

## International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

# Robust Traceable Keyword Search on Encrypted Cloud Storage

Mr.Suraj Hanumant Shinde<sup>1</sup>, Ms.Toshal Gore<sup>2</sup>, Ms.Achla Kumari<sup>3</sup>, Mr.Pravin Shivaji Kadam<sup>4</sup>,  
Prof.Anuja Palhade<sup>5</sup>

Student, Department of Information Technology Dhole Patil College of Engineering, Wagholi, India<sup>1, 2, 3, 4</sup>

Faculty, Department of Information Technology Dhole Patil College of Engineering, Wagholi, India<sup>5</sup>

**ABSTRACT:** The administration of access control and the support of keyword search are some issues which are important in secure cloud storage system. With the appearances of cloud computing, data owners are founded to outsource their tricky data management systems from local sites to the commercial public cloud and it is to achieve flexibility and economic savings. But to protecting data privacy, sensitive data have to be encrypted before outsourcing data, which out dated traditional data utilization based on plaintext keyword search. Consider many number of data users and documents in the cloud, and it is mandatory to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. This system design will provide an efficient traceable authorization search system for secure cloud storage, which overcomes all these limitations. Inflexible authorized keyword search, Abuse of attribute secret key, inefficient decryption.

**KEYWORDS:** authorized searchable encryption, traceability, multiple keywords subset search, cloud computing.

## I. INTRODUCTION

Secure search over encrypted remote data is crucial in cloud computing to provide guaranteed data privacy and usability. Avoiding unauthorized data usage, fine-grained access control is necessary in multi-user system. Sometimes, authorized user also leak the secret key for financial benefit. Thus, tracing and revoking the malicious person who abuses secret key needs to be solved imminently. CLOUD computing is a totally fascinating computing paradigm, wherein computation and storage are moved far from terminal gadgets to the cloud. This new and popular paradigm brings important revolutions and makes bold improvements for the way wherein businesses and individuals manipulate, distribute, and proportion content. By outsourcing their information technology skills to a few cloud carrier providers, cloud users may also achieve significant fee financial savings. With the arrival of cloud computing, data owners are motivated to outsource their complex records management systems from local websites to the commercial public cloud for notable flexibility and economic savings. But for protective data privateness, data must be encrypted before outsourcing, which obsoletes conventional facts utilization based on plaintext key-word search. Thus, allowing an encrypted cloud data search service is of paramount significance. Considering the multiple number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords.

## II. REVIEW OF LITERATURE

### 1. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

In this paper, With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple

# International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of “coordinate matching,” i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use “inner product similarity” to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication.[4]

## 2. Adaptively Secure Identity-Based Broadcast Encryption with a Constant-sized Ciphertext

In this paper, we present an adaptively secure identity-based broadcast encryption system featuring constant sized ciphertext in the standard model. The size of the public key and the private keys of our system are both linear in the maximum number of receivers. Also, our system is fully collusion-resistant and has stateless receivers. Compared with the state-of-the-art, our scheme is well optimized for the broadcast encryption. The computational complexity of decryption of our scheme depends only on the number of receivers, not the maximum number of receivers of the system. Technically, we employ dual system encryption technique and our proposal offers adaptive security under the general subgroup decisional assumption. Our scheme demonstrates that the adaptive security of the schemes utilizing a composite order group can be proven under the general subgroup decisional assumption while many existing systems working in a composite order group are secure under multiple subgroup decision assumptions. We note that this finding is of an independent interest, which may be useful in other scenarios.[1]

## 3. Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption

In this paper, Attribute-based encryption (ABE) provides a mechanism for complex access control over encrypted data. However in most ABE systems, the ciphertext size and the decryption overhead, which grow with the complexity of the access policy, are becoming critical barriers in applications running on resource-limited devices. Outsourcing decryption of ABE ciphertexts to a powerful third party is a considerable manner to solve this problem. Since the third party is usually believed to be untrusted, the security requirements of ABE with outsourced decryption should include privacy and verifiability. Namely, any adversary including the third party should learn nothing about the encrypted message, and the correctness of the outsourced decryption is supposed to be verified efficiently. We propose generic constructions of CPA-secure and RCCA-secure ABE systems with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption, respectively. We also instantiate our CPA-secure construction in the standard model and then show an implementation of this instantiation. The experimental results show that, compared with the existing scheme, our CPA-secure construction has more compact ciphertext and less computational costs. Moreover, the techniques involved in the RCCA-secure construction can be applied in generally constructing CCA-secure ABE, which we believe to be of independent interest[2].

