ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Relay Selection for Geographical Forwarding in Sleep-Wake Cycling Wireless Sensor Networks

K. Venkata Rangarao
Department of Computer Science & Engineering
Jogaiah Institute of Technology and Sciences College of Engineering,
Palakol, West Godavari Dt., A.P-534 268, India.

Mr.A.Veerabhadra Rao
Department of Computer Science & Engineering
Jogaiah Institute of Technology and Sciences College of Engineering,
Palakol, West Godavari Dt., A.P-534 268, India.

ABSTRACT:

Temporary keyword search on confidential data in a cloud environment is the main focus of this research. The cloud providers are not fully trusted. So, it is necessary to outsource data in the encrypted form. In the attribute-based keyword search (ABKS) schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation. These search tokens can be used to extract all the cipher texts which are produced at any time and contain the corresponding keyword. Since this may lead to some information leakage, it is more secure to propose a scheme in which the search tokens can only extract the cipher texts generated in a specified time interval but searching with a single key is time taken and to overcome this multiple keyword search is introduced. To this end, in this paper, we introduce a new cryptographic primitive called key-policy attribute-based temporary keyword search (KPABTKS) which provide this property.

INTRODUCTION

A key policy attribute based temporary keyword search for secure cloud storage

Attribute-based encryption (ABE) [1-5] is viewed as a persuading encryption framework with fine grained access control in the flowed stockpiling. Attribute-based encryption can be distributed two sorts of key-policy attribute-based encryption (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE). The KP-ABE plan suggests that the cipher text is associated with an attribute set, and a client's enigma key is associated with a way policy. A client can unscramble the cipher text if and just if the cipher text's attribute set fulfill the path policy of client's riddle key. The CP-ABE plan proposes that the cipher text is associated with a section policy, and a client's mystery key is associated with an attribute set. A client is can unscramble the cipher text if and just if his attribute set fulfill the entry policy of the cipher text.

At present, different ABE plans have been proposed, which give secure information access control and beat the deficiencies of balanced encryption setup in character based encryption plot. In any case, these plans are up to this point flawed to be utilized in the end, as the attribute of a client is dynamic, which might be changed after some time. In this way the attribute disavowal fragment is major for ABE plan to be utilized after a short time [7].

Public key encryption with keyword search

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is

Cite this article as: K. Venkata Rangarao & Mr.A.Veerabhadra Rao, "Relay Selection for Geographical Forwarding in Sleep-Wake Cycling Wireless Sensor Networks", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6 Issue 8, 2019, Page 1-8.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

Vabks: Verifiable attribute-based keyword search over outsourced encrypted data

It is ordinary nowadays for data owners to re-fitting their data to the cloud. Since the cloud can't be totally accepted, the re-appropriated data should be encoded. This in any case brings an extent of issues, for instance, How should a data owner honor search abilities to the data customers? In what limit can the endorsed data customers search over a data owner's redistributed encoded data? In what limit can the data customers be ensured that the cloud relentlessly executed the request undertakings for their advantage? Impelled by these request, we propose a novel cryptographic course of action, called unquestionable attribute-based keyword search (VABKS). The game plan allows a data customer, whose accreditations satisfy a data owner's passage control policy, to (I) search over the data owner's re-appropriated mixed data, (ii) redistribute the redundant request exercises to the cloud, and (iii) affirm whether the cloud has relentlessly executed the interest errands. We authoritatively portray the security necessities of VA B K S and delineate an improvement that satisfies them. Execution appraisal shows that the proposed plans are sensible and deployable [9].

Anonymous hierarchical identity-based encryption (without random oracles)

We present a character based cryptosystem that features totally baffling ciphertexts and dynamic key task. We give a proof of security in the standard model, based on the smooth Decision Linear multifaceted nature doubt in bilinear social affairs. The structure is gainful and handy, with little ciphertexts of size direct in the significance of the dynamic framework. Applications consolidate request on encoded data, totally private correspondence, and so on. Our results settle two open issues identifying with obscure character based encryption, our arrangement being the first to offer provable anonymity in the standard model, notwithstanding being the first to recognize totally puzzling HIBE at all levels in the pecking request.

