ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Energy Efficient and Secured Cloud Data Handling with Multi-User Access Control Strategies

K.Nithya, S. Ilakkiya M. E

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, ARM College of Engineering and Technology, Maraimalai Nagar, Chennai, Tamilnadu, India

Assistant Professor, Department of Computer Science and Engineering, ARM College of Engineering and Technology, Maraimalai Nagar, Chennai, Tamilnadu, India.

ABSTRACT: More and more clients would like to store their data into cloud servers along with the rapid development of cloud computing. The main objective of this system is to introduce duplication free cloud server with powerful encryption and decryption data logics with the avoidance of registration centers along with multiple data owners and data users. New security problems have to be solved in order to help more clients process their data in public cloud. All the cloud having certain space maintenance problems, so that a new mechanism is required in proposed system, which provides duplication free data services over cloud environment. Security is the main constraint in cloud computing environment, which depicts the nature of the third-party registration center avoidance in remote server based data maintenance scheme. In this system we follow the maximum security utility maximization with powerful Message Digest Algorithm (MD5) and Intelligent Data Hashing Algorithm (DHA), which process the data with 256-bit unbreakable encryption mechanism. More enterprises and individuals tend to outsource their personal data to the cloud server, and utilize query services to easily access data anytime, anywhere and on any device. Searchable symmetric encryption (SSE) is often considered as a way to guarantee data privacy and data efficiency. Various data owners encrypt their data with different keys leading to the following two drawbacks: (a)data users need to manage multiple keys for different data owners. (b)data users need to generate multiple trapdoors for data owners' data even for the same query condition. In this system, we focus on multiple data owners top-k query, whereby the cloud server can merge multiple data indexes encrypted with different keys and efficiently support top-k query.

KEYWORDS: Cloud Computing, Multi-keyword Ranked Search, Multiple Data Owners, Security, Cloud Storage.

I. INTRODUCTION

The main objective of this system is to provide the highest safety measure to remote server users with Authenticated Key Exchange Scheme using MD5 logic with other security schemes associated with it. As well as by the appliance of Proxy Reencryption scheme using Identity Based Provable Re-Encryption technique. In 1998, Blaze, Bleumer and Strauss proposed the concept of proxy re-encryption (PRE), where a semi-trusted proxy can transform a ciphertext for Alice into another ciphertext that Bob can decrypt. However, the proxy can learn nothing about the corresponding

DOI: 10.15680/IJIRCCE.2019. 0701036

plaintext. According to the direction of transformation, PRE schemes can be classified into two types, namely, bi-directional or unidirectional.

A PRE scheme is called bidirectional if the proxy can use the Reencryption key to divert ciphertext from Alice to Bob and vice-versa. Otherwise, it is called unidirectional. In unidirectional PRE schemes, the proxy can only transform in one direction. Blaze et al. also gave another method to classify PRE schemes, called multiuse, i.e., the ciphertext can be transformed from Alice to Bob to Charlie and so on; and single-use, i.e., the ciphertext can be transformed only once. Due to its transformation property, PRE schemes can be used in many applications, including simplification of key distribution, key escrow, distributed file systems, multicast, anonymous communication, DFA-based FPRE system, and cloud computation. Recently, the research of cloud email system has become more and more popular in business and organizations as it allows an enterprise to rent the cloud SaaS service to build an email system with less costs and maintenance efforts. Indeed, it is much cheaper and scalable than traditional on premises solution.

However, these solutions have a common drawback: the grant of content sharing capability, which is achieved through the generation of re-encryption key. Up to now, in all of the traditional identity based proxy re-encryption schemes, the generation of re-encryption key is generally divided into two ways: in uni-directional proxy re-encryption scheme, the key is generated by an authorized person A; in bi-directional scheme, it is generated by A and the recipient B. Recently, Wang et al. proposed a new scheme for the re-encryption key generation, where the key is generated by the sender S. This way has the advantage that the sender S can control the authorization granting process by using the random number, which is used in the encryption process to generate the proxy re-encryption key. In this work, we propose a new identity based proxy re-encryption system. In the new identity based proxy encryption system, the re-encryption key is generated by the sender S, and the process of agency is controlled by S thoroughly. This method can avoid the flaw of the traditional proxy Reencryption; the sender S can control the people who can get the message and the sharing content of the messages. Data sharing is another crucial utility function, i.e., sharing data files with each other. In personal health record system, data user (e.g., a patient) should have the ability to access his/her top-k data files about a specific case from different data owners (e.g., health monitors, hospitals, doctors). Similarly, the employees in an enterprise should have the ability to search data files outsourced by other employees.