## 4. Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption

In this paper, we proposed a new construction of CP-ABE, named Privacy Preserving Constant CP-ABE that significantly reduces the ciphertext to a constant size with any given number of attributes. Furthermore, PP-CP-ABE leverages a hidden policy construction such that the recipients' privacy is preserved efficiently. As far as we know, PP-CP-ABE is the first construction with such properties. Furthermore, we developed a Privacy Preserving Attribute Based Broadcast Encryption (PP-AB-BE) scheme. Compared to existing Broadcast Encryption (BE) schemes, PP-AB-BE is more flexible because a broadcasted message can be encrypted by an expressive hidden access policy, either with or without explicitly specifying the receivers. Moreover, PP-AB-BE significantly reduces the storage and communication overhead to the order of  $O(\log N)$ , where  $N$  is the system size. Also, we proved, using information theoretical

## International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

approaches, PP-AB-BE attains minimal bound on storage overhead for each user to cover all possible subgroups in the communication system [3].

### 5. Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Gussing Attack

In this paper public-key encryption with fuzzy keyword search (PEFKS)., each keyword corresponds to an exact keyword search trapdoor and a fuzzy keyword search trapdoor. Two or more keywords share the same fuzzy keyword trapdoor. To search encrypted documents containing a specific keyword, only the fuzzy keyword search trapdoor is provided to the third party, i.e., the searcher. Thus, in PEFKS, a malicious searcher can no longer learn the exact keyword to be searched even if the keyword space is small. We propose a universal transformation which converts any anonymous identity-based encryption (IBE) scheme into a secure PEFKS scheme. Following the generic construction, we instantiate the first PEFKS scheme proven to be secure under KGA in the case that the keyword space is in a polynomial size.

### 6. J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 1343- 1354.

In this paper, we proposed a simple and generic method to convert any ABE scheme with non-verifiable outsourced decryption to an ABE scheme with verifiable outsourced decryption in the standard model. To concretely assess the performance of the new method, we presented an instantiation of our generic method based on Green et al.'s outsourced CPABE scheme without verifiability.

## III. EXISTING SYSTEM

A introduced a distributed attribute based encryption technique because ciphertext policy attribute-Based Encryption allows to encrypt data under an access policy, specified as a logical combination of attributes. Such cipher-texts can be decrypted by anyone with a set of attributes that fits the policy. But in distributed attribute-based encryption, where an arbitrary number of parties can be present to maintain attributes and their corresponding secret keys. This is in bare difference to the classic ciphertext policy attribute based encryption schemes, where all keys are distributed by one central trusted party. We provide the construction of a DABE scheme; the construction is very efficient for encryption and decryption.

A Secure attribute based systems in which attributes define and classify the data to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In which a novel secure information management architecture is introduced based on emerging attribute-based encryption primitives. A policy system that meets the needs of complex policies is defined and illustrated. Based on the needs of those policies, therefore proposed a cryptographic optimizations that vastly improve enforcement efficiency.

# International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

## IV. SYSTEM ARCHITECTURE

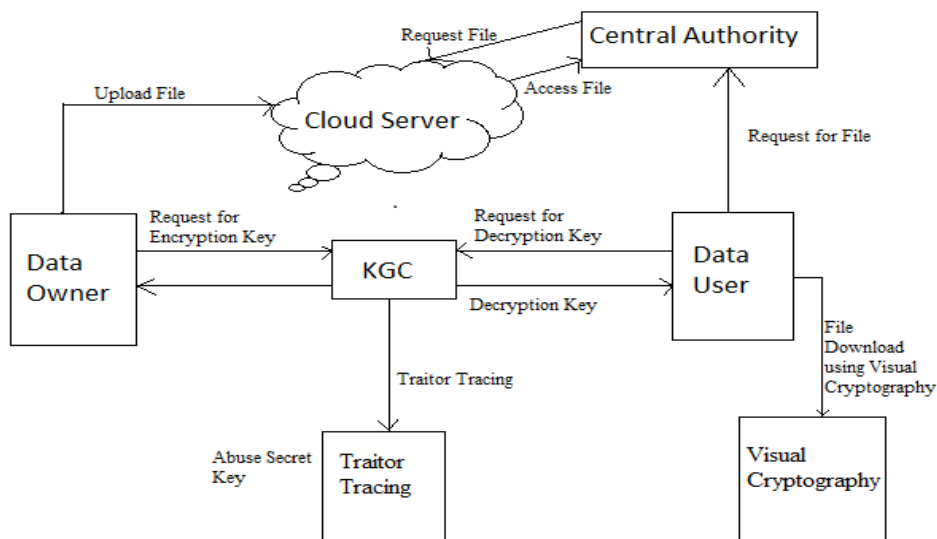


Fig. 1. Propose System Architecture

This system design will provide an efficient traceable authorization search system for secure cloud storage, which overcomes all limitations of existing system. Inflexible authorized keyword search, abuse of attribute secret key, inefficient decryption. Sometimes authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the unauthorized user who abuses secret key needs to be solved imminently.

