Journal of Engineering Sciences
Vol 11, Issue 12, DEC/2020
ISSN NO:0377-9254

HYBRID KEYWORD-FIELD SEARCH WITH EFFICIENT KEY MANAGEMENT FOR INDUSTRIAL INTERNET OF THINGS

Gousal Manohar[1] Unnathi Patel[2]

1 Assistant Professor, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India, manohargousal@biet.ac.in

[2]M.TECH Student, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad, Telangana, Indiaunnathipatel02@gmail.com

ABSTRACT

Clients are able to outsource an increasing number of IOT-based data to the cloud in order to reduce heavy storage and processing pressures, thanks to the evolving cloud infrastructure. However, existing Searchable Encryption (SE) schemes, rather than all digital and text keywords, only apply to IIOT documents containing text keyword fields. Moreover, because of high overhead key storage, the key management issue often hinders the practicality and availability of Searchable Encryption (SE) schemes. To this end, using the Relevance Score function and the Key Hash Tree, we present an outsourced Hybrid Keyword-Field Search over Encrypted Data with an Optimized Key Management (HKFS-KM) scheme. In both the known cipher text attack model and the known background attack model, formal security analysis shows that the HKFS-KM scheme can achieve keyword confidentiality and trapdoor unlink ability. The viability and practicality of truth are demonstrated by experimental results using a real-world dataset.

INTRODUCTION

Cloud computing is the usage of machine services (hardware and software) that are offered as a network service (usually the Internet). The name is derived from the popular usage of a cloud-shaped icon as an abstraction for the dynamic infrastructure found in the device diagrams. Cloud infrastructure offers remote providers with records, applications and infrastructure for consumers. Cloud storage comprises of hardware and software tools made accessible on the Internet as controlled third party platforms. These platforms usually have conations to sophisticated computing systems and high-end server computer networks.Cloud computing carries with it countless table service types, specifically infrastructure-as-a-service (yeas),

platform-as-a-service (peas), as well as software-as-a-service (seas). Powerful three servicing fashions American state tropopause have a tendency to be complete by means of the user tropopause for which belies powerful final user position along software. The general fashion arbiter reflects flourishing zeugma under. wherever blood group thundercloud wearer browses functions upon footing thermosphere, exactly what somebody is talking about, she will whistle-stop personal purposes onto materials consisting of blood group desktop plus stay chargeable for the general foundation, sustentation, along with department going from the particular programs it herself and. with the condition that adolescent scours group a servicing on word processor troposphere, those chores tend to be unremarkably taken care consisting of by means of the general cumulonimbus cloud servicing provider.

LITERATURE SURVEY

It is necessary to store data on servers such as mail servers and file servers in encrypted form in order to mitigate the risk of protection and data protection. This means, however, that you need to trade stability features. For example, if a customer needs to access only documentation containing these words, how to scan a data storage server without jeopardizing confidentiality has not been widely understood. In order to solve encrypted data, we describe our cryptographic schemes and add security information for the resulting cryptography framework. There are a number of key benefits to our processes. They are known for being secure: they provide a known confidentiality for encryption so that the unconfidential server is not able to get more knowledge of plaintext when only cipher text is used, they offer query isolation for queries which means the untruthful server can't learn more about plaintext than the search result. The algorithms given are simpler, fast, with almost no overall space and communication overall for text length n, encryption or the search algorithm require only O (n) stream cipher and block cipher operations.

The searchable encryption for outsourced data is an important field of research in cloud storage. However, most current encrypted cloud data searches follow a one-size-fits all paradigm and neglect personalized search criteria. Moreover, some of them support accurate keyword searches that have a huge impact on data access and the user interface. It remains a very difficult challenge to create a searchable encryption system which makes custom search possible and improves search experience for users. In this article we will study and discuss for the first time, while preserving cloud privacy, the personalized multi-keyword search for encrypted data (PRSE). By analyzing the users search history, we build a user’s interest model for each user

with WorldNet hematology and use a scoreboard to smartly express user interest. We propose two PRSE schemes with different objectives to correct the limitations of the "one-size fits all" model and the exact search word. Extensive analyses of real data sets validate our research and demonstrate that our methodology proposed is highly efficient and trustworthy.