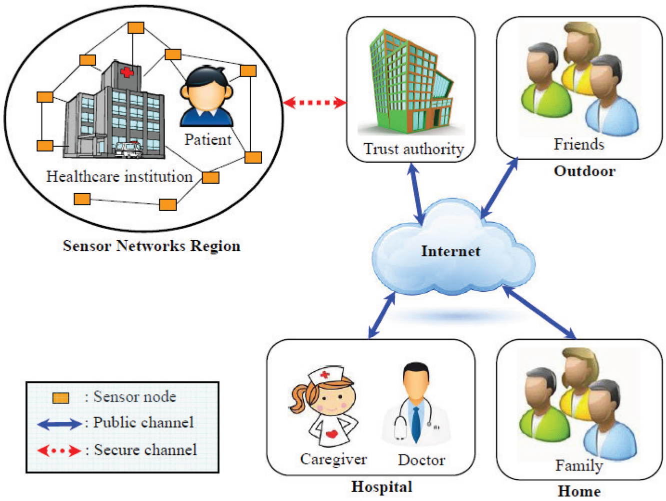


Fig. 1. Cloud Computing Environment Replication

Recent work proposed a privacy-preserving ranked multi-keyword search in a multi-user model (PRMSM), which addresses the multi-keyword search problem in the multiple data owners model. However, PRMSM is inefficient and potentially expensive for frequent queries due to matching various ciphertexts from different data owners even for the same query. Mobile Cloud Computing (MCC) provides cloud resources through on-demand basis by integrating cloud computing into mobile environment. Nowadays, both in industry as well as academia, mobile cloud computing has drawn much attention. A recent analysis done by Heavy Reading estimates that, by the end of 2017, mobile cloud computing market will generate around 68 U.S. billion dollars of direct revenue. Reports from different sources like ABI research predict that, number of worldwide mobile cloud computing users have exploded rapidly, from 42.8 million users on 2008 to 998 million users in 2014. IT organizations are now increasingly using various cloud computing software, infrastructures (like Gmail, Facebook etc.) and frameworks (like Google AppEngine, Amazon web service etc.). Cloud computing are getting popular to IT developers and users day by day. On the other side, worldwide deployment and development of various smartphone applications are also increasing exponentially. Rapid development and implementation of many IT services in mobile cloud computing necessitates extensive research on security issues. An architecture for distributed mobile cloud computing is represented in Fig. 1.

To access a mobile cloud computing service, a mobile user MUi requests the cloud service through an installed mobile App or web browser. After that a mutual authentication between MUi and the cloud service provider CSj is done by the user mobile App or web browser. Both MUi and CSj need to go through a secure mutual authentication process that should support some basic requirements. These include computation efficiency, user anonymity, session key security etc. in order to prevent various threats over insecure channel. Intrinsically, mobile cloud computing services are quite distributed and heterogeneous in nature. Thus, registering separately for each cloud service provider by maintaining respective user account is almost an impossible task. To be precise, MUi requires to access several cloud services from CSj with the help of single registered user account.

A. System Challenges

In contrast to the single-user scenario, developing an efficient scheme for multiple data owners becomes a new challenge. To implement privacy preservation and efficient searches, we commonly build a tree-based index structure for each data owner's encrypted data. For a specific query condition, data users need to generate a trapdoor for each data owner, and the cloud should also search each index. This is obviously inefficient, due to the linear relationship of the number of trapdoors and data owners. A simple way to overcome this limitation is to let each data owner utilize the same key to encrypt their data files. Nevertheless, any one of the owners being compromised may lead to a system crash.

B. Motivation Factors of the Proposed System

The following basic motivating factors are behind the proposal of our scheme in this system:
(a) As user's mobile device generally operates through battery limited equipments, mobile user authentication mechanism should consume minimum possible computation, communication and storage costs. However existing authentication schemes for mobile cloud computing environments, mostly based on resource consuming cryptosystems, such as bilinear pairing and ECC. This necessitates the design of an efficient mobile user authentication scheme that could avoid such cryptosystems without degrading overall security of the system. (b) A careful study on the existing authentication schemes under mobile cloud computing environment reveals most of those schemes have security flaws. Hence, design of more secure authentication scheme is needed in this domain. (c) Further, several schemes, such as the schemes of Shen et al., Yoon and Yoo and He and Wang involve the RC or IdP or SCG in mobile user login process which results in more communication and computation costs.

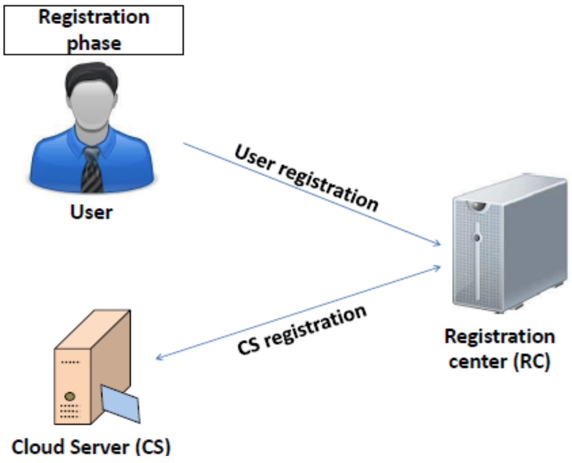


Fig.2 Framework of the Proposed Scheme (Registration Phase)

C. Major Contributions of the Proposed System

The following contributions are made in this system:
(a) The proposed scheme provides mobile user authentication in distributed mobile cloud computing environment, which supports secure key exchange, and user anonymity and intractability properties.
(b) Compared with the related existing authentication schemes proposed in the mobile cloud computing environment, the proposed scheme has the lowest computation and storage requirements. This is primarily due to usage of efficient one way cryptographic hash function, bitwise XOR operation and fuzzy extractor operation only.
(c) No trusted third party, like IdP, SCG or RC, is involved in user login and authentication phases. This reduces overall communication and computation time of the proposed scheme.
(d) The proposed scheme is lightweight in nature, and meanwhile, it also removes the security and functionality drawbacks of the earlier existing schemes.
(e) The proposed scheme has the ability to resist various known attacks, which are evident through the rigorous formal security proof through random oracle model and BAN logic, the formal security verification using the ProVerif 1.93 simulation tool as well as through informal security analysis.

