International Journal for Modern Trends in Science and Technology, 9(04): 93-97, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0904015
Available online at: http://www.ijmtst.com/vol9issue04.html

Forward Securepublic Key Encryption with Keyword Search for Outsourced Cloud Storage

K.V.V.Subba Rao, Ramayanapu Manga Devi, Gubbala Kavya Sri, Juthuga Rajeev Vishal, Nakkina Satya Veerabhadra Sekhar, Vasamsetti Venkat

Department of Computer Science and Engineering, Pragati Engineering College (A), Surampalem (East Godavari) A.P,India.

To Cite this Article
K.V.V.Subba Rao, Ramayanapu Manga Devi, Gubbala Kavya Sri, Juthuga Rajeev Vishal, Nakkina Satya Veerabhadra Sekhar and Vasamsetti Venkat. Forward Securepublic Key Encryption with Keyword Search for Outsourced Cloud Storage. International Journal for Modern Trends in Science and Technology 2023, 9(04), pp. 93-97. https://doi.org/10.46501/IJMTST0903015

Article Info
Received: 02 March 2023; Accepted: 25 March 2023; Published: 31 March 2023.

ABSTRACT

Cloud storage has become a primary industry in remote data management service but also attracts security concerns, where the best available approach for preventing data disclosure is encryption. Among them the public key encryption with keyword search (PKSE) is considered to be a promising technique, since clients can efficiently search over encrypted data files. That is, a client first generates a search token when to query data files, the cloud server uses the search token to proceed the query over encrypted data files. However, a serious attack is raised when PKSE meets cloud. Formally speaking, the cloud server can learn the information of a newly added encrypted data file containing the keyword that previously queried by using the search tokens it has received, and can further discover the privacy information. To address this issue, we propose a forward secure public key searchable encryption scheme, in which a cloud server cannot learn any information about a newly added encrypted data file containing the keyword that previously queried. To better understand the design principle, we introduce a framework for constructing forward secure public key searchable encryption schemes based on attribute-based searchable encryption. Finally, the experiments show our scheme is efficient.

1. INTRODUCTION

The invention of cloud computing has greatly eliminated the fussy tasks of managing data files by allowing clients to enjoy on-demand fast computation and massive storage resources at a very low price. Despite the conveniences, in the mechanism, clients lost physical control over their data files, which will lead to the concerns of privacy disclosure. Cryptographic techniques have been seen as a long-established approach to alleviate the concerns , which advocate that data files should be encrypted before outsourcing. As a sequence of encryption, many useful functions such as search over the outsourced data files cannot be efficiently completed. Moreover, efficient search process is indispensable for a modern cloud storage system. Searchable encryption is a cryptographic primitive that allows to execute search operations over encrypted data files, which was introduced by Song et al. [4], and can be realized in either symmetric key setting and public key setting. The former is known as symmetric searchable encryption, although it enjoys high efficiency in search process, it provides a terrible performance in data sharing for its complicated secret key distribution, since clients need to share the secret key which will be used for

decryption when sharing an encrypted data file to others. The latter is known as public key searchable encryption [6], which is more flexible than symmetric searchable encryption at the aspect of data sharing. In public key searchable encryption, a client's public key can be used by others to encrypt a data file shared to the client, and the client can use its secret key to generate search tokens for its queries, the server can use a search token to test whether an encrypted data file matches the query corresponding to the search token while learning nothing about the query. Despite its superiority in data sharing, the public key searchable encryption mechanism suffers from various attacks when being deployed in cloud storage, and may lead to privacy leakage.

2.LITERATURE SURVEY

TITLE: "Privacy-preserving collaborative model learning: The case of word vector training,"

ABSTRACT: Nowadays, machine learning is becoming a new paradigm for mining hidden knowledge in big data. The collection and manipulation of big data not only create considerable values, but also raise serious privacy concerns. To protect the huge amount of potentially sensitive data, a straightforward approach is to encrypt data with specialized cryptographic tools. However, it is challenging to utilize or operate on encrypted data, especially to perform machine learning algorithms. In this paper, we investigate the problem of training high quality word vectors over large-scale encrypted data (from distributed data owners) with the privacy-preserving collaborative neural network learning algorithms. We leverage and also design a suite of arithmetic primitives (e.g., multiplication, fixed-point representation, sigmoid function computation, etc.) on encrypted data, served as components of our construction. We theoretically analyze the security and efficiency of our proposed construction, and conduct extensive experiments on representative real-world datasets to verify its practicality and effectiveness.

