2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

EFFICIENT NORMAL LANGUAGE SEARCH FOR PRIVACY CLOUD STORAGE

YELAGANDULA ROHINI[1] MR. K. RAGHUPATI[2]

[1] PG Student, Department of Computer Science and Engineering, Chaitanya institute of technology and science Kishanpura,Hanamkonda,Warangal -506001, (.TS).india

[2]Assistant Professor, Department of Computer Science and Engineering ,Chaitanya institute of technology and science kishanpura,Hanamkonda,Warangal -506001, (TS).india

[1]yelagandula.rohini@gmail.com, [2]raghu.kanala@gmail.com

Abstract:

Cloud computing provides flexible data management and ubiquitous data access. However, the storage service provided by cloud server is not fully trusted by customers. Searchable encryption could simultaneously provide the functions of confidentiality protection and privacy-preserving data retrieval, which is a vital tool for secure storage. In this paper, we propose an efficient large universe regular language searchable encryption scheme for the cloud, which is privacy-preserving and secure against the off-line keyword guessing attack (KGA). A notable highlight of the proposal over other existing schemes is that it supports the regular language encryption and deterministic finite automata (DFA) based data retrieval. The large universe construction ensures the extendibility of the system, in which the symbol set does not need to be predefined. Multiple users are supported in the system, and the user could generate a DFA token using his own private key without interacting with the key generation center.

I.INTRODUCTION

Much like the popularity of portable personal electronic devices, cloud storage service has been booming over the last decade. Its outstanding advantages, such as considerable storage space, flexible accessibility and convenient data retrieval, strongly catch the attention of Internet users. Accordingly, to date not only individuals but also industries prefer to remotely store their data to cloud servers, such that they can get rid of the burden of local data management and maintenance. This makes cloud storage service share a great piece of market cut in the field of data management even in the ear of big data. Remotely data storage delivers convenience to Internet users and meanwhile, brings security concerns. The fact that users cannot have full physical possession of their data immediately rises up two serious practical questions: how to guarantee theMuch like the popularity of portable personal electronic devices, cloud storage service has been booming over the last decade. Its outstanding advantages, such as considerable storage space, flexible accessibility and convenient data retrieval, strongly catch the attention of Internet users. Accordingly, to date not only individuals but also industries prefer to remotely store their data to cloud servers, such that they can get rid of the burden of local data management and maintenance. This makes cloud storage service share a great piece of market cut in the field of data management even in the ear

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

of big data. Remotely data storage delivers convenience to Internet users and meanwhile, brings security concerns. The fact that users cannot have full physical possession of their data immediately rises up two serious practical questions: how to guarantee the

II.EXISTING SYSTEM:

- Searchable encryption technology not only exerts encryption protection of the data, but also supports efficient search function without undermining the data privacy. The data user generates a token of the content that he wants to search using his private key. Receiving the token, the cloud server searches on the encrypted data without decrypting the cipher text. The most important point is that the server learns nothing about the plaintext of neither the encrypted data nor the searched content during the data retrieval procedure. However, most of the available searchable encryption schemes only support some basic search patterns, such as single keyword search, conjunctive keyword search and Boolean search. Since the cloud computing is a fierce competition industry, it is of vital importance to provide good user experience. It is urgent to design novel searchable encryption schemes with expressive search pattern for cloud storage.
- **Disadvantages:-**
- 1. Encryption searching is a time consuming process.
- 2. Data confidentiality is less.
- 3. Security Is less.

III.PROPOSED SYSTEM:

In this paper, we design a secure data storage system supporting regular language search, which is privacy preserving and proved secure in standard model based on decisional bilinear Diffie-Hellman hardness assumption. A highlight of this proposal is that the regular language search is enabled, which provides much more flexible search pattern compared with other available searchable encryption schemes. In our system, the encryption algorithm takes as input a public key and regular language described string with arbitrary length. Then, the generated ciphertext is outsourced to cloud server. In the data retrieval phase, user defines a deterministic finite automata (DFA) and generates a search token of the DFA using his secret key. The DFA defines a set of transitions, an initial state and an accept state. If and only if the regular language embedded in the ciphertext is acceptable by the DFA of the search token, the file will be regarded as a match file. This test process is executed by the cloud server without knowing any plaintext of the regular language and the DFA.

Advantages:-

1. Security is high.
2. It provides good searching scheme.
3. Data confidentiality is more.

2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

Architecture:

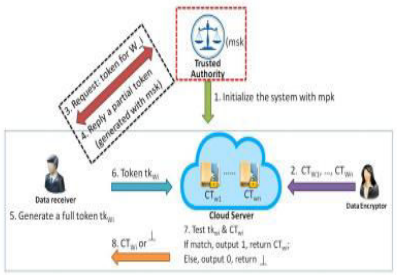

Fig. 1: System Architecture

Algorithm:

AES Encryption: The AES is Advanced Encryption Standard key is a Symmetric encryption key this is key is based on ANSCI code formation. This algorithm block key size is 128bit to 256bit. This cryptography is more secured. In our process the cloud data is secure encrypted at using AES encryption. After the encryption process is completed the AES key is generated.