D. Server Prevention Modes

The proposed scheme protects server impersonation attack where an adversary A can masquerade as a cloud server and try to respond with valid message to MUi. When CSj receives the user login message, it replies with an authorization message Msg2 = fC2; H3; TSjg. This message contains the hash value H3 = H(IDi jjM1 jjRNj jjTSi jjTSj jjSKCSj;MUi). Moreover, Msg2 also contains C2 = Bji RNj TSj IDi. A can not obtain Bji = Aij = H(H(IDi rij) jjXj) as it requires the server secret key Xj and random number rij . As a consequence, the proposed scheme also resists server impersonation attack. 12) Privileged-Insider Attack: In this attack, we assume that the registration information IDi; (RPWBik) from the mobile user registration request message is known to a privileged-insider user of the RC, who acts an adversary A. Later, after completing the mobile user registration process, it is also assumed that A also attains the stolen/lost mobile device, and then extract the information stored in the device using the power analysis attack. As discussed in C3, it is computationally difficult task for A to obtain PWi and the biometric key i from V 0 ij and A0 ij in polynomial time. Furthermore, without having the random secret k, A can not compute RPWBi from RPWBik. Therefore, A cannot also obtain PWi and i from RPWBi. Hence, the proposed scheme is free from the privileged-insider attack.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

E. Searchable Encryption

Searchable encryption provides a secure search service over encrypted data. Song D et al. proposed the searchable symmetric encryption(SSE) scheme that achieved ciphertext search. Goh et al. proposed a more secure SSE scheme using Bloom filter. However, a false positive may cause misjudgment. Later, Curtmola et al. proposed other schemes: SSE-1 and SSE-2. In term of efficiency, SSE-1 was better than SSE-2. In term of security, SSE-2 was safer. However, these works mostly focus on the single keyword or boolean search and don't support ranked search. Wang et al. raised a secure ranked keyword search scheme which returned the top-k relevant files and was only designed only for single keyword search. The multi-keyword ranked search allows users to input multiple query keywords for personalized queries. In earlier systems, Cao et al. proposed the first secure multi-keyword ranked search scheme over encrypted cloud data (MRSE), and the documents are ranked by the "inner product" between file vectors and query vectors. However, they do not consider the weight of different keywords.

The work of past approaches enriched the multi-keyword search. Wang et al., Chuah et al. proposed multi-keyword fuzzy search scheme aimed at the tolerance of Zhang et al. proposed a secure ranked multi-keyword search scheme in a multi-owner model (PRMSM) that not only allows the cloud server to perform a multi-keyword search without knowing any sensitive information, but also enable the data owner to flexibly change the encryption key. However, these schemes rarely focus on query efficiency. Practically, query efficiency is one of the most important indicators of the user experience. Kamara et al. proposed a secure search scheme based on the tree-based index, which can efficiently perform searches. However, it is designed only for a single keyword search. Later, Xu et al. presented an efficient multi-keyword ranked search scheme (MKQE) that enabled a dynamic keyword dictionary and improved the precision of the search. Sun et al. created a privacy-preserving multi-keyword text search scheme. They divided the vector index into multiple layers and proposed a tree-based index structure by applying the MD-algorithm that realized more efficient search functionality, yet resulting in a loss of precision. Xia et al. constructed a tree-based index structure and proposed a greedy depth-first search (GDFS) algorithm that achieved higher search efficiency. Unfortunately, these works don't consider multiple data owners scenario. Dong et al. considered a practical scenario where multiple users share data via an untrusted third party. To implement it, the authors proposed a novel multi-user searchable data encryption scheme based on proxy cryptography. Different from the existing searchable encryption schemes, their scheme allowed the users to update the shared data set and each user can be reader and writer simultaneously.

Furthermore, the rigious proof had been represented to prove the security of their scheme. Popa et al. focused on web applications and proposed a new platform Mylar which is a combination of system techniques and novel cryptographic primitives, including data sharing, computing over encrypted data and verifying application code. The results with 6 applications showed that Mylar is a good multi-user web application with data sharing. In earlier system, the authors proposed a secure and effective Near-duplicate detection (NDD) system over encrypted in-network storage which supported multi-user and multi-key searchable encryption. However, those schemes cannot solve the multi-keyword ranked search problem in the multi-user setting. Therefore, their schemes cannot directly be deployed for addressing our problem. In past approach, Yao et al. proposed multi-source encrypted indexes merge (MEIM) mechanism, where the cloud can merge the encrypted indexes from data owners without knowing the index content. They focused on personal health records, and only considered a numerical "attribute value" for each attribute while ignoring queries on data files that must be built on vectors.

II. SYSTEM IMPLEMENTATION

A. USER AUTHORIZATION AND AUTHENTICATION

The User Authorization and Authentication module is one of most popular and important factor to enter into the required portals and applications. This enhanced authentication and authorization norms module allows the user (Data Owner and Data User) to register and authenticate themselves into the system with proper identities such as Name,

DOI: 10.15680/IJIRCCE.2019. 0701036

Mobile Number, E-Mail-Id, address, Username and Password and so on. Once the authorization and authentication processes are done, the users have specific rights to proceed into the application and access all the features present into it. The User Authorization and Authentication module is derived based on three-factor authentication, which enables user to proceed with three levels of authentication features such as Automatic Password Generation, Username and Password authentication and Key Generation process. For all the authentication module is the pathway of all users to proceed into the system and accessing the features.