TITLE: "SPACF: A secure privacypreserving authentication scheme for VANET with cuckoo filter,"

ABSTRACT: With the ubiquitous advancement in smart medical devices and systems, the potential of Remote Patient Monitoring (RPM) network is evolving in modern healthcare systems. The medical professionals (doctors, nurses, or medical experts) can access vitals and sensitive physiological information about the patients and provide proper treatment to improve the quality of life through the RPM network. However, the wireless nature of communication in the RPM network makes it challenging to design an efficient mechanism for secure communication. Many authentication schemes have been proposed in recent years to ensure the security of the RPM network. Pseudonym, digital signature, and Authenticated Key Exchange (AKE) protocols are used for the Internet of Medical Things (IoMT) to develop secure authorization and privacy-preserving communication. However, traditional authentication protocols face overhead challenges due to maintaining a large set of key-pairs or pseudonyms results on the hospital cloud server. In this research work, we identify this research gap and propose a novel secure and efficient privacy-preserving authentication scheme using cuckoo filters for the RPM network. The use of cuckoo filters in our proposed scheme provides an efficient way for mutual anonymous authentication and a secret shared key establishment process between medical professionals and patients. Moreover, we identify the misbehaving sensor nodes using a correlation-based anomaly detection model to establish secure communication. The security analysis and formal security validation using SPAN and AVISPA tools show the robustness of our proposed scheme against message modification attacks, replay attacks, and man-in-the-middle attacks.

TITLE: "Multi-authority attributebased encryption access control scheme with policy hidden for cloud storage,"

ABSTRACT: Ciphertext policy attribute-based encryption (CP-ABE) is an encryption mechanism that can provide fine-grained access control and adequate cloud storage security for Internet of Things (IoTs). In this field, the original CP-ABE scheme usually has only a single trusted authority, which will become a bottleneck in IoTs. In addition, different users may illegally share their private keys to obtain improper benefits. Besides, the data owners also require the flexibility to change their access policy. In this paper, we construct a multiauthority CP-ABE scheme on prime order groups over a large attribute universe. Our scheme can support white-box traceability along with policy updates to solve the abovementioned three problems and, thus, can fix

the potential requirements of IoTs. More precisely, the proposed scheme supports multiple authority, white box traceability, large attribute domains, access policy updates, and high expressiveness. We prove that our designed scheme is static secure and traceable secure based on the state-of-the-art security models. Moreover, by theoretical comparison, our scheme has better performance than other schemes. Finally, extensive experimental comparisons show that our proposed algorithm can be better than the baseline algorithms.

3. EXISTING SYSTEM

In real world, keywords are usually selected from a low-entropy space, thus, an adversary can launch keyword guessing attack to discover the keyword information of search tokens. Specifically, for each keyword in keyword space, the adversary can encrypt it and then test with the received search token. If the test succeeds, the adversary obtains the keyword information contained in the search token. Some previous works have given efficient methods to against keyword guessing attack .Our scheme can use the generic framework from, which provides a universal transformation from any public key searchable encryption scheme to a keyword guessing attack secure public key searchable encryption scheme, the core idea is to set up an aided keyword server. For the space limitation, in this paper, we omit the transformation for our scheme, interested readers can refer to for more details.

3.2 PROPOSEDSYSTEM

To achieve the forward security for public key searchable encryption, our intuition is to bind a search token (or an encrypted data file) and its generation time together. when processing search, the algorithm first checks whether the encrypted data file is generated before the search token. However, as well-known, it is difficult to execute number comparison operations over encrypted data.

