public-key encryption with keyword search (PEKS), which keeps publickey encrypted documents amendable to secure keyword search. However, PEKS resist against keyword guessing attack by assuming that the size of the keyword space is beyond the polynomial level. But this assumption is ineffective in practice. PEKS are insecure under keyword guessing attack. As we observe, the key to defend such attack is to avoid the availability of the exact search trapdoor to adversaries. Accordingly, we compromise the exactness of search trapdoor by mapping at least two different keywords into a fuzzy search trapdoor. We propose a novel concept called public-key encryption with fuzzy keyword search (PEFKS), by which the un-trusted server only obtains the fuzzy search trapdoor instead of the exact search trapdoor, and define its semantic security under chosen keyword attack (SS-CKA) and in distinguish ability of keywords under non-adaptively chosen keywords and keyword guessing attack (IK-NCK-KGA). For the keyword space with and without uniform distribution, we respectively present two universal transformations from anonymous identity-based encryption to PEFKS, and prove their SSCKA and IK-NCK-KGA securities. To our knowledge, PEFKS is the first scheme to resist against keyword guessing attack on condition that the keyword space is not more than the polynomial level.

C: A Multi-Parameter Analysis of Hard Problems on Deterministic Finite Automata, Henning Fernaua, Pinar Heggernesb, Yngve Villange,Year of Publishing: 2014

We initiate a multi-parameter analysis of two well-known NP-hard problems on deterministic finite automata (DFAs): the problem of finding a short synchronizing word, and that of finding a DFA on few states consistent with a given sample of the intended language and its complement. For both problems, we study natural parameterizations and

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

classify them with the tools provided by Parameterized Complexity. Somewhat surprisingly, in both cases, rather simple FPT algorithms can be shown to be optimal, mostly assuming the (Strong) Exponential Time Hypothesis.

C: Learning Deterministic Finite Automata with a Smart State Labeling Evolutionary Algorithm,Simon M. Lucas and T. Jeff Reynolds,Year of Publishing: 2005

Learning a Deterministic Finite Automaton (DFA) from a training set of labeled strings is a hard task that has been much studied within the machine learning community. It is equivalent to learning a regular language by example and has applications in language modeling. In this paper, we describe a novel evolutionary method for learning DFA that evolves only the transition matrix and uses a simple deterministic procedure to optimally assign state labels. We compare its performance with the Evidence Driven State Merging (EDSM) algorithm, one of the most powerful known DFA learning algorithms. We present results on random DFA induction problems of varying target size and training set density. We also study the effects of noisy training data on the evolutionary approach and on EDSM. On noise free data, we find that our evolutionary method out performs EDS Mon small sparse data sets. In the case of noisy training data, we find that our evolutionary method consistently outperforms EDSM, as well as other significant methods submitted to two recent competitions.

D:Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage, Baojiang Cui, Zheli Liu and Lingyu Wang, Year of Publishing: 2015

The capability of selectively sharing encrypted data with different users via public cloud storage may greatly ease security concerns over inadvertent data leaks in the cloud. A key challenge to designing such encryption schemes lies in the efficient management of encryption keys. The desired flexibility of sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents. However, this also implies the necessity of securely distributing to users a large number of keys for both encryption and search, and those users will have to securely store the received keys, and submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data. The implied need for secure communication, storage, and complexity clearly renders the approach impractical. In this paper, we address this practical problem, which is largely neglected in the literature, by proposing the novel concept of key aggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient.

III. EXISTING SYSTEM

In existing system the data's which are uploaded by the server side are all Stored in the database with all formats in the regular language so that the security of data's are very less and there is a possibility of information theft and information loss possibility is there, so in future only encrypted data's alone should be stored in cloud.