B. SECURED AND ENCRYPTED DATA MAINTENANCE

The Secured and Encrypted Data handling process allows the data owner to maintain the data into the remote cloud server with proper authentication strategies and security. For this module, the base is derived from Intelligent Data Hashing Algorithm (IDHA), which is used to perform the Encryption and Decryption process efficiently, which converts the plain text into encrypted text and then maintained the data into remote server. So, that no one can break the server as well as break the data presented into it. For all the entire module of Secured and Encrypted Data Maintenance is helpful to data owner to maintain the data securely in remote place without any hesitation.

C. AUTHORIZED PARTY DATA SEARCH

The Authorized Party Data Search module is helpful to data user to search for the stored records into the server. The user has several stages of validations such as authentication with three-factor law and needs to request for the required data which is presented into the server. Once the request is raised, the system generates the random security key for the respective user and allows them to enter the key into the portal. The key verification strategy checks the entered key is valid or not, if the key is proper then allows the user to download the requested data from the server, if the key is not proper then immediately the system blocks the user to proceed further.

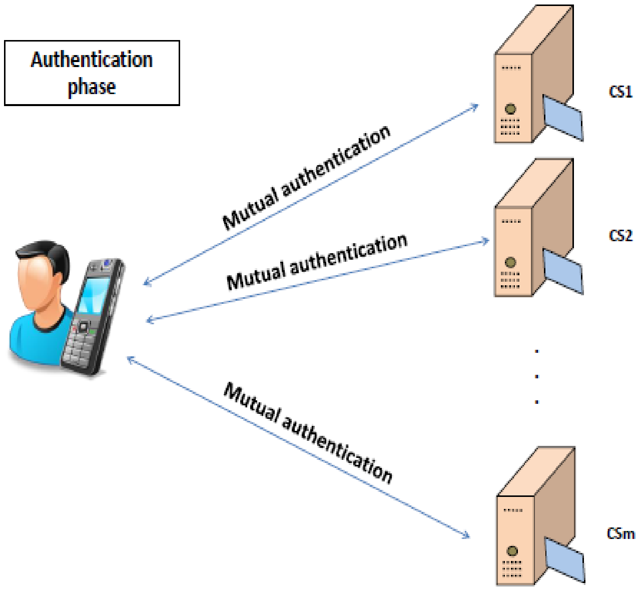


Fig.3. Framework of the Proposed Scheme (Authentication Phase)

D. PAGE RANKING SCENARIO

The Page Rank scenario is a ranking methodology used by Search engines to rank the resulting in their search results. Page Rank is a way of measuring the importance of website pages. According to Google: Page Rank works by counting the number and quality of links to a page to determine a rough estimate of how important the website is. The underlying assumption is that more important websites are likely to receive more links from other websites. It is not the only algorithm used by Google to order search engine results, but it is the first algorithm that was used by the company, and it is the best-known.

E. DOWNLOAD FILE BY MULTIPLE USER OR MULTIPLE FILE BY SINGLE USER

Multiple requests of different clients can be served simultaneously from the different cloud servers. In this module multiple user or client can download the single file from the fog or may be the single user download the multiple file by using conflict free algorithm in this both process download time will reduced simultaneously. Simulation results show that this proposed algorithm exhibits near optimum performance compared to the optimum solution, and a significant reduction in download time as compared to the per-server network coding scheme.

III. LITERATURE SURVEY

Cloud based augmentation for mobile devices: motivation, taxonomies, and open challenges - S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya - 2014. [1] Recently, Cloud-based Mobile Augmentation (CMA) approaches have gained remarkable ground from academia and industry. CMA is the state-of-the-art mobile augmentation model that employs resource-rich clouds to increase, enhance, and optimize computing capabilities of mobile devices aiming at execution of resource-intensive mobile applications. Augmented mobile devices envision to perform extensive computations and to store big data beyond their intrinsic capabilities with least footprint and vulnerability. Researchers utilize varied cloud-based computing resources (e.g., distant clouds and nearby mobile nodes) to meet various computing requirements of mobile users. However, employing cloud-based computing resources is not a straightforward panacea. Comprehending critical factors (e.g., current state of mobile client and remote resources) that impact on augmentation process and optimum selection of cloud-based resource types are some challenges that hinder CMA adaptability.

This paper comprehensively surveys the mobile augmentation domain and presents taxonomy of CMA approaches. The objectives of this study is to highlight the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. We present augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based. We critically analyze the state-of-the-art CMA approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present a taxonomy. Vital decision making and performance limitation factors that influence on the adoption of CMA approaches are introduced and an exemplary decision making flowchart for future CMA approaches are presented. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions.

Mobile Cloud Computing: A Survey, State of Art and Future Directions - M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, and N. Venkatasubramanian - 2014. [2] In the recent years, cloud computing frameworks such as Amazon Web Services, Google AppEngine and Windows Azure have become increasingly popular among IT organizations and developers. Simultaneously, we have seen a phenomenal increase in the usage and deployment of smartphone platforms and applications worldwide. This paper discusses the current state of the art in the merger of these two popular technologies that we refer to as Mobile Cloud Computing (MCC). We illustrate the applicability of MCC in various domains including mobile learning, commerce, health/wellness and social medias. We further identify research gaps covering critical aspects of how MCC can be realized and effectively utilized at scale. These include improved resource allocation in the MCC environment through efficient task distribution and offloading, security and privacy.

