e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

A SECURE KEYWORD SEARCH AND DATA SHARING MECHANISMFOR CLOUD COMPUTING

Jamuna B*1, Dr. Sreedevi E*2

*1Student, Department Of MCA, Sree Vidyanikethan Institute Of Management, Tirupathi, Andhra Pradesh, India.

*2Assistant Professor, Department Of MCA, Sree Vidyanikethan Institute Of Management, Tirupathi, Andhra Pradesh, India.

DOI : https://www.doi.org/10.56726/IRJMETS30961

ABSTRACT

The emergence of cloud infrastructure has considerably reduced the prices of hardware and package resources in computing infrastructure. to make sure security, the info is sometimes encrypted before it's outsourced to the cloud. not like looking out and sharing the plain information, it's difficult to go looking and share the info once encoding. still, it's a important task for the cloud service supplier because the users expect the cloud to conduct a fast search and come back the result while not losing information confidentiality. to beat these issues, we tend to propose a ciphertext-policy attribute-based mechanism with keyword search and information sharing (CPAB-KSDS) for encrypted cloud information. The projected answer not solely supports attribute-based keyword search however conjointly allows attribute-based information sharing at identical time, that is in distinction to the prevailing solutions that solely support either one among 2 options. in addition, the keyword in our theme may be updated throughout the sharing section while not interacting with the PKG. during this paper, we tend to describe the notion of CPAB-KSDS moreover as its security model. Besides, we tend to propose a concrete theme and prove that it's against chosen ciphertext attack and chosen keyword attack secure within the random oracle model. Finally, the projected construction is incontestible sensible and economical within the performance and property comparison.

I. INTRODUCTION

What is cloud computing?

Cloud computing is that the utilization of computing resources (hardware and software) that unit delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped image as Associate in Nursing abstraction for the advanced infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, code and computation. Cloud computing consists of hardware and code resources created on the market on world wide net as managed third-party services. These services usually provide access to advanced code applications and high-end networks of server computers.

How Cloud Computing Works?

The goal of cloud computing is to use ancient supercomputing, or superior computing power, usually used by military and analysis facilities, to perform tens of trillions of computations per second, in consumer-oriented applications like cash portfolios, to deliver personal data, to produce data storage or to power immense, immersive computer games.

The cloud computing uses networks of huge groups of servers usually running low worth shopper computer technology with specialised connections to unfold data-processing chores across them. This shared IT infrastructure contains immense pools of systems that unit joined on. Often, virtualization techniques unit accustomed maximize the malleability of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing supported the definitions provided by the National Institute of Standards and word (NIST) unit created public below:

- On-demand self-service: a shopper can unilaterally provision computing capabilities, like server time and network storage, professional re nata automatically whereas not requiring human interaction with each service's provider.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

- Broad network access: Capabilities unit on the market over the network and accessed through ancient mechanisms that promote use by heterogeneous skinny or thick shopper platforms (e.g., mobile phones, laptops, and PDAs).
- Resource pooling: The provider's computing resources unit pooled to serve multiple customers using a multi- tenant model, with altogether entirely fully completely different physical and virtual resources dynamically appointed and reassigned in step with shopper demand. there is a fashion of location-independence throughout this the patron usually has no management or data over the precise location of the provided resources but is also able to specify location at succeeding level of abstraction (e.g., country, state, or data center). samples of resources embody storage, processing, memory, network metric, and virtual machines.
- Fast elasticity: Capabilities unit of measurement reaching to be quickly and elastically provisioned, in some cases automatically, to quickly scale out and quickly liberated to quickly scale in. To the patron, the capabilities on the marketplace for provisioning usually appear to be unlimited and can be purchased in any quantity at any time.

II. LITERATURE SURVEY

1) Fuzzy identity-based cryptographyAUTHORS: A. Sahai and B. Waters

We introduce a brand new form of Identity-Based cryptography (IBE) theme that we have a tendency to decision Fuzzy Identity-Based cryptography. In Fuzzy IBE we have a tendency to read Associate in Nursing identity as set of descriptive attributes. A Fuzzy IBE theme permits for a non-public key for Associate in Nursing identity, ω, to decode a ciphertext encrypted with Associate in Nursing identity, ω ′, if and providing the identities ω and ω ′ ar getting ready to one another as measured by the "set overlap" distance metric. A Fuzzy IBE theme will be applied to alter cryptography exploitation biometric inputs as identities; the error-tolerance property of a Fuzzy IBE theme is exactly what permits for the utilization of biometric identities, that inherently can have some noise anytime they're sampled. to boot, we have a tendency to show that Fuzzy-IBE will be used for a sort of application that we have a tendency to term "attribute-based encryption".