IV. PROPOSED SYSTEM

In this work, cloud storage of secured data's of various fields and retrieving those data's whenever necessary. All those data's will be in different formats like text, image, video etc and all these will be encrypted and stored in database DFA search technique is used to read the data's in the form of encrypted data and convert the data's into regular language and display those information to authorized user whenever they need. In server side operations they can also manipulate all the data's which they uploaded.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

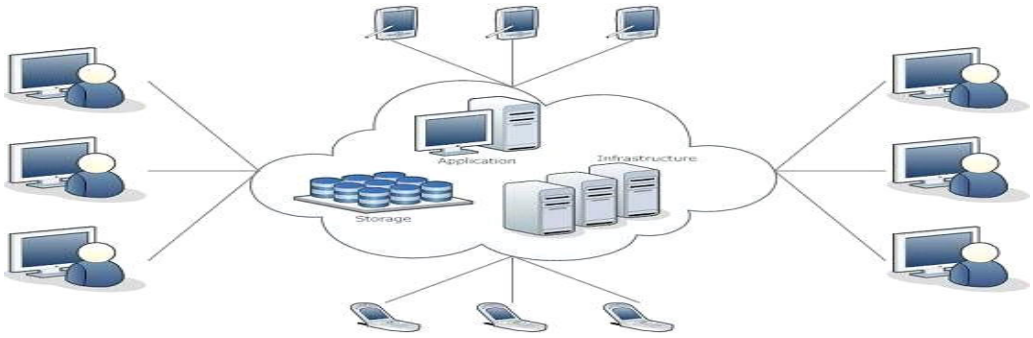

Fig.1.2

Data Owner and User Authentication:
User has to fill the registration form with required mandatory input fields to be filled completely and enroll themselves to access the cloud information and downloading the documents from the data's retrieved from the cloud. Finally a user id and password is generated and can be used as a key to access the information from the cloud.

Server Page File Upload:
In this module Server side will upload the required data's for various fields according to the basic requirements of the user and all these information are gathered and then encrypted and finally stored inside the public cloud. All the formats of data's and file like text, image, video, pdf etc can be stored in the cloud in encrypted form.

Authorized User's Page to access cloud:
Different User's will create their account with specific user name and password and with that information only cloud can retrieve their account and from that account user can access and search various kinds of data by proving the particular name of the data or any related names of that data's for the cloud to read and identify the required user information and the data's and fetched from the cloud database backend and the information is displayed in user's account so that the user can read and download the data's.

Server side data manipulation:
Server has the rights not only to upload the data's in cloud; he also manipulates the data's according to user needs. Some data's are hidden based on age restrictions and server can kill the information which are hazardous to society and user's so always manipulation rights will be there in server side computing and after manipulation or editing the data's all these data's once again encrypted and stored back inside the public cloud.

V. EXPERIMENTAL RESULTS

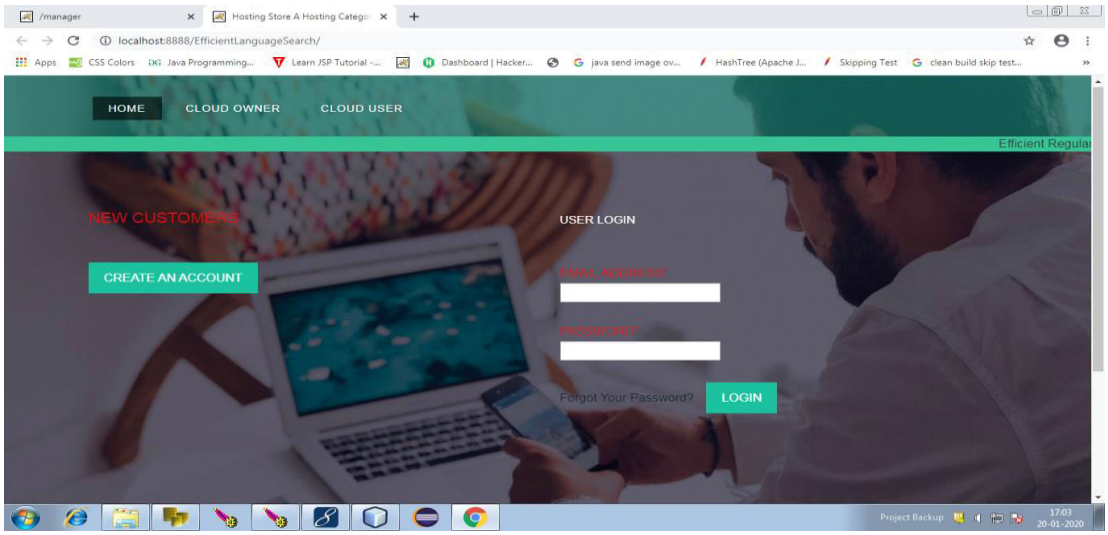

Fig.1.3

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

This is the User Interface Design which includes the registration of owner and the user.

