International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

System Approach for Single Keyword Search for Encrypted data files Guarantees in Public Infrastructure Clouds

B.Nandan[1], M.Haripriya[2], N.Tejaswi[3], N. Sai Kishore[4]

Associate Professor, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India[1]
B Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India[2]
B Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India[3]
B Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India[4]

Abstract-*Cloud computing offers an important technique that is platform integrity verification that support the virtualized cloud infrastructure for hosts. Many of the cloud vendors have assembled and the judicious implementations of this mechanism. Cloud storage provides us with convenient, huge, and scalable storage at low cost, but data privacy is a major problem that prevents users from storing files on the cloud trust worthy. One way to improve privacy from data owner point of view is to encrypt the files before storing them onto the cloud and decrypt the files after downloading them. To safeguard the cloud infrastructure from corporate executive threats and advanced persistent threats, we tend to see a vast improvement vectors pertaining these implementations. Secondly, to the most effective of our information, none of the solutions provides cloud tenants a symbol concerning the integrity of figure hosts supporting their way of looking forward towards the cloud infrastructure.*

KeyWords:**CloudStorage,Security,Virtualized Infrastructure**

1. INTRODUCTION

The infrastructure cloud (IaaS) service model offers tenants with a improved assets flexibility and availability, where they are encased from the trivial details of hardware maintenance, rent computing resources to be utilized and operate complex systems. Many organizations work on delicate data to avoid relocation and replication of operations to IaaS platforms due to defense concerns. In this paper we use Order-preserving encryption (OBP) to achieve efficiency and security of data stored in a cloud, we also use another techniques like auditing protocols and third party assistance for the key management updates into a cloud by which the accessing becomes easier and the security is guaranteed and the violation of the data decreases. The industry has invested for strict security and they suggest best practices [5].The main aim of this project is to through light on IaaS. It is in its simplified form, and exposes to its users that it is coherent platform as it supports the hosts of clouds who operates VM guests can communicate by a virtual network by providing the basic requirements that are identified when an deployment of Distributed Electronic Health Record (EHR) system for an IaaS computing platform. In these years for IaaS the threats and migration has been under the intensive security [1][2][3]. At first, details of such principal solutions are not closed totally and may therefore not be enforced and enhanced by alternative cloud platforms [3].

1.2.RELATED WORK

Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues.[6] given a mechanism reliably detects whether or not the host is running a platform implementation that the remote party trusts. These platforms will effectively secure a VM running in a single host. Antonis Michalas, Nicolae Paladi and Christian Gehrmann.[7] aimed for a paperless medical system where patients and doctors are able to book appointments via the Internet, create electronic prescriptions and store their medical history in a central database, easily accessible from anyone with appropriate access rights. Patrick McDaniel, Kevin ButlerRadu Sion, Erez Zadok, Kui Ren and Marianne Winslett.[8] There are long-standing concerns beginning in large-scale systems. A recent report ready for the chairman and ranking member of the senate Committee on independent agency and environmental Affairs [8] highlighted beginning united of 3 key future technologies for securing our national crucial infrastructure.

1.3. EXISTING SYSTEM

When providers are offering security enhancements such as protection of data at rest, end-users have limited or no control over such mechanisms. There is a clear need for usable and cost-effective cloud platform security mechanisms suitable or organizations that rely on cloud infrastructure. Traditional public auditing protocols, another important task of the Third-party assistance (TPA) is to check the integrity of the client's files stored in cloud. The TPA does not know the real secret key of the client for

cloud storage auditing, but only holds an encrypted version.

2. PROPOSED SYSTEM

Proposed system presents experimental results to demonstrate the validity and efficiency of the proposed protocols to overcome the drawbacks of existing system. A basic structure underlying a system, concept, prototype is implemented on a transparent and replicable testing of scientific theories, computational tools, and new technologies, operating a public electronic health record system, showing that the proposed protocols can be integrated into existing cloud environments. Threats and mitigation is another technique where its Blinding technique with homomorphic property to form the encryption algorithm to encrypt the secret keys held by the TPA. It makes our protocol secure and the decryption operation efficient. Meanwhile, the TPA can complete key.

PROPOSED TECHNIQUE

Threats and mitigation

TECHNIQUE DEFINITION

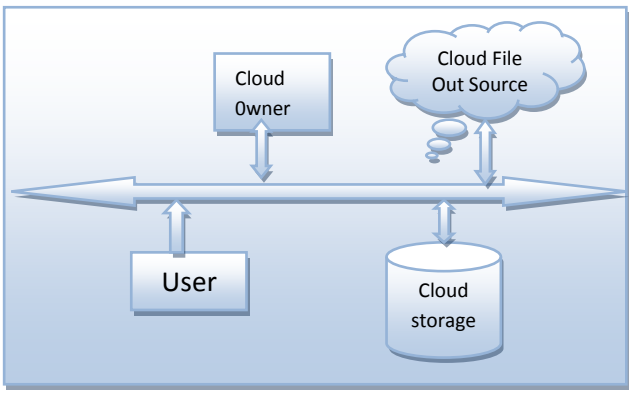
Blinding technique with homomorphism property to form the encryption algorithm to encrypt the secret keys held by the TPA. It makes our protocol secure and the decryption operation efficient. Meanwhile, the TPA can complete key updates under the encrypted state.