Efficient public key encryption with revocable keyword search

Open key encryption with keyword search is a novel cryptographic rough engaging one to look on the mixed data direct. In the known plans, once getting a trapdoor, the server can look related data without any controls. In any case, in reality, it is a portion of the time essential to shield the server from glancing through the data all the time in light of the way that the server isn't totally trusted. In this paper, we propose open key encryption with revocable keyword search to address the issue. We in like manner develop a strong advancement by segregating the whole presence of the structure into indisputable events to achieve our goals. The proposed arrangement achieves the properties of the in recognizability of ciphertexts against a flexible picked keywords attack security under the co-decisional bilinear Diffie–Hellman supposition [11] in our security model. Differentiated and two somewhat schemes, our own offers much better execution to the extent computational cost.

Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement

Keyword-based interest over mixed re-appropriated data has transformed into a huge instrument in the present circulated registering circumstance. A large portion of the present strategies are focusing on multi-keyword exact match or single keyword soft chase. In any case, those present procedures discover less rational centrality in evident applications differentiated and the multi-keyword soft request strategy over mixed data. The primary undertaking to manufacture such a multi-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

keyword soft request plan was represented by Wang et al., who used zone sensitive hashing limits and Bloom isolating to meet the target of multi-keyword cushioned chase. Incidentally, Wang's arrangement was convincing for a one letter mess up in keyword anyway was not reasonable for other typical spelling bungles. Additionally, Wang's arrangement was powerless against server out-of-demand issues during the situating system and did not consider the keyword weight. In this paper, based on Wang et al's. plot, we propose a viable multi-keyword cushy situated pursuit plan based on Wang et al's. plot that can address the recently referenced issues. In any case, we develop another procedure for keyword change based on the uni-gram, which will simultaneously improve the accuracy and makes the ability to handle other spelling messes up. Likewise, keywords with a comparable root can be addressed using the stemming estimation. In addition, we consider the keyword weight when picking an adequate organizing record set. Assessments using genuine data exhibit that our arrangement is fundamentally profitable and achieve high accuracy.

EXISTING SYSTEM:

In PEKS, each data owner who knows the public key of the intended data user generates a searchable cipher-text by means of his/her public key, and outsources it to the cloud. In attribute-based keyword search (ABKS) to allow a data owner to control the access of data users for searching on his/her outsourced encrypted data. However, in all of the PEKS and ABKS schemes [12], once the cloud receives a valid search token related to a certain keyword, the cloud can investigate the keyword's presence in the past and any future cipher-text. So, if the adversary realizes the corresponding keyword of the target search token, then she will be able to get some information about the next documents which will be outsourced to the cloud. By using this we cannot protect our documents .To provide security a new cryptographic primitive called key-policy attribute-based temporary keyword search (KPABTKS) which provide this property. To evaluate the security of our scheme, we formally prove that the keyword secrecy property and is secure against selectively chosen keyword attack (SCKA) [10].But searching with a single keyword is time taken and to overcome this we proposed key-policy attribute-based temporary keyword search(KPABTKS) with multiple keywords.

DISADVANTAGES:

- It is difficult to find and search file with the single key word.
- User can't access the data in time if they don't know the key.

PROPOSED SYSTEM

In this we propose a multi keyword searchable encryption scheme in which the search token is applicable to find the cipher text in special time instance. In this schema, we use a multi keyword search to retrieve the data within a time interval. Furthermore, we show that the complexity of the encryption algorithm is linear with respect to the number of the involved attributes. Performance evaluation shows our scheme's practicality [8].

Advantages:

- Security is high.
- Efficiency is improved.
- Data can be available within the time interval. So, there is no possibility lose the data.

Implementation

MODULES

- Data owner
- Data user
- Cloud Server (CS)
- Trusted Third Party (TTP)

Data owner:

The whole technique, main person is the data owner can generates the cipher text and encryption time while uploading it to the cloud. He has an ability to give multiple keywords during file uploading time. He has an ability to give that specific time interval within that interval only user can see that cipher text.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data user:

Data user is an entity who is looking for the documents or files which are uploaded by the data owners. If he search that file by using multiple keywords which are uploaded by the data owner within the time interval then he can view that cipher text and encryption time. If he satisfied that access policy, he sends file request to cloud for running the search operations.