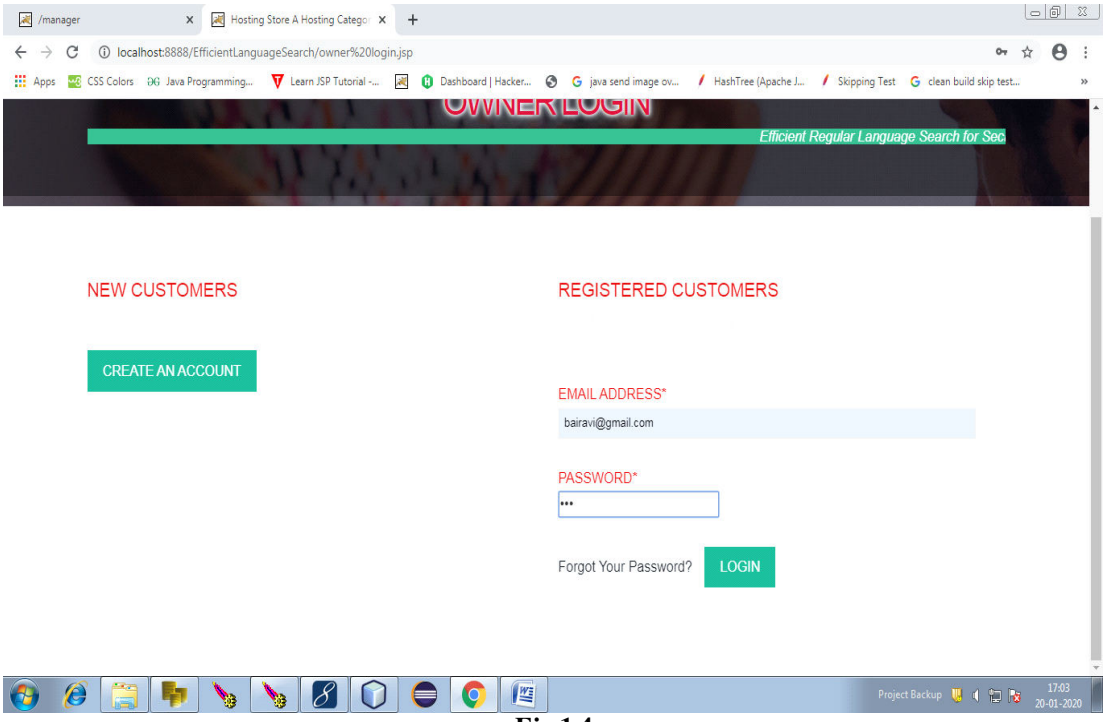

Fig.1.4

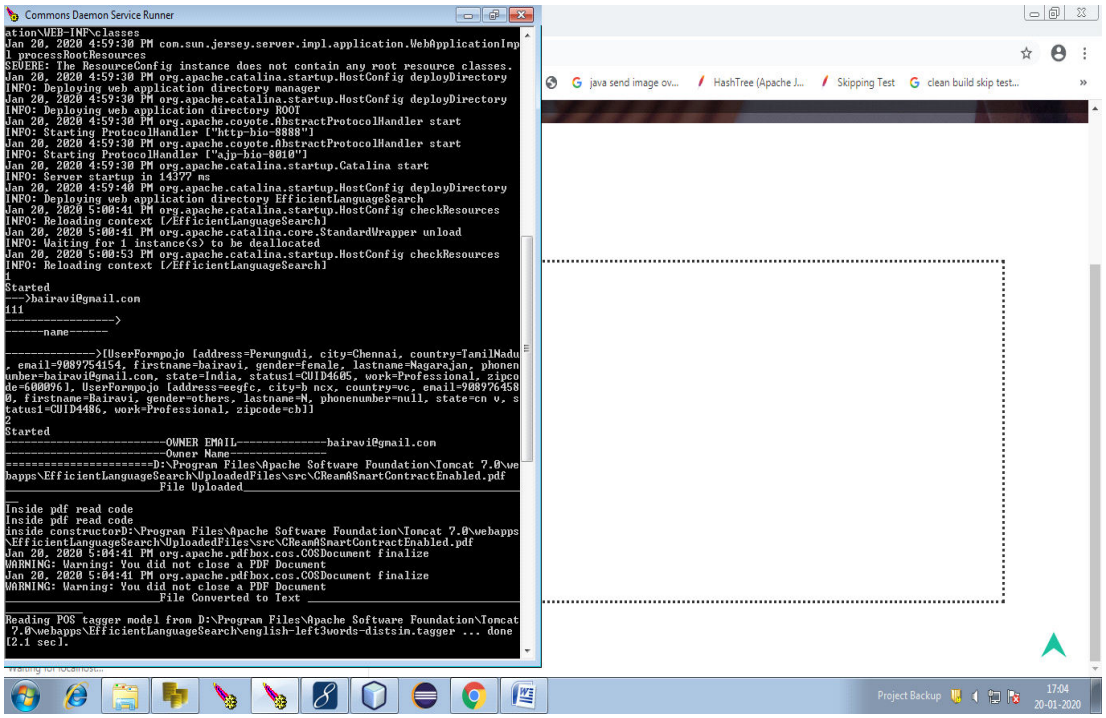

Fig.1.5

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