PROPOSED SYSTEM ADVANTAGES

- Low power resource only used.
- Data is secured for storing in cloud

2.1. SYSTEM ARCHITECTURE

In this paper it is discussed mainly about the requirements, architecture, and the way of providing user security in uploading, updating and downloading the files from cloud. The system architectures are depicted below.



ARCHITECTURE OF PROVIDING USER SECURITY GUARENTEES

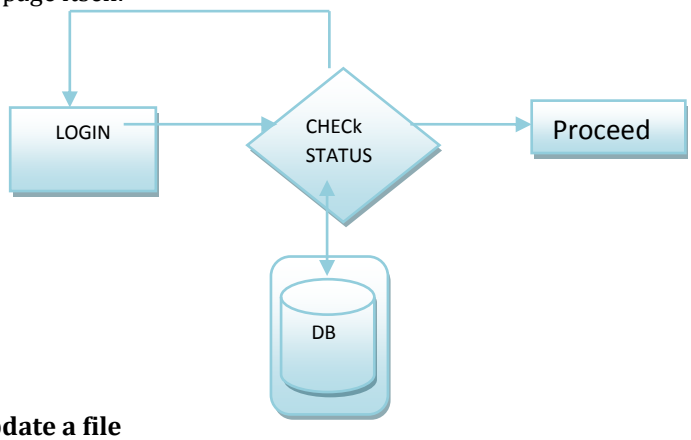
Architecture diagram explains the relationship between different components of system. Through this we can understand the concept very easily. Here, all the components cloud owner, user, cloud file outsource and cloud storage will connect to a base line for interaction .Cloud owner and the user has to authenticate by giving their unique identification numbers and passwords .Once they are verified, they will be redirected to the page where they can access and get control over the files based upon their access rights. Then user can access file from the cloud storage and after getting the private key from owner the data is decrypted and the file can be outsourced.

2.2. MODULES

CLOUD OWNER

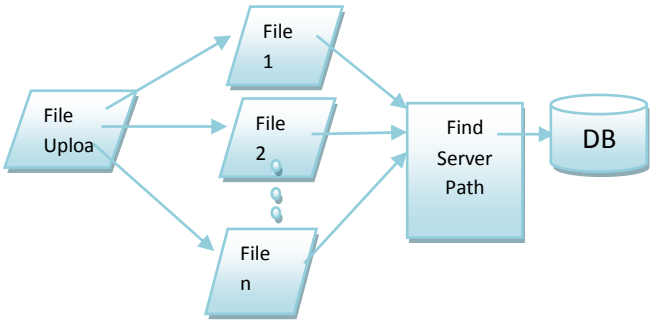
i. Authentication

The user has to give exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.



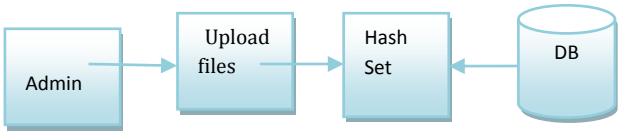
ii. Update a file

In this scheme data owner upload the multimedia files in the cloud server. Each service has different set of files. Data owner collect several file from the local path and stored in the Cloud Server. This cloud server has collection of server cluster which uniquely connected with the cloud server.



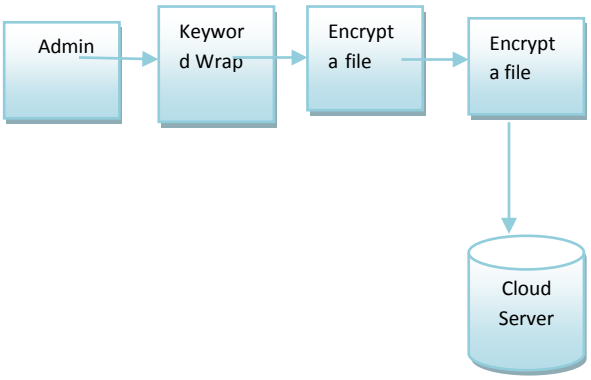
iii. Hash Set

The cloud owner will update the file information to the hash set. Which also holds the information of each the files stem words as well as the encryption key and the keyword.



iV. File outsource

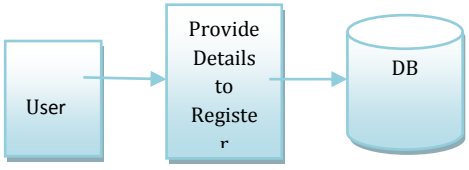
After the completion of the wrapping the file has to be encrypted before the outsourcing process. Each and every time cloud owner has to encrypt the file before outsource into cloud. This is for security reasons in the cloud server.