In this paper we have a tendency to gift 2 constructions of Fuzzy IBE schemes. Our constructions will be viewed as Associate in Nursing Identity-Based cryptography of a message underneath many attributes that compose a (fuzzy) identity. Our IBE schemes ar each error-tolerant and secure against collusion attacks. to boot, our basic construction doesn't use random oracles. we have a tendency to prove the safety of our schemes underneath the Selective-ID security model.

2) Ciphertext-Policy Attribute-Based cryptographyAUTHORS: J. Bethencourt, A. Sahai, and B. Waters

In many distributed systems a user ought to solely be able to access information if a user posses an explicit set of credentials or attributes. Currently, the sole technique for implementing such policies is to use a sure server to store the info and mediate access management. However, if any server storing the info is compromised, then the confidentiality of the info are going to be compromised. during this paper we have a tendency to gift a system for realizing advanced access management on encrypted information that we have a tendency to decision ciphertext-policy attribute-based cryptography. By exploitation our techniques encrypted information will be unbroken confidential notwithstanding the storage server is untrusted; furthermore, our ways ar secure against collusion attacks. Previous attribute-based cryptography systems used attributes to explain the encrypted information and designed policies into user's keys; whereas in our system attributes ar wont to describe a user's credentials, and a celebration encrypting information determines a policy for World Health Organization will decode. Thus, our ways ar conceptually nearer to ancient access management ways like role-based access management (RBAC). additionally, we offer Associate in Nursing implementation of our system and provides performance measurements.

3) Privacy-preserving personal health record exploitation multi-authority attribute-based cryptography with revocation

AUTHORS: H. Qian, J. Li, Y. Zhang, and J. Han

Personal health record (PHR) service is Associate in Nursing rising model for health info exchange. In PHR systems, patient's health records and knowledge ar maintained by the patient himself through the online. In reality, PHRs ar typically outsourced to be hold on at the third parties like cloud service suppliers. However,

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

there are serious privacy considerations concerning cloud service because it could expose user's sensitive information like PHRs to those cloud service suppliers or unauthorized users. exploitation attribute-based cryptography (ABE) to cipher patient's PHRs in cloud atmosphere, secure and versatile access management will be achieved. Yet, issues like measurability in key management, fine-grained access management, and economical user revocation stay to be addressed . during this paper, we have a tendency to propose a privacy-preserving PHR, that supports fine-grained access management and economical revocation. To be specific, our theme achieves the goals (1) climbable and fine-grained access management for PHRs by exploitation multi-authority ABE theme, and (2) economical on-demand user/attribute revocation and dynamic policy update. In our theme, we have a tendency to contemplate matters that multiple information homeowners exist, and patient's PHRs ar encrypted and hold on in semi-trust servers. The access structure in our theme is communicatory access tree structure, and also the security of our theme will be reduced to the quality decisional additive Diffie–Hellman assumption.

III. METHODOLOGY

Java Technology

Java technology is every a programming language and a platform. The Java programming language The Java programming language may be a application-oriented language which is able to be defined by all of the next buzzwords With most programming languages, you either compile or interpret a program so as that you're going to run it on your laptop. The Java programming language is unusual during this a program is every compiled and understood. With the compiler, first you translate a program into Associate in Nursing intermediate language referred to as Java memory device unit codes —the platform-independent codes understood by the interpreter on the Java platform. The interpreter parses and runs each Java memory device unit code instruction on the laptop. Compilation happens merely once; interpretation happens anytime the program is dead. the next figure illustrates but this works.