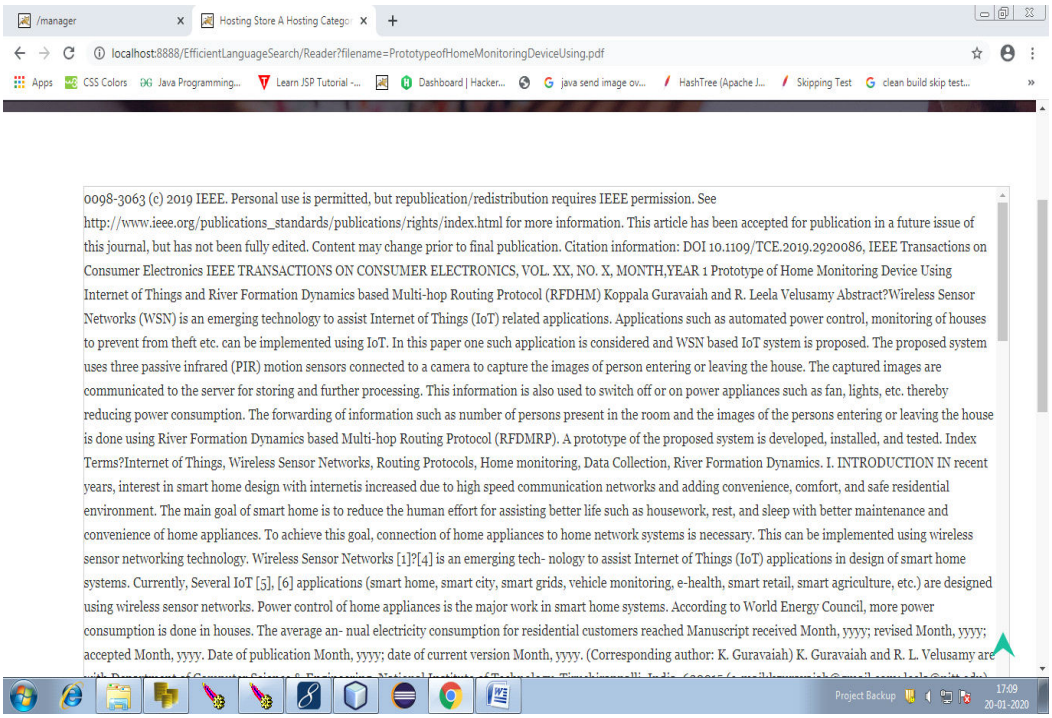

Fig.1.6

VI.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.

VII. FUTURE ENHANCEMENT

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.