## V. ALGORITHM

### AES Algorithm

1. KeyExpansions  
For each round AES requires a separate 128-bit round key block plus one more.
2. InitialRound  
AddRoundKey—with a block of the round key, each byte of the state is combined using bitwise xor.
3. Rounds
  - SubBytes—in this step each byte is replaced with another byte.
  - ShiftRows—for a certain number of steps, the last three rows of the state are shifted cyclically.
  - MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  - AddRoundKey
1. Final Round (no MixColumns)
  - SubBytes
  - ShiftRows
  - AddRoundKey.

# International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

## MD5 Algorithm

Computation of the MD5 digest value is performed in separate stages that process each 512-bit block of data along with the value computed in the preceding stage:

1. The first stage begins with the message digest values initialized using consecutive hexadecimal numerical values.
2. Each stage includes four message digest passes which manipulate values in the current data block and values processed from the previous block.
3. The final value computed from the last block becomes the MD5 digest for that block.

## Visual Cryptography

- Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.
- Visual Cryptography is a wide area of research used in data hiding, securing images, color imaging, multimedia and other such fields.

## VI. RESULT

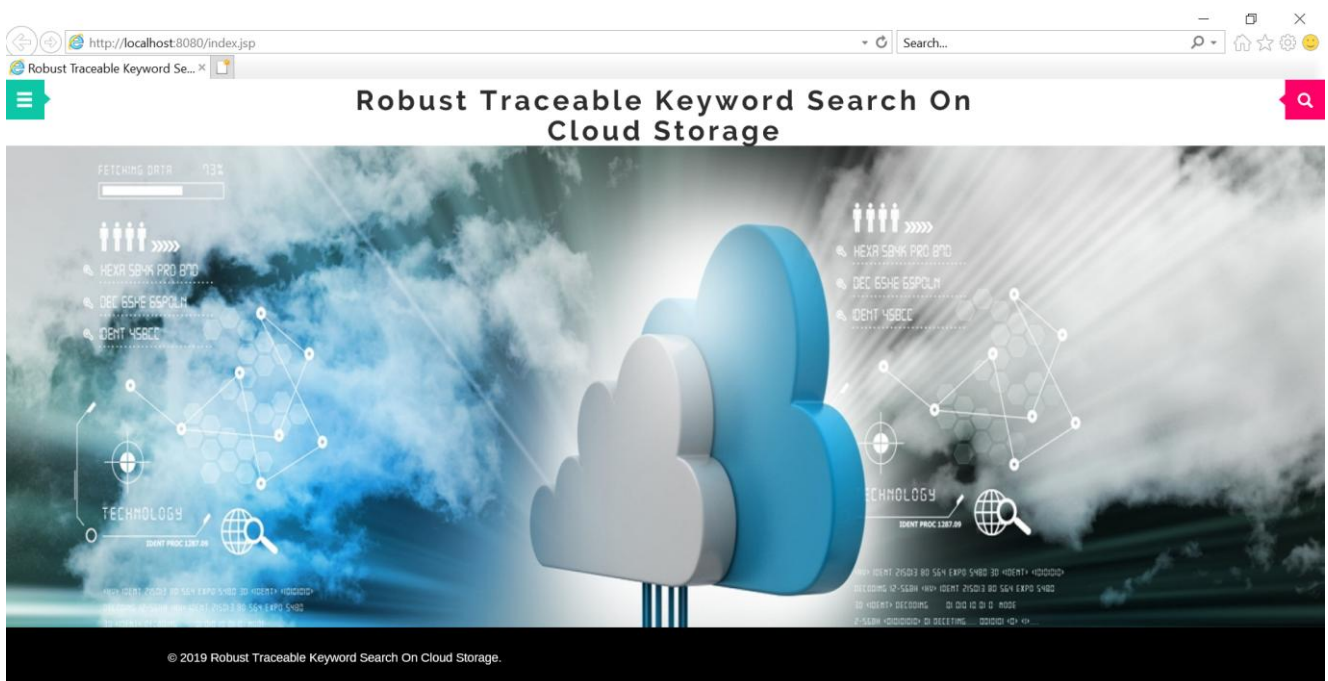


Fig 1: Homepage

# International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

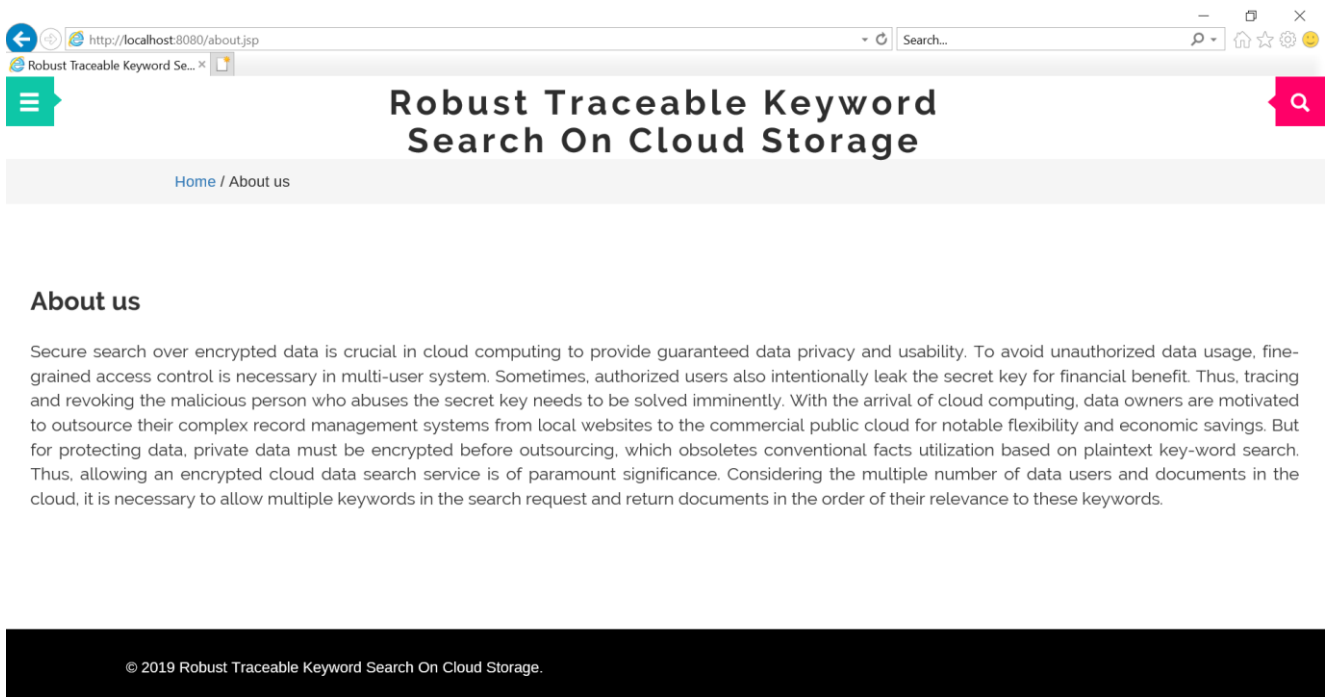


Fig 2: About Us

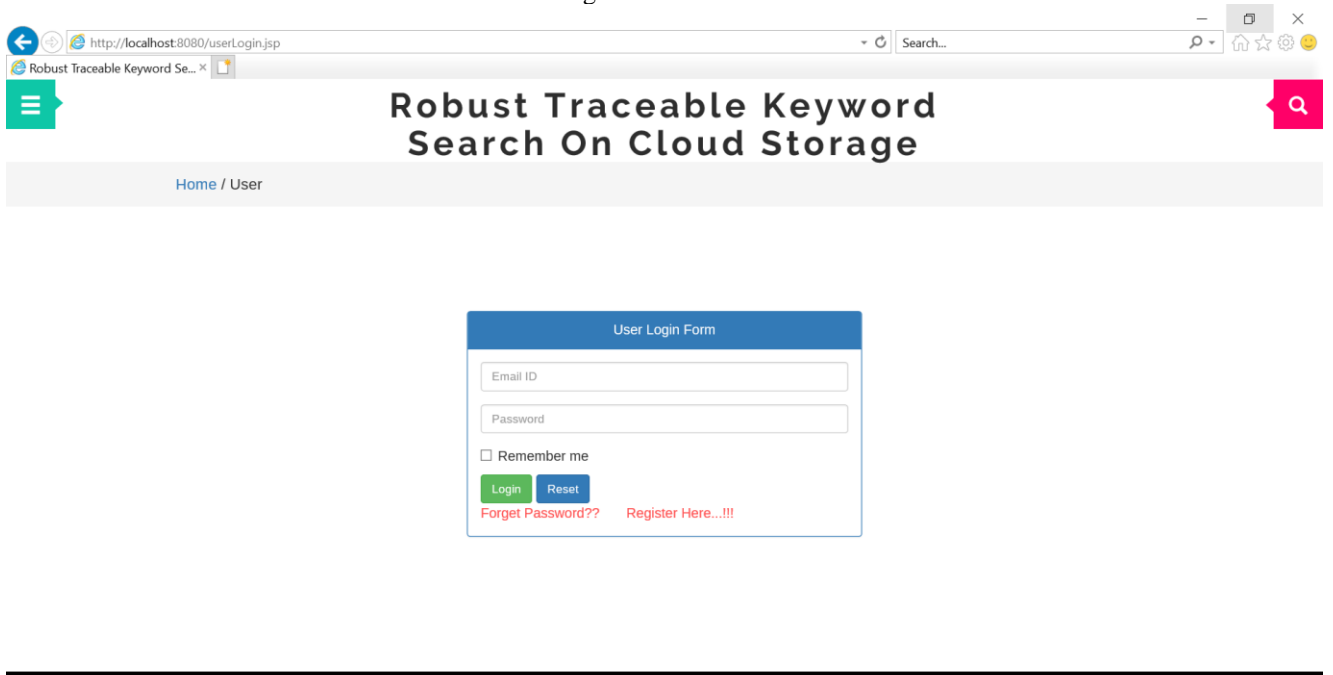


Fig 3: User Login

# International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

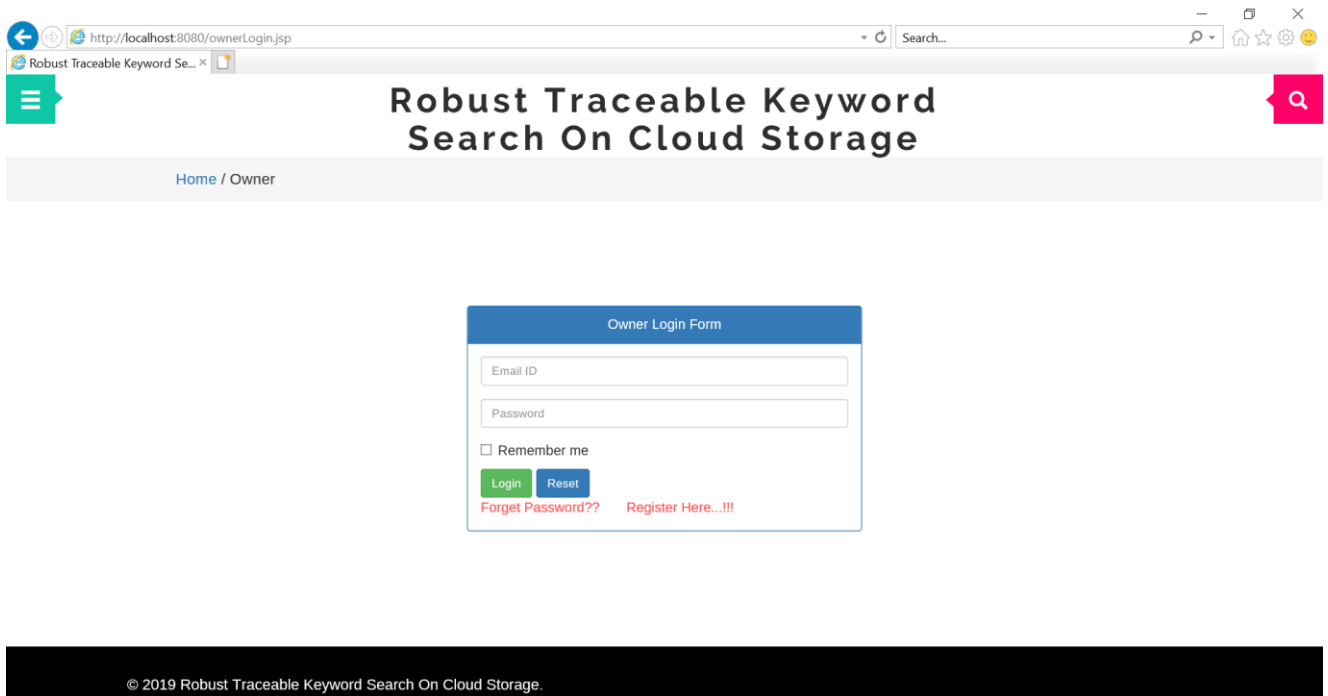


Fig 4: Owner Login

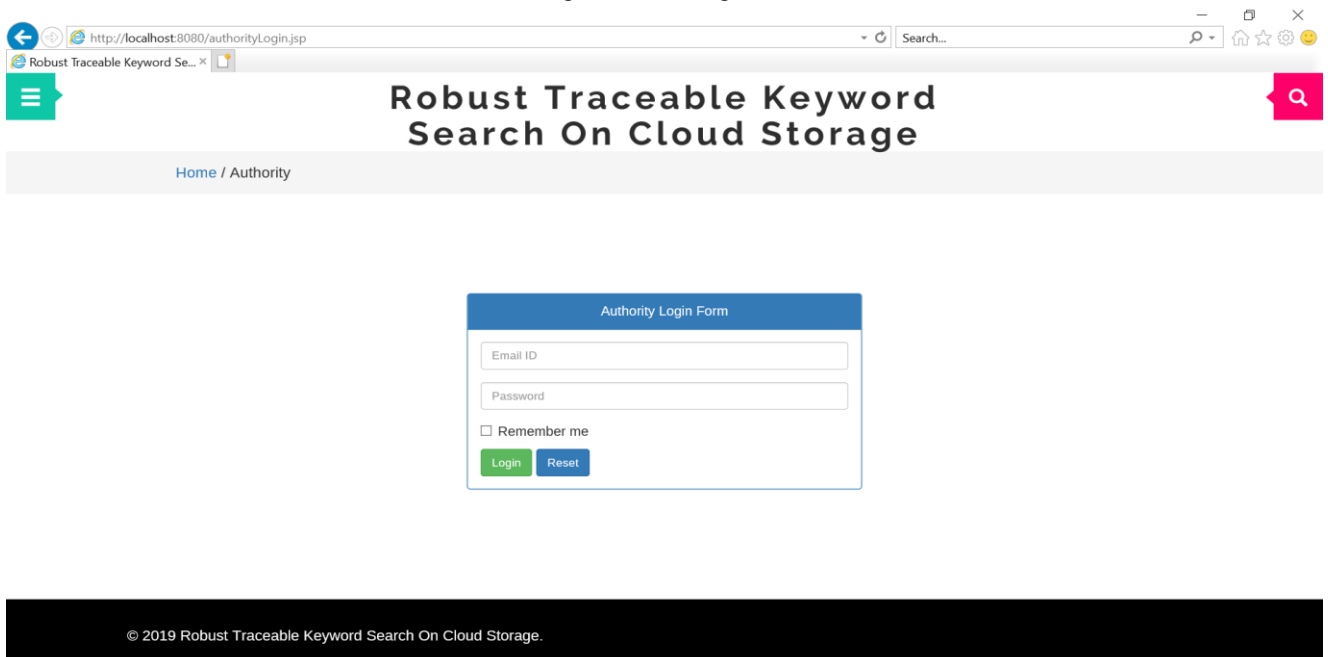


Fig 5: Authority Login

# International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020

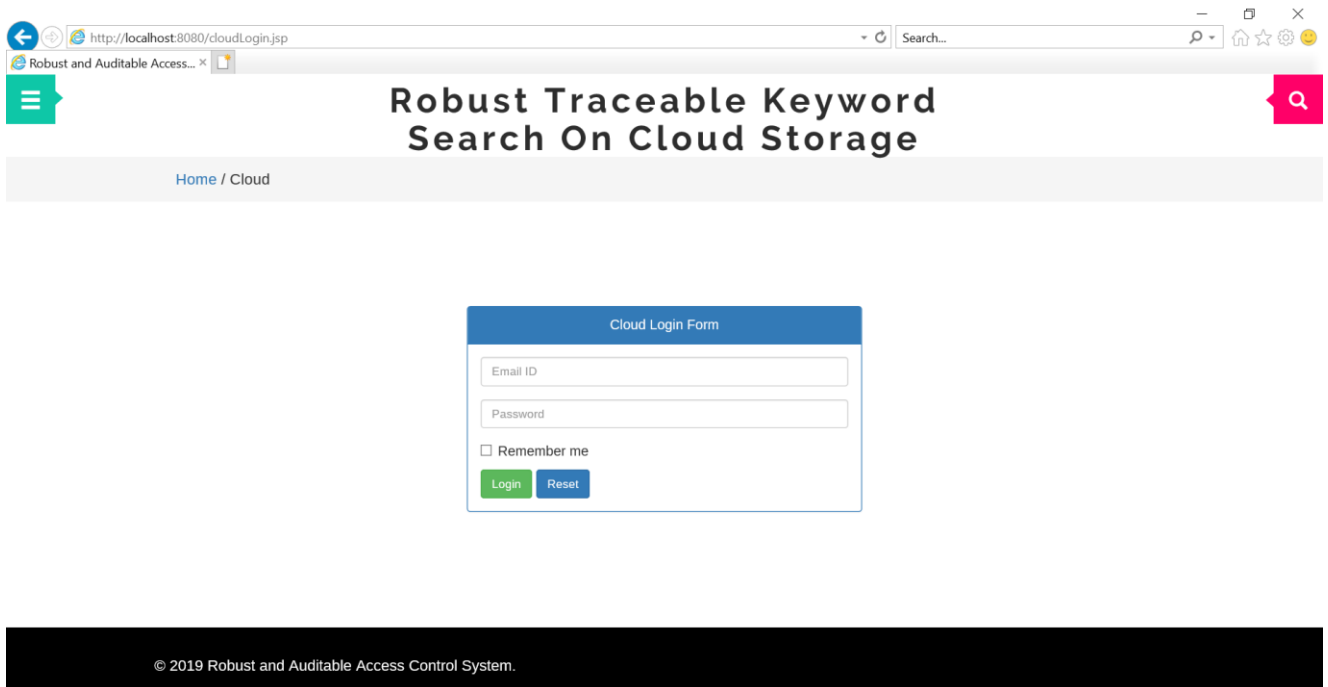