SQL

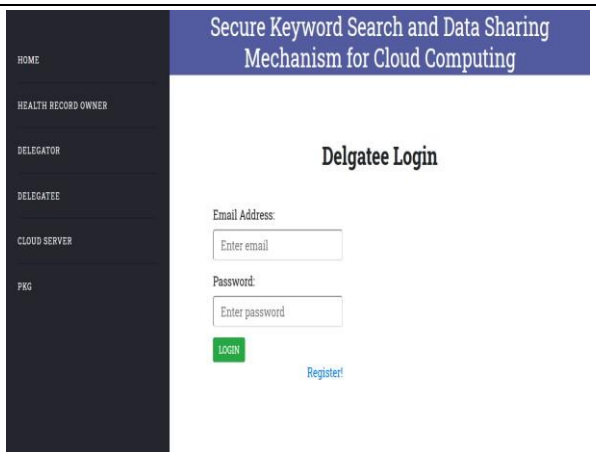
SQL may be a domain-specific language utilized in programming and designed for managing information command in an exceedingly} very on-line database management system (RDBMS), or for stream method in an exceedingly} very relative information stream management system (RDSMS). it's notably useful in handling structured information, i.e. information incorporating relations among entities and variables. SQL offers two main advantages over older read–write genus Apis like ISAM or VSAM. Firstly, it introduced the construct of accessing many records with one single command. Secondly, it eliminates the need to specify how to succeed in a record, e.g. with or whereas not associate index. Originally based upon relative maths and tuple relative calculus, SQL consists of the numerous sorts of statements,[6] which might be informally classed as sublanguages, commonly: a information search language (DQL),[a] a information definition language (DDL),a data management language (DCL), and a information manipulation language (DML).The scope of SQL includes information question, information manipulation (insert, update and delete), information definition (schema creation and modification), and information access management. tho' SQL is truly a declarative language , it to boot includes procedural elements.

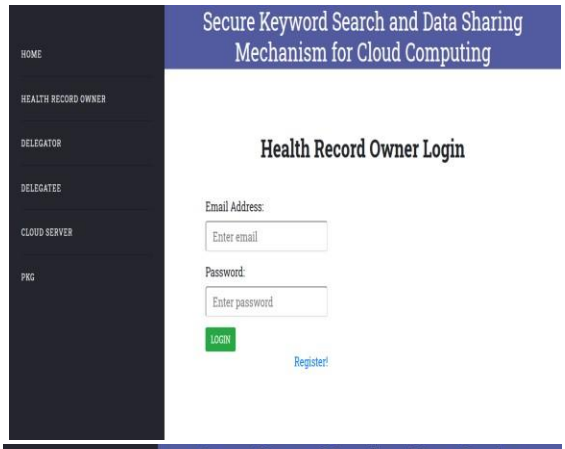
IV. IMPLEMENTATION

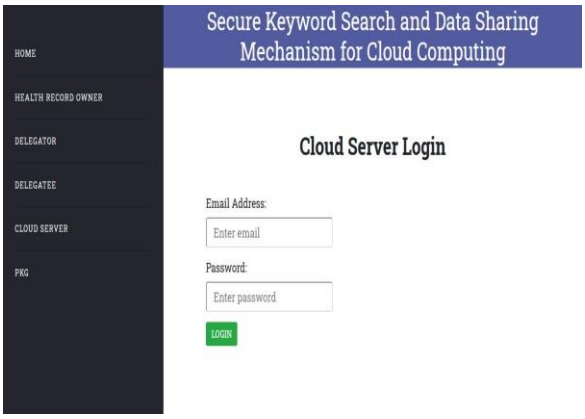
MODULES:

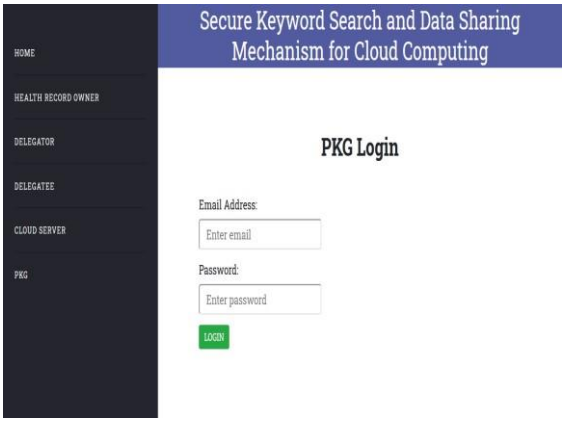
- Health Record owner
- Delegator
- Delegate
- Cloud Server
- PKG

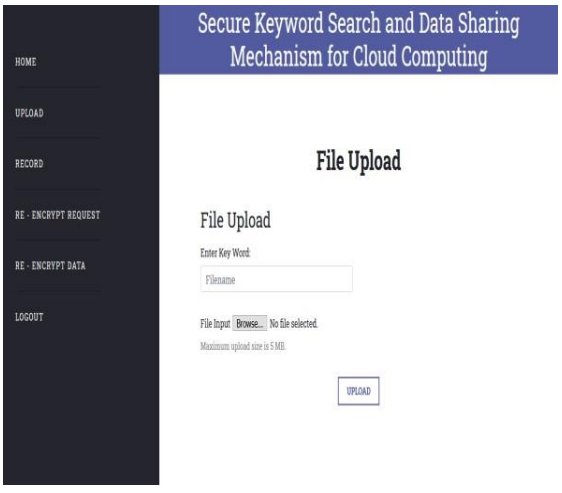
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