Cloud Server (CS):

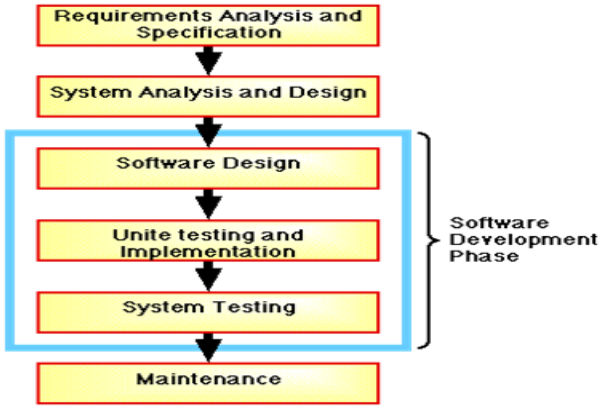
Cs isthe people who place a major role in that, Cs can store the cipher text along with the encryption time and specific time interval. Here Cs can receive the search tokens' from the user and find the files corresponding to that keyword, and sends them back to the data user.

Trusted Third Party (TTP):

TTP Is a fully trusted entity who receives user's request from cloud and generates their secret keys corresponding to his/her keywords .finally TTP sends that secrete keys back to the users by using his/her credentials [6].

Waterfall Model:

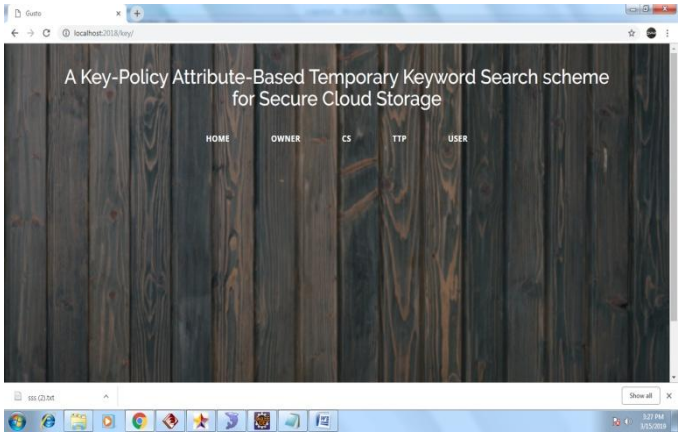
The Waterfall Model was first Process Model to be introduced. It is also referred to as a linear-sequential life cycle model. It is very simple to understand and use. In a waterfall model, each phase must be completed fully before the next phase can begin. At the end of each phase, a review takes place to determine if the project is on the right path and whether or not to continue or discard the project. In waterfall model phases do not overlap [4].