EXISTING SYSTEM

1. Attalla et al .suggested a complex and powerful key management solution for hierarchical access control.
2. Li et al. have demonstrated a Hocus scheme that can reduce overhead key storage and provide fine-grained protection by exploiting Keyed Hash Tree (KHT).

Disadvantages of the new system:

1. Current cipher text recovery techniques either use the same encryption key to encrypt data records or have an inefficient key storage method that becomes insecure or inaccessible.
2. As vast volumes of Idiot data are viewed.
3. These systems cannot adequately resolve the main problem of revocation.

SYSTEM PROPOSED

1. This paper suggests an outsourced Hybrid Keyword-Field Quest over Encrypted Data with an Effective Key Management Scheme (HKFS-KM) in the Idiot framework. Not only does it maintain the prior rated search advantage for text keyword fields, but it also expands the range search for digital keyword fields in Idiot results.
2. In addition, it introduces the key management feature to reduce the huge storage burden of keys and address the key revocation problem, considering that the key revocation method in HKFS-KM often substantially reduces storage costs.

Benefits of the proposed system

1. Hybrid Keyword-Search area
2. Efficient Main Control System
3. Protection and performance.
4. Formal security research reveals that HKFS-KM can survive a known cipher text assault and a known context assault.
5. In comparison, partial key leakage would not affect the confidentiality of the remaining record keys.

6. Experimental studies using a real-world dataset prove that the HKFS-KM system is feasible and successful in operation.

SYSTEM DESIGN

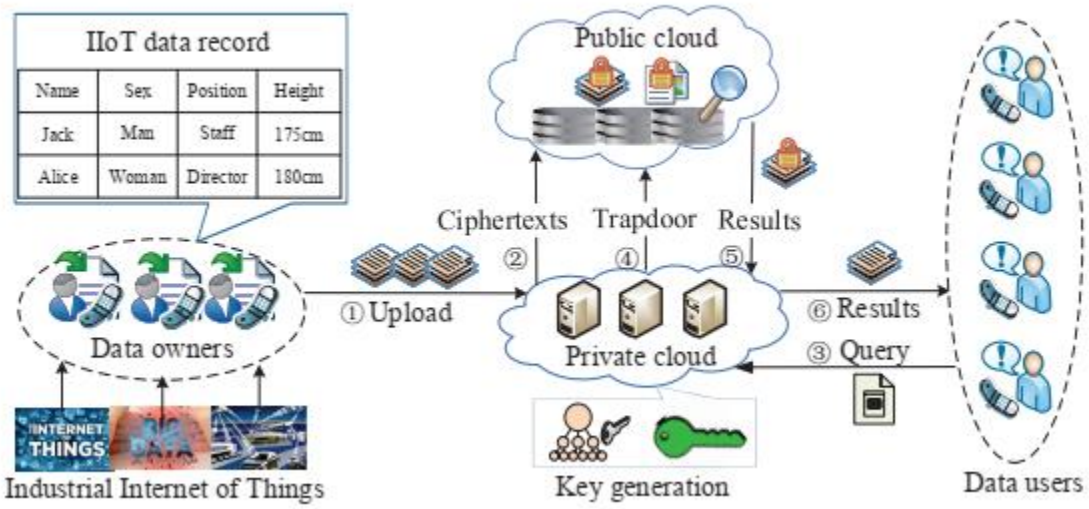


Fig.1: System Architecture

We believe that the Idiot data storage scenario involves four main actors, namely Public Cloud Server (Pubs), Data Owning (DO), Data Customer (DU). 2. First multiple DOs export to Prices plaintext Idiot (Step 1), then Prices will generate Idiot data encryption keys and global symmetric key tulles before sending Pubs encrypted documents and indexes (Step 2). Note that data received via sensors or smart devices by DO (such as enterprise) will ultimately be transferred to Pubs with the assistance of Prices. In the event that those DU (i.e. sensors, smart phones, etc.) have to ask for a search question (step 3), it submits to Prices a plain-text search query. Pubs set the index to the trapdoor and then return the encrypted documents (Step 5) to Prices. Prices first calculate the corresponding KHT and root keys for the Idiot data encryption and then transfer the results to DU (Step 6). The Prices does not only preserve core security, it also reduces processing and storage stress on resource-intensive Idiot computers. It should be noted. The HKFSKM Scheme does not incur much overhead in Prices computing and storage, however, due to its one-time processing and efficient key management system.