IV.IMPLEMENATATION:

System Model

In the first module, we develop the System Model to implement our proposed system. Our System model consists of Admin, users, data owners, and Cloud Servers. Admin provides the accessibility to Data-owners. Initially Data-owner needs to register and admin approves the each data owner request. The respective Password and login credentials will be sent to the Email ID of Data owner.

- ✓ In Users sub-module, Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.
- ✓ In data owners sub-module, the proposed scheme should allow new data owners to enter this system without affecting other data owners or data users, i.e., the scheme should support data owner scalability in a plug-and-play model.
- ✓ In Cloud Server sub-module of system model, the owner sends the encrypted data to the cloud server through Admin. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data

Data User Authentication

- ✓ To prevent attackers from pretending to be legal data users performing searches and launching statistical attacks based on the search result, data users must be authenticated before the administration server re-encrypts trapdoors for data users. Traditional authentication methods often follow three steps. First, data requester and data authenticator share a secret key, say, $k0$. Second, the requester encrypts his personally identifiable information $d0$ using $k0$

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

and sends the encrypted data $(d0)k0$ to the authenticator. Third, the authenticator decrypts the received data with $k0$ and authenticates the decrypted data.

- ✓ The key point of a successful authentication is to provide both the dynamically changing secret keys and the historical data of the corresponding data user.

Illegal Search Detection

- ✓ In our scheme, the authentication process is protected by the dynamic secret key and the historical information. We assume that an attacker has successfully eavesdropped the secret key. Then he has to construct the authentication data; if the attacker has not successfully eavesdropped the historical data, e.g., the request counter, the last request time, he cannot construct the correct authentication data. Therefore this illegal action will soon be detected by the administration server.
- ✓ Further, if the attacker has successfully eavesdropped all data of *Uj*, the attacker can correctly construct the authentication data and pretend himself to be *Uj*without being detected by the administration server. However, once the legal data user *Uj*performs his search, since the secret key on the administration server side has changed, there will be contradictory secret keys between the administration server and the legal data user. Therefore, the data user and administration server will soon detect this illegal action.

Search over owner:

- ✓ The proposed scheme should allow keyword search over encrypted files which would be encrypted with different keys for different data owners. It also needs to allow the cloud server to rank the search results among different data owners and return the top-*k* results. The cloud server stores all encrypted files and keywords of different data owners.

The administration server will also store a secret data on the cloud server. Upon receiving a query request, the cloud will search over the data of all these data owners. The cloud processes the search request in two steps. First, the cloud matches the queried keywords from all keywords stored on it, and it gets a candidate file set. Second, the cloud ranks files in the candidate file set and finds the most top-*k* relevant files. Finally, we apply the proposed scheme to encode the relevance scores and obtain the top-*k* search results

V.CONCLUSION:

In this paper, privacy preserving provable data possession scheme (named SEPDP) for untrusted and outsourced storage system is presented. Further, SEPDP is extended to support dynamic data updation by multiple owners and batch auditing. Security of the scheme is analyzed and showed that SEPDP protects data privacy from TPA while infeasible for CSP to forge the response without storing the appropriate blocks. The most appealing features of the proposed

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


scheme is to support all the important features including blockless verification, privacy preserving, batch auditing and data dynamics with lesser computation overhead.

VI.REFERENCES:

RENCES [1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. J. Cryptology, 21(3):350–391, 2008.

[2] J. Baek, R. Safavi-Naini, and W. Susilo.On the integration of public key data encryption and public key encryption with keyword search.In ISC, vol. 4176 of LNCS, pp. 217–232.Springer, 2006.

[3] M. Bellare, A. Boldyreva, and A. O'Neill.Deterministic and efficiently searchable encryption.In CRYPTO, vol. 4622 of LNCS, pp. 535–552.Springer, 2007.

[4] S. Benabbas, R. Gennaro, and Y. Vahlis.Verifiable delegation of computation over large datasets.In CRYPTO, vol. 6841 of LNCS, pp. 111–131.Springer, 2011.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search.In EUROCRYPT, vol. 3027 of LNCS, pp. 506–522.Springer, 2004.

[6] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data.In TCC, vol. 4392 of LNCS, pp. 535–554.Springer, 2007.

[7] C. Bosch, A. Peter, B. Leenders, H. W. Lim, Q. Tang, H. Wang, P. H. ¨ Hartel, and W. Jonker. Distributed searchable symmetric encryption.In PST, pp. 330–337.IEEE, 2014.

[8] C. Bosch, Q. Tang, P. H. Hartel, and W. Jonker.Selective document ¨ retrieval from encrypted database.In ISC, vol. 7483 of LNCS, pp. 224– 241.Springer, 2012.

[9] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy.Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data.In PKC, vol. 5443 of LNCS, pp. 196–214.Springer, 2009.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou. Privacy-preserving multikeyword ranked search over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst., 25(1):222–23