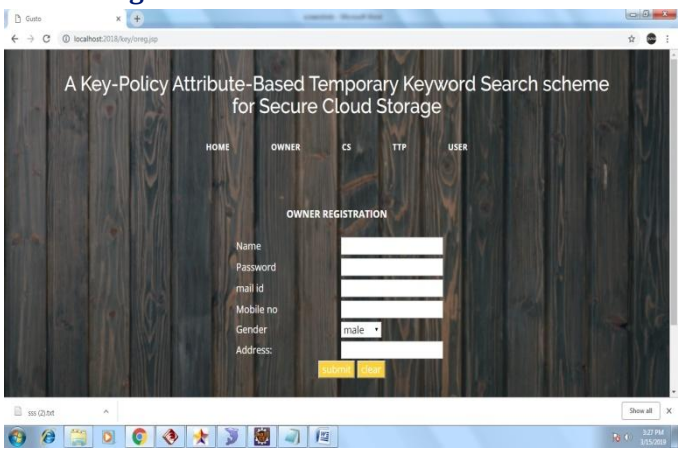
Results

Resulted Screens

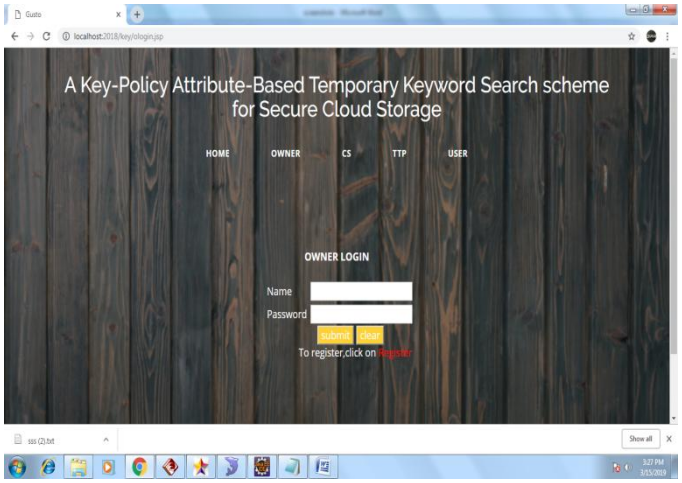
Home



Owner Registration

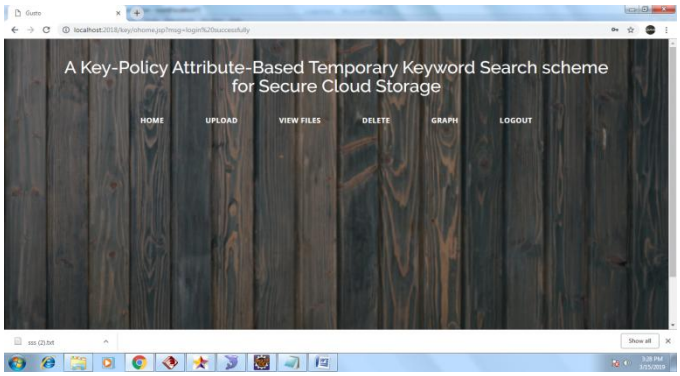


Owner Login

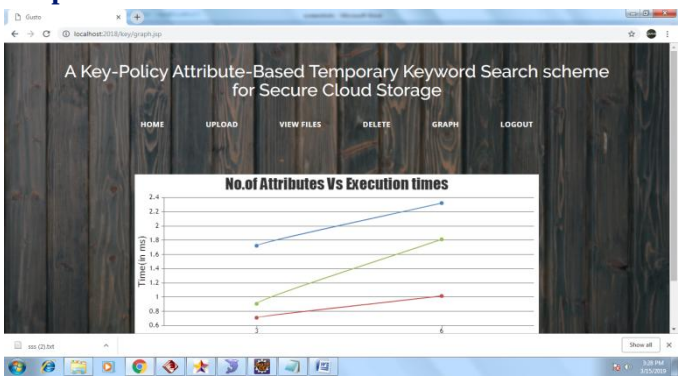


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

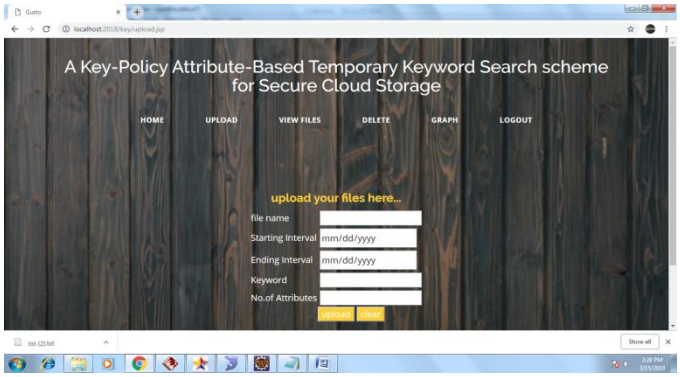
Owner Home



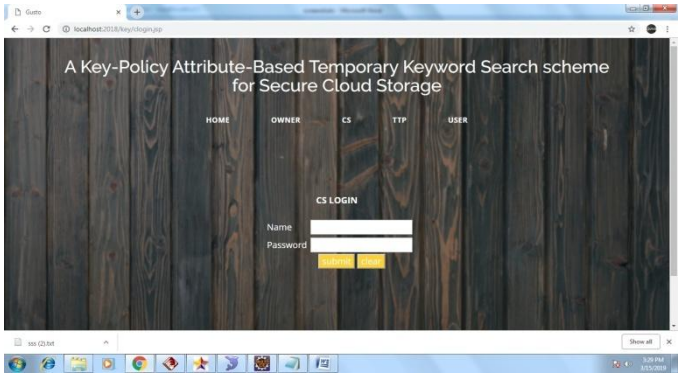
Graph



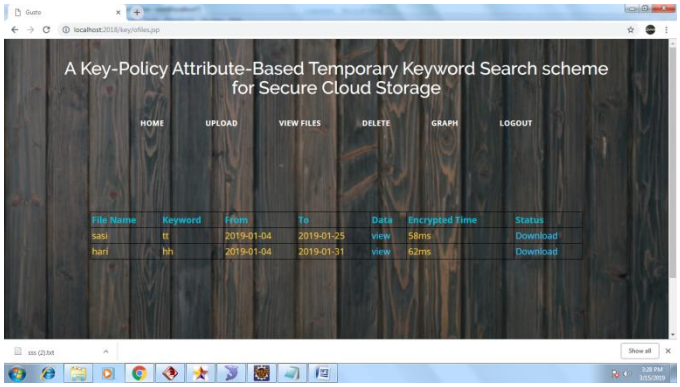
Upload



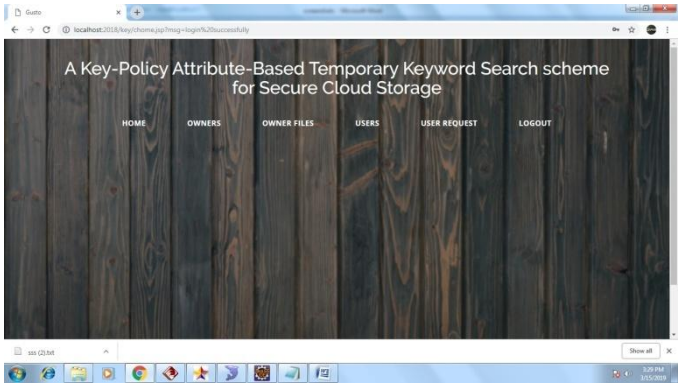
CS Login



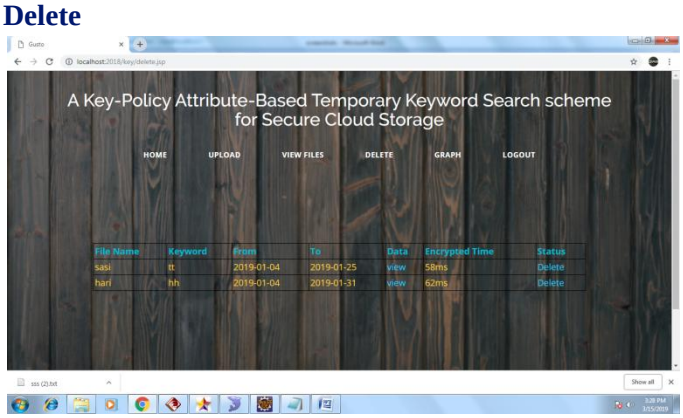
View Files



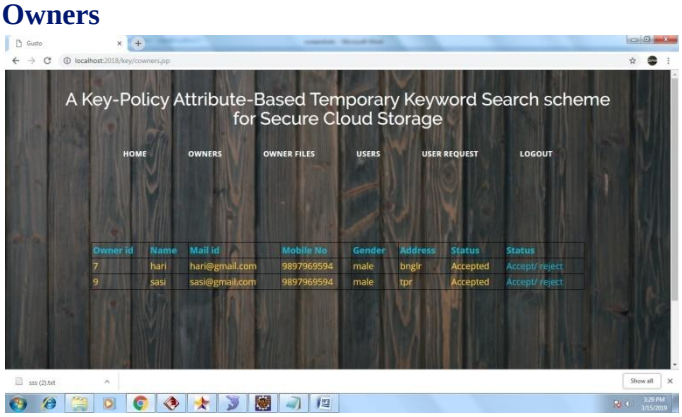
CS Home



Delete

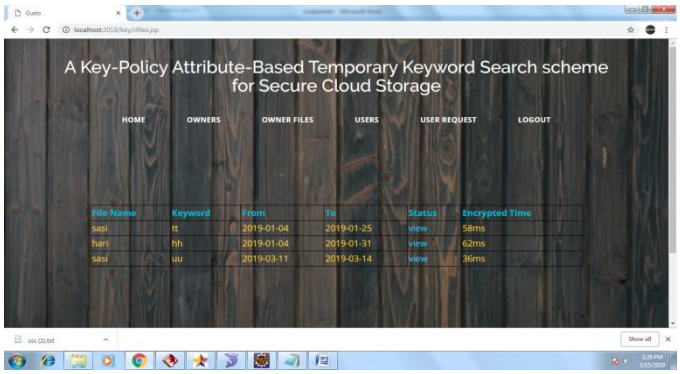


Owners

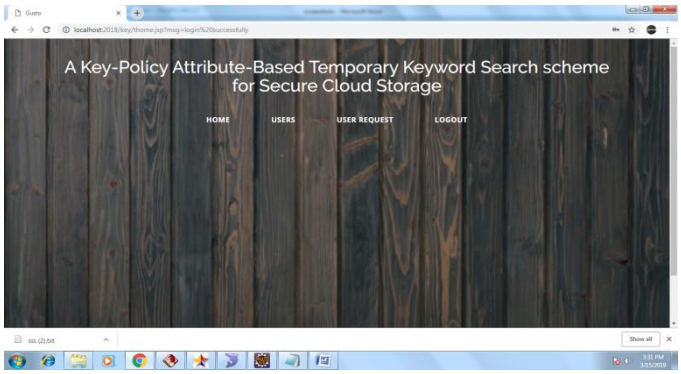


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

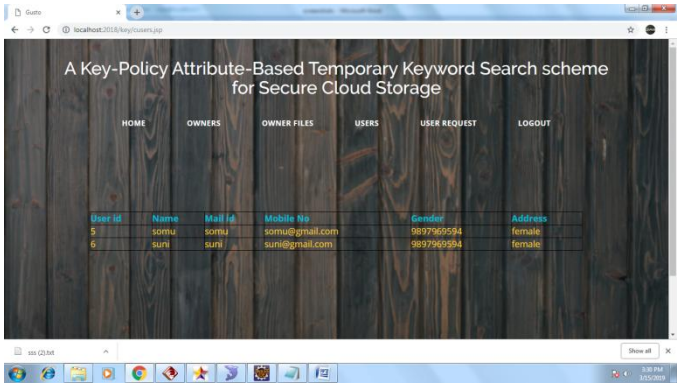
Owner Files



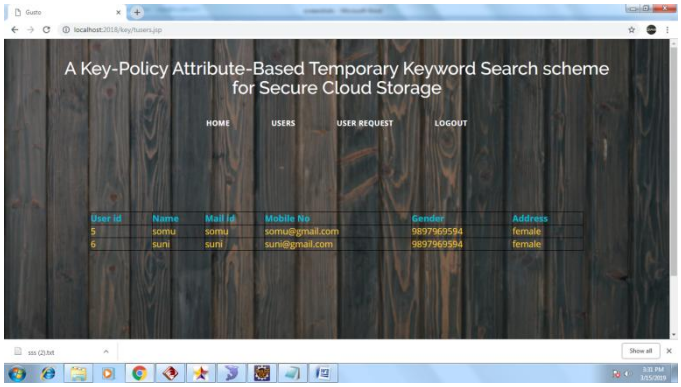
TTP Home