Security and privacy for storage and computation in cloud computing - L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos - 2014. [3] Cloud computing emerges as a new computing paradigm that aims to provide reliable, customized and quality of service guaranteed computation environments for cloud users. Applications and databases are moved to the large centralized data centers, called cloud. Due to resource virtualization, global replication and migration, the physical absence of data and machine in the cloud, the stored data in the cloud and the computation results may not be well managed and fully trusted by the cloud users. Most of the previous work on the cloud security focuses on the storage security rather than taking the computation security into consideration together. In this paper, we propose a privacy cheating discouragement and secure computation auditing protocol, or SecCloud, which is a first protocol bridging secure storage and secure computation auditing in cloud and achieving privacy cheating discouragement by designated verifier signature, batch verification and probabilistic sampling techniques. The detailed analysis is given to obtain an optimal sampling size to minimize the cost. Another major contribution of this paper is that we build a practical secure-aware cloud computing experimental environment, or SecHDFS, as a test bed to implement SecCloud. Further experimental results have demonstrated the effectiveness and efficiency of the proposed SecCloud.

Security in cloud computing: Opportunities and challenges - M. Ali, S. U. Khan, and A. V. Vasilakos - 2015. [4]
The cloud computing exhibits, remarkable potential to provide cost effective, easy to manage, elastic, and powerful resources on the fly, over the Internet. The cloud computing, upsurges the capabilities of the hardware resources by optimal and shared utilization. The above mentioned features encourage the organizations and individual users to shift their applications and services to the cloud. Even the critical infrastructure, for example, power generation and distribution plants are being migrated to the cloud computing paradigm.
However, the services provided by third-party cloud service providers entail additional security threats. The migration of user’s assets (data, applications, etc.) outside the administrative control in a shared environment where numerous users are collocated escalates the security concerns. This survey details the security issues that arise due to the very nature of cloud computing. Moreover, the survey presents the recent solutions presented in the literature to counter the security issues. Furthermore, a brief view of security vulnerabilities in the mobile cloud computing are also highlighted. In the end, the discussion on the open issues and future research directions is also presented.

4S: A secure and privacy-preserving key management scheme for cloudassisted wireless body area network in m-healthcare social networks - J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos - 2015. [5] Cloud-assisted wireless body area networks (WBANs) significantly facilitate efficient patient treatment of high quality, unfortunately in the meanwhile greatly challenge the patient’s data confidentiality and privacy. The existing work mainly focused on the traditional scenario where patients securely stay indoors. In this paper, we consider a more practical situation of cloud-assisted WBANs in m-healthcare social networks where patients traverse among blocks outdoors and WBANs are more vulnerable to sophisticated attacks including even node compromise attack.

To solve the problem, a secure and privacy-preserving key management scheme resilient to both time-based and location-based mobile attacks is proposed by the cooperation of the mobile patients in the same social group for both hierarchical and distributed environment. It also protects patient’s identity privacy, sensor deployment privacy and location privacy by exploiting the blinding technique and embedding human body’s symmetric structure into Blom’s symmetric key mechanism with modified proactive secret sharing. Especially, the computationally-intensive privacy-preserving key material updating is outsourced to the cloud server and the unchanged pair wise keys after key material updating dramatically saves the resources for energy-constrained WBANs. Finally, the security analysis and simulation results show our scheme far outperforms the previous ones in terms of resisting mobile attacks and storage, computation and communication overhead.

IV. SYSTEM ANALYSIS

A. Existing System

Data Storage service is one of the most widely consumed cloud services. Cloud users have greatly benefited from cloud storage since they can store huge volume of data without upgrading their devices and access them at any time and in any place. However, cloud data storage offered by Cloud Service Providers [CSPs] still incurs some problems. First of all, various data stored at the cloud may request different ways of protection due to different data sensitivity. The data stored at the cloud include sensitive personal information, publicly shared data, data shared within a group, and so on. As outsourced data could disclose personal or even sensitive information of users, so, they have no idea to provide sensitive information over cloud environment.

DISADVANTAGES OF EXISTING SYSTEM

(a) Encrypted Data could incur much waste of cloud storage and complicate data sharing among authorized users.
(b) We are still facing challenges on encrypted data storage and management with Deduplication.

B. Proposed System

In the proposed system of development the following things are concentrated more and they are describes as below: To save cloud storage across multiple third parties, we need to manage and preserve data security with privacy. As well as encrypted data storage with deduplication schemes are necessary in various situations. A Secure Lightweight Remote User Authentication Scheme is designed to support both deduplication and access control according to the demands of data owners, which can adapt to different application scenarios. This approach can support data sharing among eligible users in a flexible way, which can be controlled by either the data owners or other trusted parties or both of them. The performance of the proposed scheme is justified with security analysis and its implementation is based on powerful DHA security norms. To enable an efficient ranked multi-keyword search for multiple data owners over encrypted cloud data, our scheme aims to achieve the following goals:

(a) Multi-keyword Ranked Search for Multiple Data Owners: This scheme not only allows multi-keyword searches over encrypted cloud data (which are encrypted with different keys for different data owners) but also allow the cloud server to return the ranked top-k encrypted files.

(b) Search Efficiency: We explore a tree-based index structure and an efficient search algorithm. The cloud server will merge encrypted indexes without knowing the corresponding sensitive information. The authenticated data user only needs to encrypt query keywords once to efficiently retrieve all files of interest.