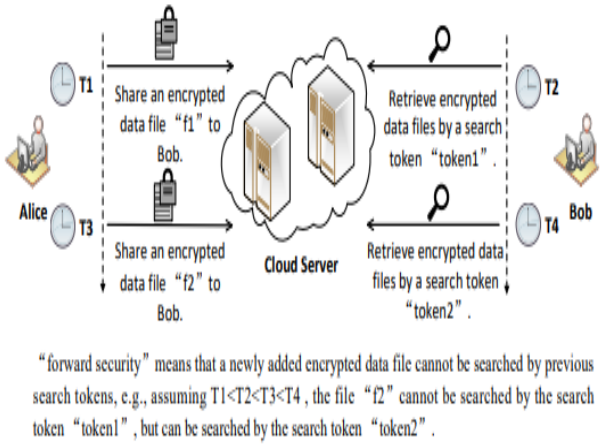
To overcome this, we resort to the 0-Encoding and 1-Encoding approach in , which can transform the numerical comparison problem into a problem of distinguishing whether two sets have same elements. To deal with the latter, let us have an example of comparing ”10” in a search token and ”5” in an encrypted data file, as shown in Figure 3, we can encode ”5” into a set {011, 1} by the 0-Encoding algorithm, and then generate an OR gate over the set, the last is to embed the OR gate into the encrypted data file. For the search token, we can encode ”10” into a set {101, 1} by

the 1-Encoding algorithm, and then embed the set into the search token. Thus, an encrypted data file can be searched by a search token if the set embedded in the search token can match the OR gate embedded in the encrypted data file.

4. SYSTEM ARCHITECTURE

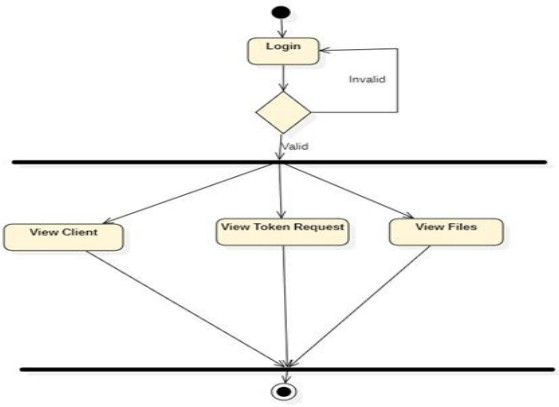
BelowdiagramdepictsthewholesystemarchitectureofForward secure public key encryption.

.



ActivityDiagram

A graphical representations of work process of stepwise exercises and activities with supportfor decision, emphasis and simultaneousness, used to depict the business and operational well-orderedstreamof parts ina framework furthermoredemonstratesthegeneral streamof control



5.SYSTEM IMPLEMENTATION

There are 2 modules:

1.User

2.Admin

User:-

Admin:-

1.Register 1. Login

2.Login 2. View Client

3.UploadFiles 3.View Token Request

4.Token Request 4.View Files

5.Search Files

6.Action

7.Request Files

8.My profile

9.Logout

Types of Software Testing: Different Testing Types with Details

We, as testers, are aware of the various types of Software Testing like Functional Testing, Non-Functional Testing, Automation Testing, Agile Testing, and their sub-types, etc.

Each type of testing has its own features, advantages, and disadvantages as well. However, in this tutorial, we have covered mostly each and every type of software testing which we usually use in our day-to-day testing life.