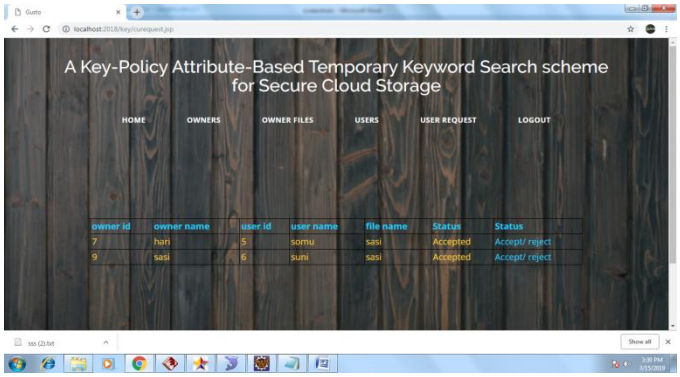
Users



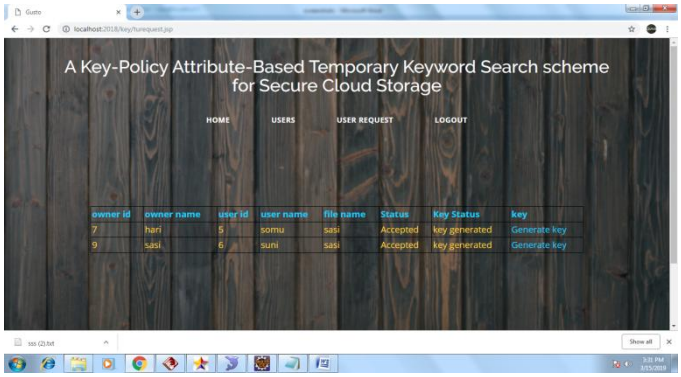
Users



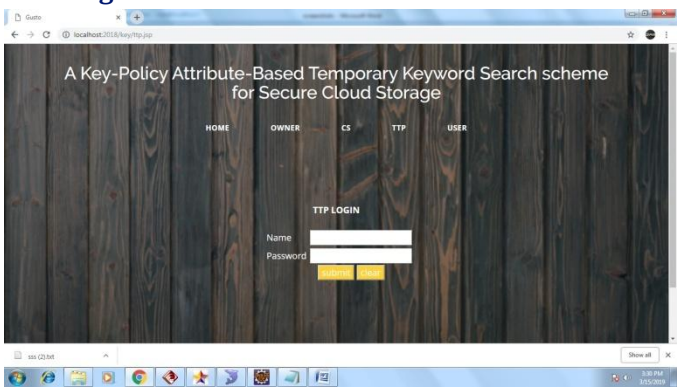
User Request



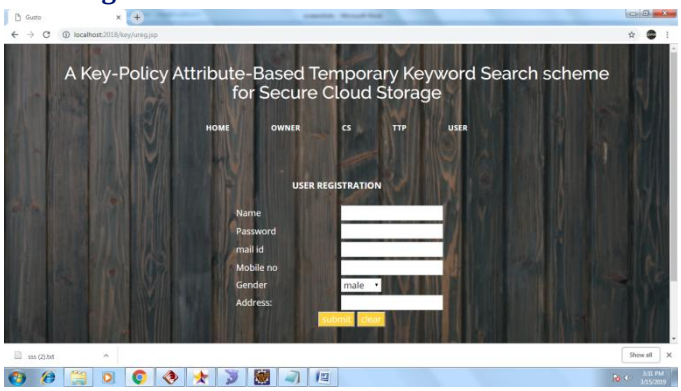
User Request



TTP Login

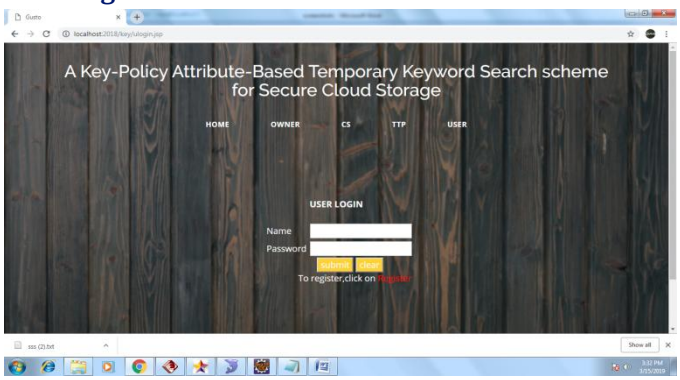


User Registration

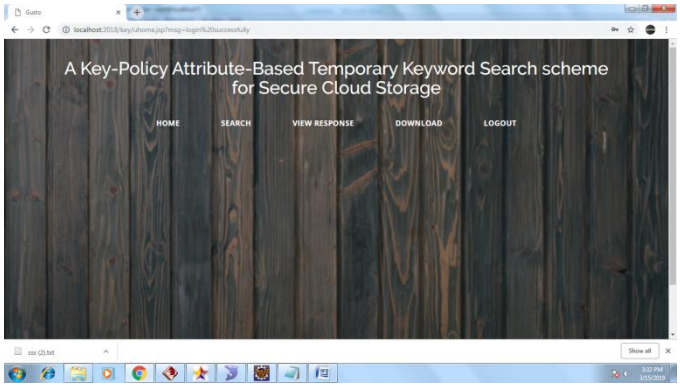


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

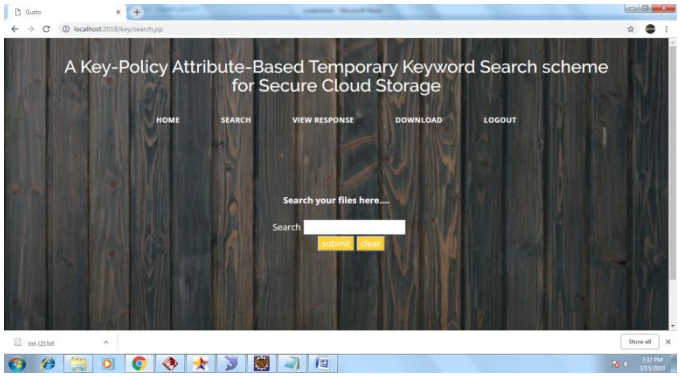
User Login



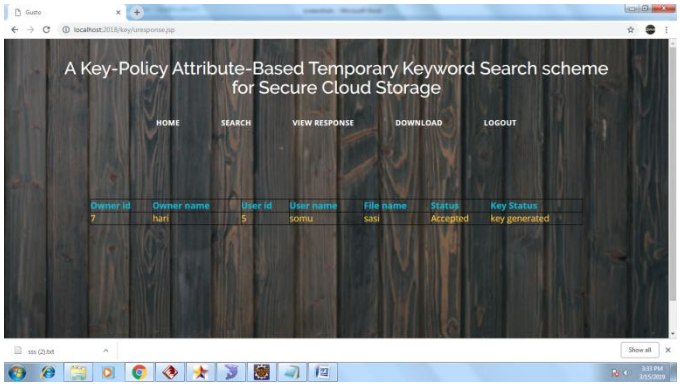
User Home



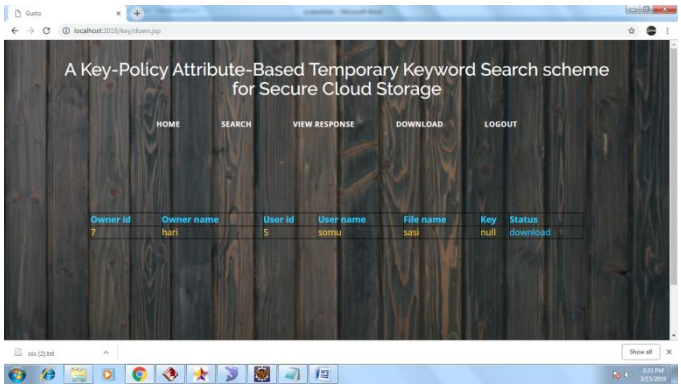
Search



View Responce



Download



CONCLUSION

In this paper, we have proposed a keyword searchable attribute-based encryption scheme with attribute update for cloud storage. Our new scheme supports both the user's attribute update and supports multi-user keywords search, as long as user's trapdoor could match keyword index stored in the cloud storage, then the user can