Fig 6: Cloud Login

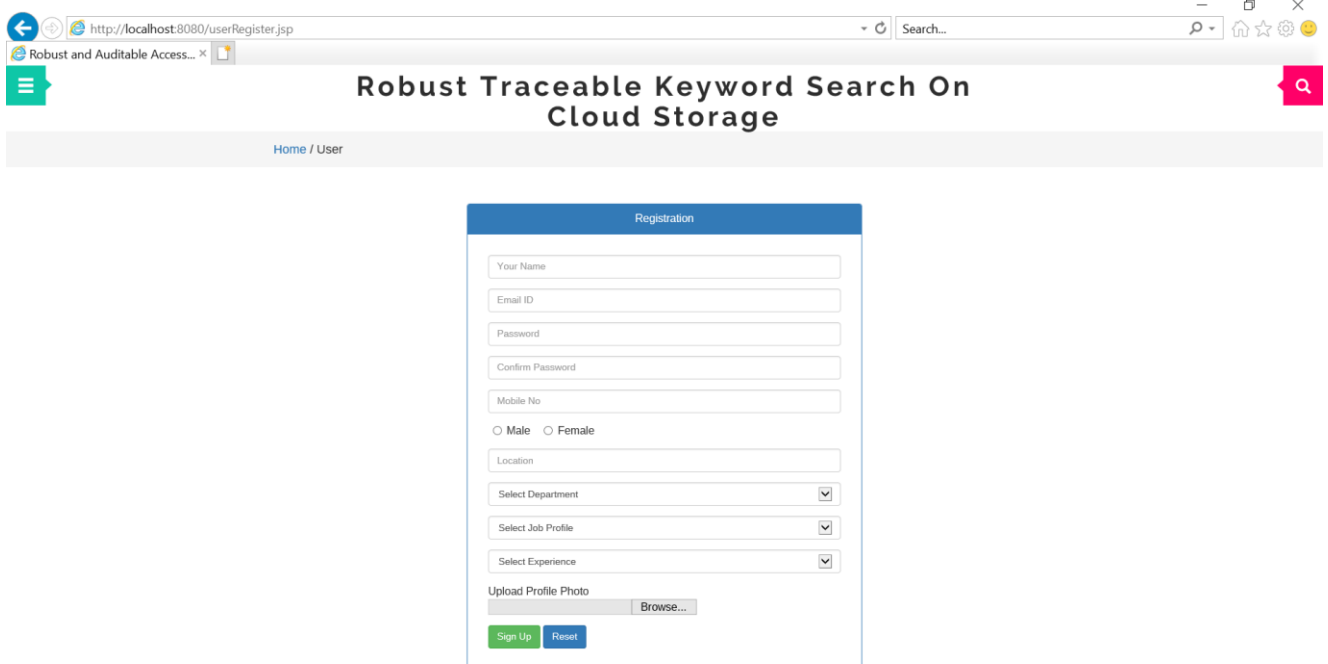


Fig 7: User Registration

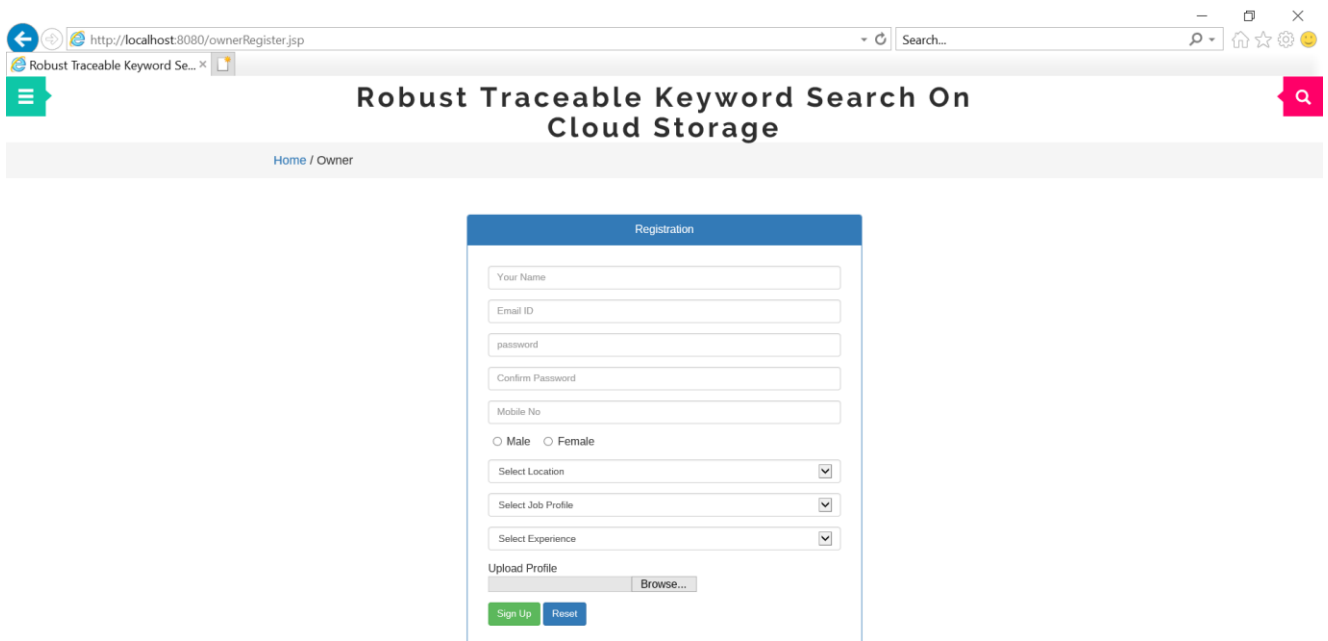


# International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 9, Issue 3, March 2020



Registration

Your Name

Email ID

password

Confirm Password

Mobile No

Male  Female

Select Location

Select Job Profile

Select Experience

Upload Profile

Browse...

Sign Up Reset

Fig 8: Owner Registration

## VII. APPLICATIONS

1. Health Care
2. Military
3. Industrial Area

## VIII. BENEFITS

1. Cost Effective
2. Secure
3. Robust

## XI. CONCLUSION

In this work, we propose a new paradigm of searchable encryption system, and proposed a concrete construction. And to develop a system that will provide secure, trustful and reliable communication. In future we can divide and place data on multiple cloud server to achieve more security.

## REFERENCES

1. J. Kim, W. Susilo, M. Au and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 3, pp. 679-693.
2. X. Mao, J. Lai, Q. Mei, K. Chen and J. Weng, "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption," IEEE Transactions on Dependable and Secure Computing, publish online, DOI: 10.1109/TDSC.2015.2423669.
3. Zhou, D. Huang, and Z. Wang. "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption." IEEE Transactions on Computers, 2015, vol. 64, no.1, pp. 126- 138.



ISSN(Online): 2319-8753  
ISSN (Print): 2347-6710

## International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: [www.ijirset.com](http://www.ijirset.com)

**Vol. 9, Issue 3, March 2020**

4. N. Cao, C. Wang, M. Li, K. Ren, W. Lou. "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, 2014, 25(1): 222- 233.
5. P. Xu, H. Jin, Q. Wu and W. Wang. "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Gussing Attack," IEEE Transactions on Computers, 2013, vol. 62, no. 11, 2266-2277.
6. J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 1343- 1354.