(c) Security: The scheme proposed should achieve the following three security goals: (i) Keyword Semantic Security. We will prove that TBMSM is semantically secure against the chosen keyword attack under the selective security model. (ii) Keyword Security. We will prove that TBMSM realized keyword privacy in the random oracle model. (iii) Relevance Score Security. We need to ensure that the cloud server cannot infer

ADVANTAGES OF PROPOSED SYSTEM

(a) Flexible Cloud Data Deduplication with proper Access Control facilities
(b) The proposed scheme is more secured, advanced and efficient.
(c) Intelligent Data Hashing Algorithm (IDHA) is introduced to provide efficient and secured data storage over cloud environment.

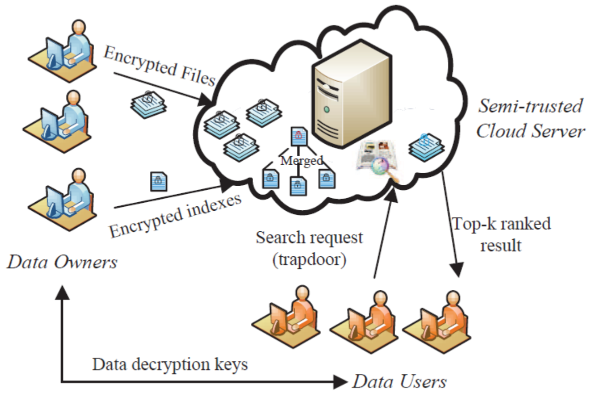
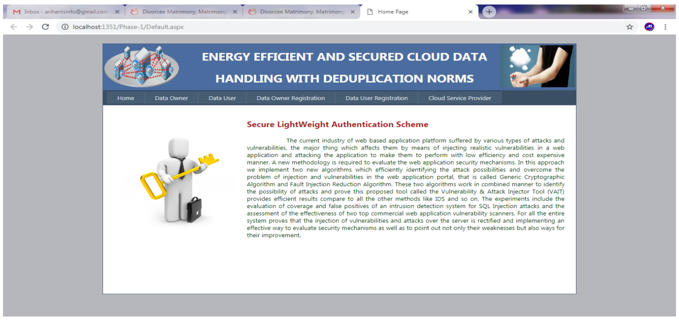


Fig.4 System Architecture Design

V. RESULTS AND DISCUSSION

In this section, we provided the simulated results of entire project with its practical proofs. The following figure shows the Homepage perspective of the Proposed System.

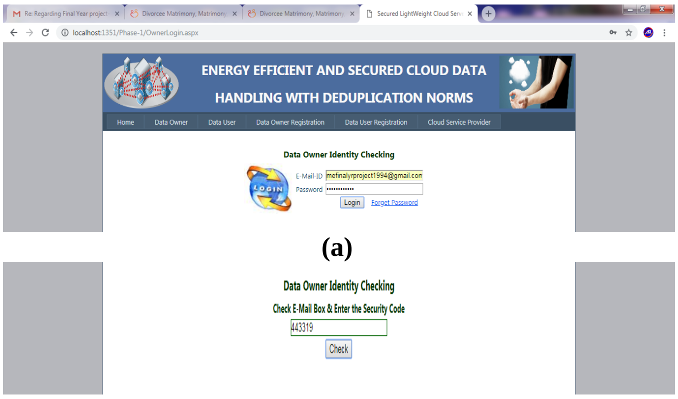

Inbox - arihantsinfo@gmail.com
Divorcee Matrimony, Matrimony
Divorcee Matrimony, Matrimony
Home Page
localhost:1351/Phase-1/Default.aspx
ENERGY EFFICIENT AND SECURED CLOUD DATA HANDLING WITH DEDUPLICATION NORMS
Home
Data Owner
Data User
Data Owner Registration
Data User Registration
Cloud Service Provider

Secure LightWeight Authentication Scheme

The current industry of web based application platform suffered by various types of attacks and vulnerabilities, the major thing which affects them by means of injecting realistic vulnerabilities in a web application and attacking the application to make them to perform with low efficiency and cost expensive manner. A new methodology is required to evaluate the web application security mechanisms. In this approach we implement two new algorithms which efficiently identifying the attack possibilities and overcome the problem of injection and vulnerabilities in the web application portal, that is called Generic Cryptographic Algorithm and Fault Injection Reduction Algorithm. These two algorithms work in combined manner to identify the possibility of attacks and prove this proposed tool called the Vulnerability & Attack Injector Tool (VAIT) provides efficient results compare to all the other methods like IDS and so on. The experiments include the evaluation of coverage and false positives of an intrusion detection system for SQL Injection attacks and the assessment of the effectiveness of two top commercial web application vulnerability scanners. For all the entire system proves that the injection of vulnerabilities and attacks over the server is rectified and implementing an effective way to evaluate security mechanisms as well as to point out not only their weaknesses but also ways for their improvement.

Fig.5 Home Page

The following figure illustrates the Data Owner's Login Page of the proposed system.