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.
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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

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 multicloud storage[J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-340.
15. J, Tan X, Chen X, et al. Opor: Enabling proof of retrievability 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.
24. Farmanbar A, Firouzi S, Park S J, et al. Multidisciplinary insight into clonal expansion of HTLV-1Cinfected cells in adult T-cell leukemia via modeling by deterministic finite automata coupled with high-throughput sequencing[J]. BMC medical genomics, 2017, 10(1): 4.
25. D.X. Song, D.Wagner, A. Perrig, "Practical techniques for searches on encrypted data", in: IEEE Symposium on Security and Privacy, 2000, pp. 44-55.
26. Wang C, Cao N, Ren K, et al. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE Transactions on parallel and distributed systems, 2012, 23(8): 1467-1479.
27. Liu Q, Tan C C, Wu J, et al. Towards differential query services in cost-efficient clouds[J]. IEEE Transactions on parallel and Distributed Systems, 2014, 25(6): 1648-1658.
28. Xu P, Jin H, Wu Q, et al. Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack[J]. IEEE Transactions on computers, 2013, 62(11): 2266-2277.
29. Li H, Yang Y, Luan T H, et al. Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(3): 312-325.
30. Cui B, Liu Z, Wang L. Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage[J]. IEEE TRANSACTIONS ON COMPUTERS, 2014, 6(1): 1.
31. Yang Y, Ma M. Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for EHealth Clouds [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(4):746-759.
32. Yang Y. Attribute-based data retrieval with semantic keyword search for e-health cloud[J]. Journal of Cloud Computing, 2015, 4(1): 1.
33. Liang K, Susilo W. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1981-1992.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003185

34. Chen R, Mu Y, Yang G, et al. Dual-server public-key encryption with keyword search for secure cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(4): 789-798.
35. Yang Y, Ma M. Semantic Searchable Encryption Scheme Based on Lattice in Quantum-Era[J]. Journal of Information Science and Engineering, 2016, 32(2).
36. Xia Q, Ni J, Kanpogninge A J B A, et al. Searchable Public- Key Encryption with Data Sharing in Dynamic Groups for Mobile Cloud Storage[J]. J. UCS, 2015, 21(3): 440-453.
37. Li H, Liu D, Dai Y, et al. Engineering searchable encryption of mobile cloud networks: when qoe meets qop[J]. IEEE Wireless Communications, 2015, 22(4): 74-80.
38. Yang Y, Ma M, Lin B. Proxy re-encryption conjunctive keyword search against keyword guessing attack[C]//Computing, Communications and IT Applications Conference (ComComAp), 2013. IEEE, 2013: 125-130.
39. Wu Y, Lu X, Su J, et al. An Efficient Searchable Encryption Against Keyword Guessing Attacks for Sharable Electronic Medical Records in Cloud-based System[J]. Journal of medical systems, 2016, 40(12): 258.
40. J.W. Byun, H. S. Rhee, H.-A. Park, and D. H. Lee, Offline keyword guessing attacks on recent keyword search schemes over encrypted data, in Proc. 3rd VLDB Workshop Secure Data Manage. (SDM), vol. 4165. Seoul, Korea, Sep. 2006, pp. 75C83.
41. W. C. Yau, R. C. W. Phan, S. H. Heng, and B. M. Goi, Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester, Int. J. Comput. Math., vol. 90, no. 12, pp. 2581C2587, 2013.
42. [42] B. Waters. Functional encryption for regular languages. In CRYPTO, vol. 7417 of LNCS, pp. 218C235. Springer, 2012.
43. Sipser, M.: Introduction to the theory of computation. Thomson Course Technology (2006)
44. Fang, L., Susilo, W., Ge, C. Wang, J. Public key encryption with keyword search secure against keyword guessing attacks without random oracle. Information Sciences 238 (2013): 221-241.
45. Attrapadung N. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2014: 557-577.
46. Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C. X. 509 Internet public key infrastructure online certificate status protocol- OCSP. No. RFC 2560. 1999.
47. Chow S S M, Dodis Y, Rouselakis Y, et al. Practical leakageresilient identity-based encryption from simple assumptions[C]//Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010: 152-161.
48. B. Lynn. The Stanford Pairing Based Crypto Library. [Online]. Available: http://crypto.stanford.edu/pbc, accessed Dec 31, 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details