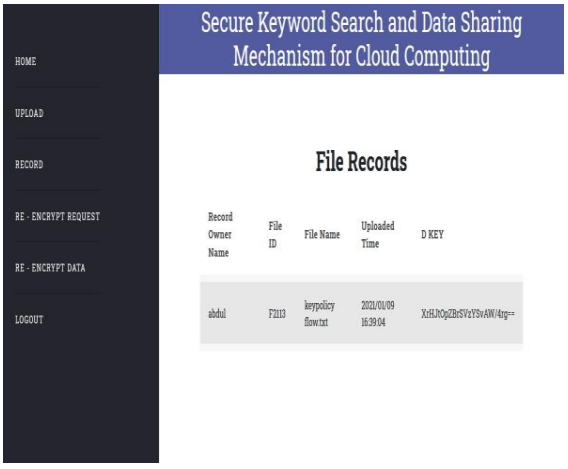


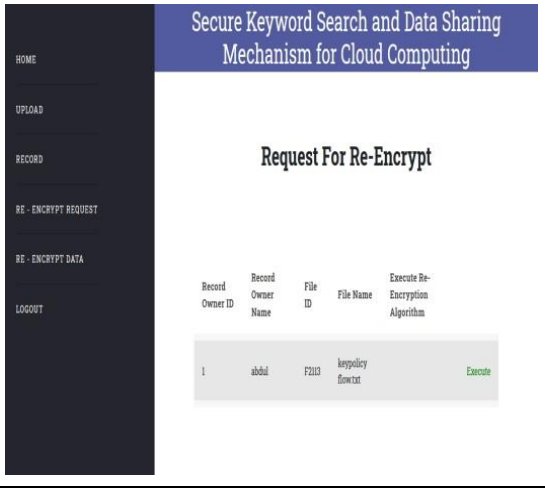












e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:11/November-2022 Impact Factor- 6.752 www.irjmets.com

V. MODULES DESCRIPTION

Health Record Owner:

In Health Record Owner module, Initially record Owner must have to register their detail. After successful registration record owner can login and upload files into cloud server with encrypted keywords and hashing algorithms. He/she can view the files that are uploaded in cloud. Health Record Owner can approve or reject the file request sent by data users. After request approval data owner will send the secret key and verification object through mail.

Delegator:

In Delegator module, Initially Delegator must have to register their detail and after login he/she has to verify their login through secret key. Delegator can search all the files upload by health record owners. He/she can send request to the files and then request will send to the health record owners.

Delegate:

If health record owner approve the request then Delegate will receive secret key, verification object and decryption key in registered mail.

Cloud Server (CS):

In Cloud Server module, Cloud Provider can view all files details. Cloud can view all data analysis.

PKG:

In PKG module, PKG can view all delegator details and PKG can view all delegate Details.

VI. CONCLUSION

In this work, a new notion of ciphertext-policy attribute-based mechanism (CPAB-KSDS) is introduced to support keyword searching and data sharing. A concrete CPAB-KSDS scheme has been constructed in this paper and we prove its CCA security in the random oracle model. The proposed scheme is demonstrated efficient and practical in the performance and property comparison. This paper provides an affirmative answer to the open challenging problem pointed out in the prior work, which is to design an attribute-based encryption with keyword searching and data sharing without the PKG during the sharing phase. Furthermore, our work motivates interesting open problems as well including designing CPAB-KSDS scheme without random oracles or proposing a new scheme to support more expressive keyword search.

VII. REFERENCES

[1] Agarwal, Mohit & Singh, Abhishek &Arjaria, Gautama Siddhartha & Sinha, Amit & Gupta, Suneet. (2020). ToLeD: herb malady Detection pattern Convolutional Neural Network. Procedia subject field. 167. 293-301. 10.1016/j.procs.2020.03.225

[2] P. Tm, A. Pranathi, K. SaiAshritha, N. B. Chittaragi and S. G. Koolagudi, "Tomato disease Detection pattern Convolutional Neural Networks," 2018 Eleventh International Conference on trendy Computing (IC3), 2018, pp. 1-5, doi: 10.1109/IC3.2018.8530532.