Re: Regarding Final Year project
Divorcee Matrimony, Matrimony
Divorcee Matrimony, Matrimony
Secured LightWeight Cloud Serv
localhost:1351/Phase-1/OwnerLogin.aspx
ENERGY EFFICIENT AND SECURED CLOUD DATA HANDLING WITH DEDUPLICATION NORMS
Home
Data Owner
Data User
Data Owner Registration
Data User Registration
Cloud Service Provider
LOGIN
Login
Forget Password
Check

Data Owner Identity Checking

E-Mail-ID: mefinalyrproject1994@gmail.com
Password: ••••••••••••

(a)

Data Owner Identity Checking

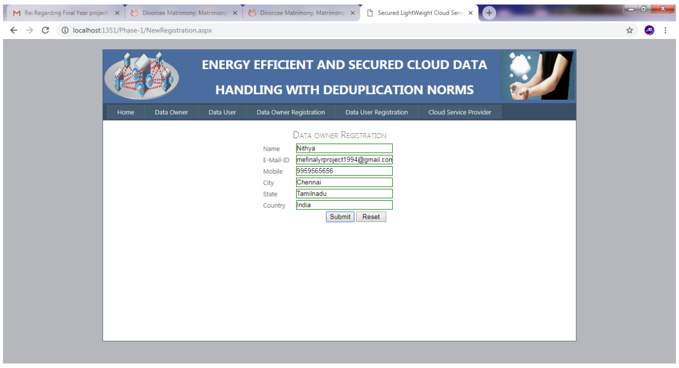
Check E-Mail Box & Enter the Security Code

443319

(b)

Fig.6 (a) User Login Page (b) Security Code Verification

The following figure illustrates the Data Owner Registration Page of the proposed system.

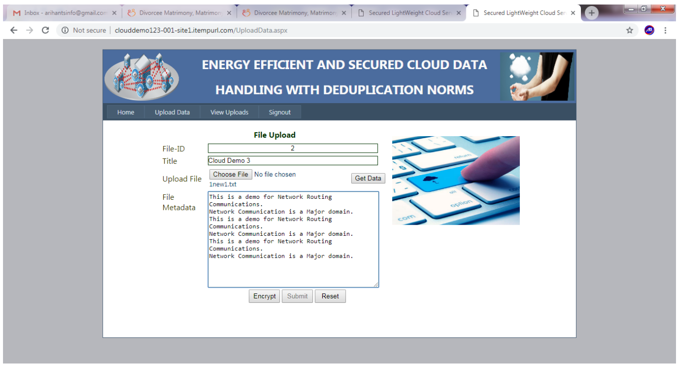

Re: Regarding Final Year project
Divorcee Matrimony, Matrimony
Divorcee Matrimony, Matrimony
Secured LightWeight Cloud Serv
localhost:1351/Phase-1/NewRegistration.aspx
ENERGY EFFICIENT AND SECURED CLOUD DATA
HANDLING WITH DEDUPLICATION NORMS
Home
Data Owner
Data User
Data Owner Registration
Data User Registration
Cloud Service Provider

DATA OWNER REGISTRATION

Name: Nithya
E-Mail-ID: mefinalyrproject1994@gmail.con
Mobile: 9959565656
City: Chennai
State: Tamilnadu
Country: India

Fig.7 Registration Page

The following figure illustrates the File Uploading View of the proposed system.


Inbox - arihantsinfo@gmail.com
Divorcee Matrimony, Matrimon
Divorcee Matrimony, Matrimon
Secured LightWeight Cloud Ser
Secured LightWeight Cloud Ser
Not secure
clouddemo123-001-site1.itempurl.com/UploadData.aspx
ENERGY EFFICIENT AND SECURED CLOUD DATA
HANDLING WITH DEDUPLICATION NORMS
Home
Upload Data
View Uploads
Signout

File Upload

File-ID: 2
Title: Cloud Demo 3
Upload File: Choose File No file chosen 1new1.txt
File Metadata:

```
This is a demo for Network Routing
Communications.
Network Communication is a Major domain.
This is a demo for Network Routing
Communications.
Network Communication is a Major domain.
This is a demo for Network Routing
Communications.
Network Communication is a Major domain.
```

Fig.8 File Uploading

VI. CONCLUSION AND FUTURE SCOPE

We consider a multiple data owners model in cloud computing and propose an efficient ranked multi keyword search scheme over encrypted data. In this system, we proposed a heterogeneous data storage management scheme, which offers flexible cloud data Deduplication and access control. Our scheme can adapt to various application scenarios and demands and offer economic big data storage management across multiple CSPs. It can achieve data de-duplication and access control with different security requirements.

In future, the proposed work is further extended by means of some intensive algorithms such as Machine Learning in association with AI algorithms to make powerful authentication strategies and has a plan to improve the security as well as its accuracy higher than the proposed system.

REFERENCES

[1] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya., "Cloudbased augmentation for mobile devices: motivation, taxonomies, and open challenges," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 337–368, 2014.
[2] M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, and N. Venkatasubramanian, "Mobile Cloud Computing: A Survey, State of Art and Future Directions," Mobile Network Application, vol. 19, pp. 133–143, 2014.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