USER MODULE

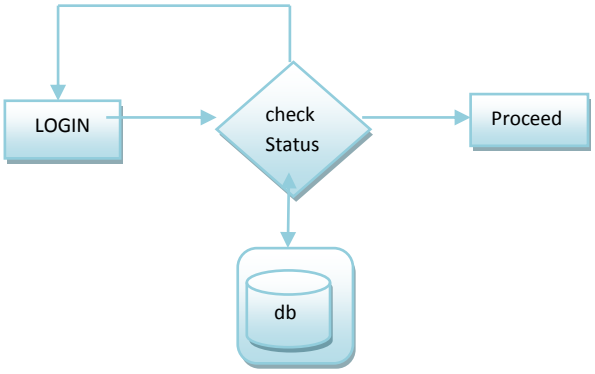
i. Registration

If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password.



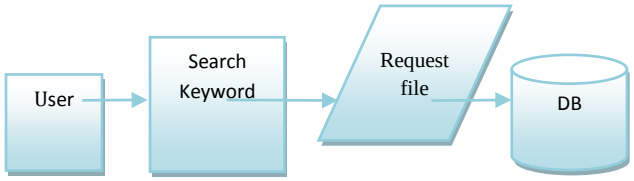
ii. Login

The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.



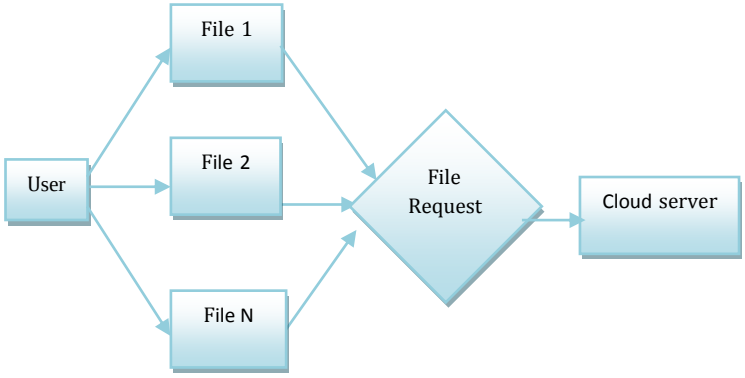
iii. Keyword search

The user after the successful login goes to view the Searching page. In that category contains could request the file into cloud server. During the Process the keyword has to be encrypted and that could be wrapped to the cloud server.



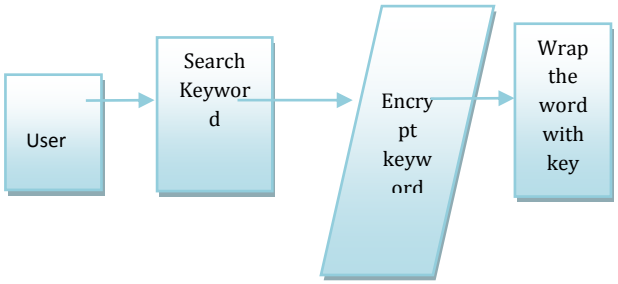
iv. Requesting File

In this phase the authenticated users view the multimedia services. The user wants to see the particular category of files then they have to access the category and they can generate a request. Once the Request is generated the Resource managers assign the task to the cloud server.



V. Wrap keyword

The requested key is then wrapped with keyword and encrypted key. If this file is fetch by the attacker or the hacker then would be difficult to get the original format. So it's tough chance to get the information.