search interesting encrypted file successfully. The performance evaluation results confirm that the proposed scheme is more efficient than other attribute based encryption schemes with attribute update. In addition, we outsource the operation with high computation cost to the cloud storage to reduce the user's computational burden. Moreover, our scheme also is proven to be semantic security against chosen ciphertext-policy and chosen plaintext attack in the general bilinear group model.

REFERENCES

[1] K. Yigzaw, A. Michalas, and J. Bellika, “Secure and scalable statistical computation of questionnaire data in r,” IEEE Access, vol. PP, no. 99, pp. 1–1, 2016.

[2] A. Michalas, N. Paladi, and C. Gehrmann, “Security aspects of e-health systems migration to the cloud,” in e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on, pp. 212–218, IEEE, 2014.

[3] A. Michalas and M. Bakopoulos, “Secgod google docs: Now i feel safer!,” in 2012 International

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Conference for Internet Technology And Secured Transactions, pp. 589–595, Dec 2012.

[4] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2016. [5] K. Y. Yigzaw, A. Michalas, and J. G. Bellika, "Secure and scalable deduplication of horizontally partitioned health data for privacy-preserving distributed statistical computation," BMC Medical Informatics and Decision Making, vol. 17, no. 1, p. 1, 2017.

[6] A. Michalas and R. Dowsley, "Towards trusted ehealth services in the cloud," in 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), pp. 618–623, Dec 2015.

[7] R. Dowsley, A. Michalas, and M. Nagel, "A report on design and implementation of protected searchable data in iaas," tech. rep., Swedish Institute of Computer Science (SICS), 2016.

[8] Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hbsch, and I. Paraskakis, "Paasword: A holistic data privacy and security by design framework for cloud services," in Proceedings of the 5th International Conference on Cloud Computing and Services Science, pp. 206–213, 2015. [9] A. Michalas and K. Y. Yigzaw, "Locless: Do you really care your cloud files are?," in 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC), pp. 618–623, Dec 2015.

[10] A. Michalas, "Sharing in the rain: Secure and efficient data sharing for the cloud," in 2016 International Conference for Internet Technology And Secured Transactions, pp. 589–595, Dec 2016.

[11] 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.

[12] Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hubsch, and ¨ I. Paraskakis, "Paasword: A holistic data privacy and security by design framework for cloud services," pp. 1–16, 2017.