[3] “Heavy Reading Real World Research (2013),” The mobile cloud market outlook to 2017. Accessed on July 2017.
[4] “ABI Research Report, Mobile Cloud Applications,” http: //www.abiresearch.com/research/1003385-Mobile+Cloud+Computing. Accessed on July 2017.
[5] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, “Security and privacy for storage and computation in cloud computing,” Information Sciences, vol. 258, pp. 371–386, 2014.
[6] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Information Sciences, vol. 305, pp. 357–383, 2015.
[7] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, “4S: A secure and privacy-preserving key management scheme for cloudassisted wireless body area network in m-healthcare social networks,” Information Sciences, vol. 314, pp. 255–276, 2015.
[8] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, “Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1299–1314, 2015.
[9] Z. Yan, X. Li, M. Wang, and A. Vasilakos, “Flexible Data Access Control based on Trust and Reputation in Cloud Computing,” IEEE Transactions on Cloud Computing, 2017, DOI: 10.1109/TCC.2015.2469662.
[10] J. L. Tsai and N. Lo, “A privacy-aware authentication scheme for distributed mobile cloud computing services,” IEEE Systems Journal, vol. 9, no. 3, pp. 805–815, 2015.
[11] P. Mell, T. Grance, “The nist definition of cloud computing,” COMMUN ACM., vol. 53, no. 6, pp. 50 – 50, 2010.
[12] D. Song, D. Wagner, A. Perrig, “Practical techniques for searches on encrypted data,” in: SP’00, Berkeley, CA, 2000.
[13] E. Goh, “Secure indexes,” Cryptology ePrint Archive, pp. 216 – 216, 2003.
[14] A. Broder, M. Mitzenmacher, “Network applications of bloom filters: A survey,” Internet Math., vol. 1, no. 4, pp. 485 – 509, 2002.
[15] H. Cui, X. Yuan, Y. Zheng, C. Wang, “Enabling secure and effective near-duplicate detection over encrypted in-network storage,” in: INFOCOM’ 16, San Francisco, CA, 2016.
[16] Q. Liu, G. Wang, J. Wu, “Secure and privacy preserving keyword searching for cloud storage services,” J NETW COMPUT APPL., vol. 35, no. 3, pp. 927 – 933, 2012.
[17] C. Wang, N. Cao, J. Li, K. Ren, W. Lou, “Secure ranked keyword search over encrypted cloud data,” in: ICDCS’10, Genoa, Italy, 2010.
[18] C. Liu, L. Zhu, J. Chen, “Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud,” J NETW COMPUT APPL., vol. 86, pp. 3 – 14, 2017.
[19] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, “Privacy-preserving multikeyword ranked search over encrypted cloud data,” in: INFOCOM’11, Shanghai, China, 2011.
[20] A. Ibrahim, H. Jin, A. Yassin, D. Zou, “Secure rank-ordered search of multi-keyword trapdoor over encrypted cloud data,” in: APSCC’12, Guilin, China, 2012.
[21] C. Orencik, M. Kantarcioglu, E. Savas, “A practical and secure multikeyword search method over encrypted cloud data,” in: CLOUD’13, Santa Clara Marriott, CA, 2013.
[22] Z. Shen, J. Shu, W. Xue, “Preferred keyword search over encrypted data in cloud computing,” in: IWQoS’13, Montreal, Canada, 2013.
[23] B. Wang, S. Yu, W. Lou, Y. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in: INFOCOM’14, Toronto, Canada, 2014.
[24] M. Chuah, W. Hu, “Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data,” in: ICDCS’11, Minneapolis, MN, 2011.
[25] S. Pasupuleti, S. Ramalingam, R. Buyya, “An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing,” J NETW COMPUT APPL., vol. 64, pp. 12 – 22, 2016.
[26] W. Zhang, Y. Lin, S. Xiao, J. Wu, S. Zhou, “Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing,” IEEE Trans Comput., vol. 65, no. 5, pp. 1566 – 1577, 2016.
[27] S. Kamara, C. Papamanthou, “Parallel and dynamic searchable symmetric encryption,” in: FC’13, Okinawa, Japan, 2013.
[28] Z. Xu, W. Kang, R. Li, K. Yow, C. Xu, “Efficient multi-keyword ranked query on encrypted data in the cloud,” in: ICPADS’12, Nanyang Executive Center, Singapore, 2012.
[29] W. Sun, B. Wang, N. Cao, H. Li, W. Lou, Y. Hou, H. Li, “Privacypreserving multi-keyword text search in the cloud supporting similaritybased ranking,” IEEE T Parall Distr., vol. 25, no. 11, pp. 3025 – 3035, 2014.
[30] R. Li, Z. Xu, W. Kang, K. Yow, C. Xu, “Efficient multi-keyword ranked query over encrypted data in cloud computing,” FUTURE GENER COMP SY., vol. 30, pp. 179 – 190, 2014.
[31] X. Yao, Y. Lin, Q. Liu, J. Zhang, “Privacy-preserving Search over Encrypted Personal Health Record in Multi-Source Cloud,” IEEE Access, vol. 6, pp. 3809 – 3823, 2018.
[32] Y. Yi, R. Li, F. Chen, A. Liu, Y. Lin, “A digital watermarking approach to secure and precise range query processing in sensor networks,” in: INFOCOM’13, Turin, Italy, 2013.
[33] B. Chor, E. Kushilevitz, O. Goldreich, M. Sudan, “Private information retrieval,” Eurocrypt., pp. 41 – 50, 1995.
[34] C. Manning, P. Raghavan, H. Schutze, “Introduction to information retrieval,” J AM SOC INF SCI TEC., vol. 43, no. 3, pp. 824 – 825, 2009.
[35] I. Witten, A. Moffat, T. Bell, “Managing Gigabytes: Compressing and indexing documents and images,” Computer Bulletin, vol. 41, no. 6, pp. 2101 – 2101, 1995.
[36] Request for comments database.https://www.ietf.org/rfc.html.