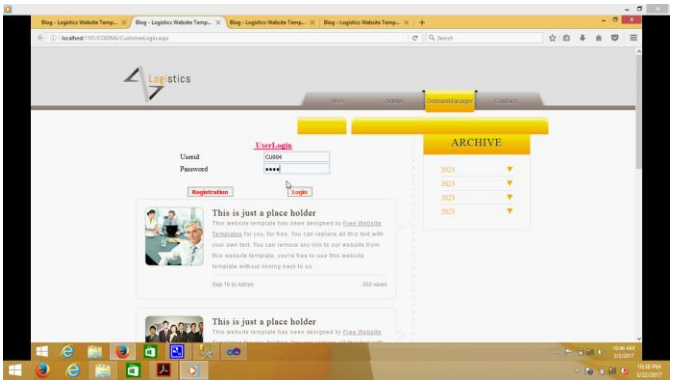


2.3. ALGORITHM USED

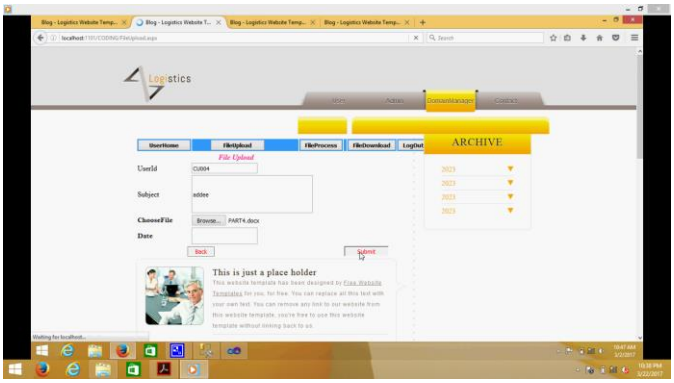
ORDER PRESERVING ENCRYPTION

An order-preserving symmetric encryption (or OPE) scheme is a deterministic symmetric encryption scheme whose encryption algorithm produces cipher texts that pre-serve numerical ordering of the plaintexts. In OPE; the order of the underlying plaintexts can be compared only with the computation of sub-linear complexity2 from the cipher texts without decrypting them. Owing to such efficiency, more efficient range queries can be supported with OPE compared to the case of using OB.

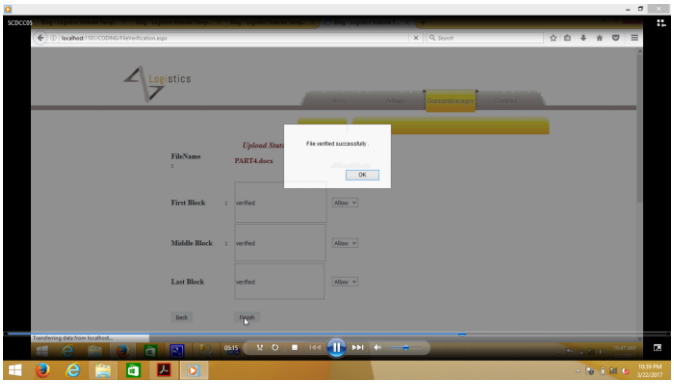
2.4. RESULTS



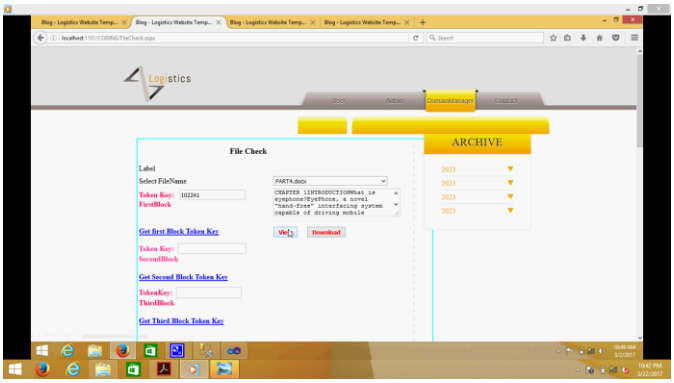
DESCRIPTION: Here user will login by giving his authenticated user identification number and a highly secured password.



DESCRIPTION: Once the user get logged in to his/her account they can upload files into the database unless it is verified by the domain manager.



DESCRIPTION: After uploading the file it will be verified by domain manager and when once it is verified we will get a notification that file has been verified successfully.



DESCRIPTION: Users can view and download the file by giving the token key provided by domain manager.

3. CONCLUSIONS

In this paper, we have proposed an system architecture about providing user security guarantees in public infrastructure clouds and single keyword search scheme to search the encrypted data files efficient and also the data security over the cloud. However, some extensions are still possible of our current work remaining. In future, We would like to propose a multi-keyword search scheme as our OPE algorithm is a simple one, another extension is to find a powerful algorithm which will not harm the efficiency

REFERENCES

[1] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel, "Seeding Clouds With Trust Anchors," in Proceedings of the 2010 ACM Workshop on Cloud Computing Security, CCSW '10, (New York, NY, USA), pp. 43–46, ACM, 2010.

[2]N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.

[3] N. Paladi, A. Michalas, and C. Gehrmann, "Domain based storage protection with secure access control for the cloud," in Proceedings of the 2014 International Workshop on Security in Cloud Computing, ASIACCS '14, (New York, NY, USA), ACM, 2014.

[4] M. Jordon, "Cleaning up dirty disks in the cloud," Network Security, vol. 2012, no. 10, pp. 12–15, 2012.

[5] Cloud Security Alliance, "The notorious nine cloud computing top threats 2013," February 2013.

[6] O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing(CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.