6.RESULTS

Fig7.1 This fig showsthe home page of our project

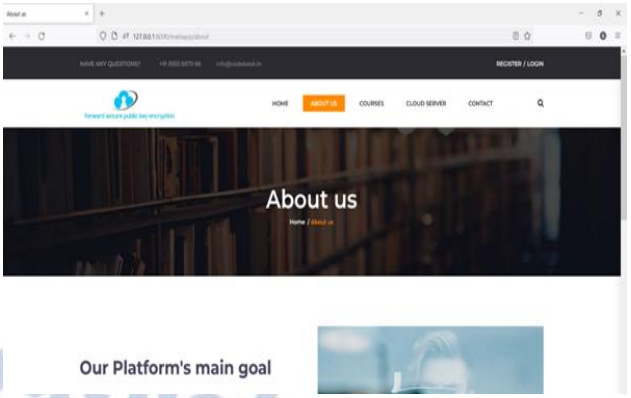


Fig 7.2Fig7.2This figshowsthe About Page

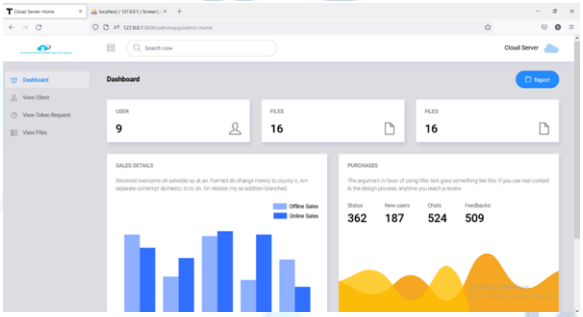
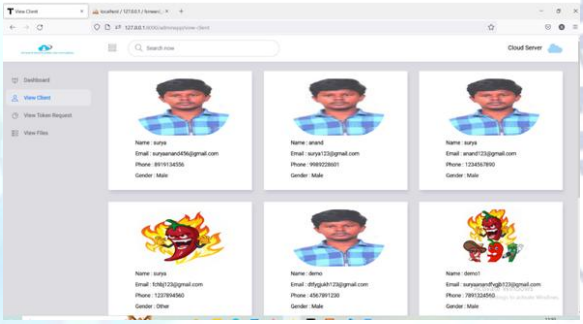
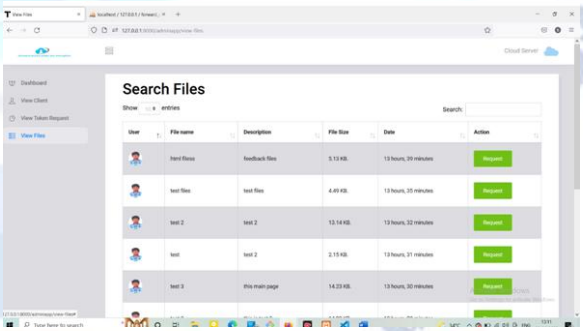


Fig 7.3 the figure shows Admin Page





7. CONCLUSION & FUTURE WORK

In this paper, we study the forward security for public key searchable encryption, which means a new added encrypted data file cannot be searched by the search tokens generated before the encrypted data file. This security is urgently required for the public key searchable encryption schemes deployed in cloud storage, and can greatly reduce the privacy information leaked to a cloud server.

As a solution, we

(a) Comparison of Encryption

(b) Comparison of Token Generation

(c) Comparision of Search Fig. Comparison with Boneh et al. in terms of encryption, token generation and search. propose a concrete scheme based on the 0-Encoding and 1- Encoding approach and give its security proof, further, we also show how to obtain a forward secure public key searchable encryption scheme from an attribute-based searchable encryption scheme by introducing a generic framework. Finally, we design experiments to illustrate the practicality of our proposed scheme in terms of encryption, token generation and search.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Q. Wang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, and X. Huang, "Privacy-preserving collaborative model learning: The case of word vector training," IEEE Trans. Knowl. Data Eng, vol. 30, no. 12, pp. 2381–2393, 2018.

[2] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacypreserving authentication scheme for VANET with cuckoo filter," IEEE Trans. Vehicular Technology, vol. 66, no. 11, pp. 10 283–10 295, 2017.

[3] H. Zhong, W. Zhu, Y. Xu, and J. Cui, "Multi-authority attributebased encryption access control scheme with policy hidden for cloud storage," Soft Comput., vol. 22, no. 1, pp. 243–251, 2018.

[4] D. X. Song, D. A. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.

[5] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in ACM Conference on Computer and Communications Security, 2006, pp. 79–88.

[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in International Conference on the Theory and Applications of Cryptographic Techniques, 2004, pp. 506–522.

[7] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in USENIX Security Symposium, 2016, pp. 707–720.

[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryptionrevisited:Consistency properties, relation to anonymous ibe, and extensions," in Annual International Cryptology Conference, 2005, pp. 205–222.

[9] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-preserving encryption for numeric data," in ACM Conference on Management of Data, 2004, pp. 563–574.

[10] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Orderpreserving symmetric encryption," in International Conference on the Theory and Applications of Cryptographic Techniques, 2009, pp. 224–241.