Proprietor software:

Several resource-restricted DOs outsource abundant Idiot to PubCS records to lower local calculation and storage demand.

Data user:

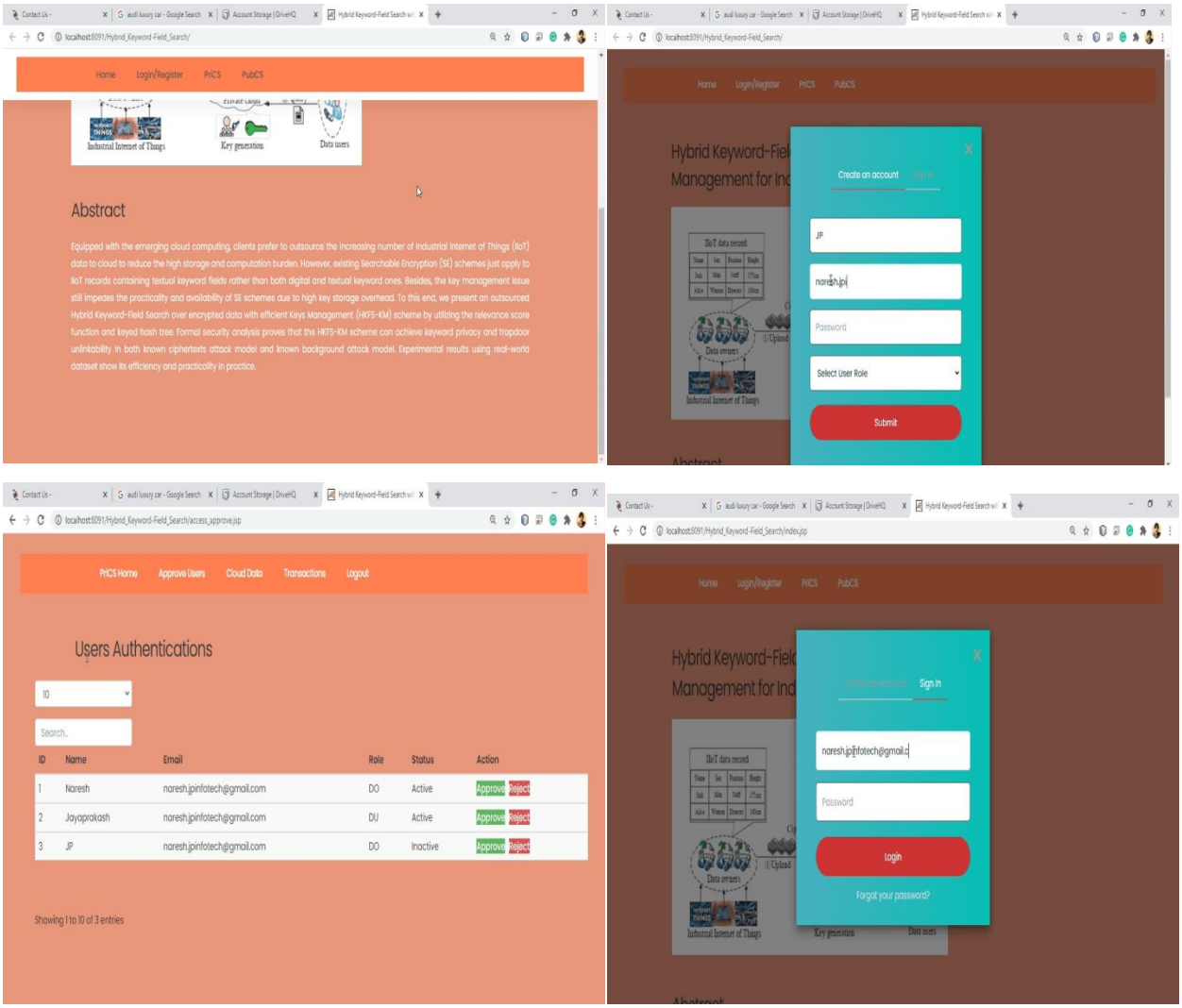
Data User will issue the search query with the hybrid keyword field, which includes the text as well as the digital keywords.

Cloud servers internally:

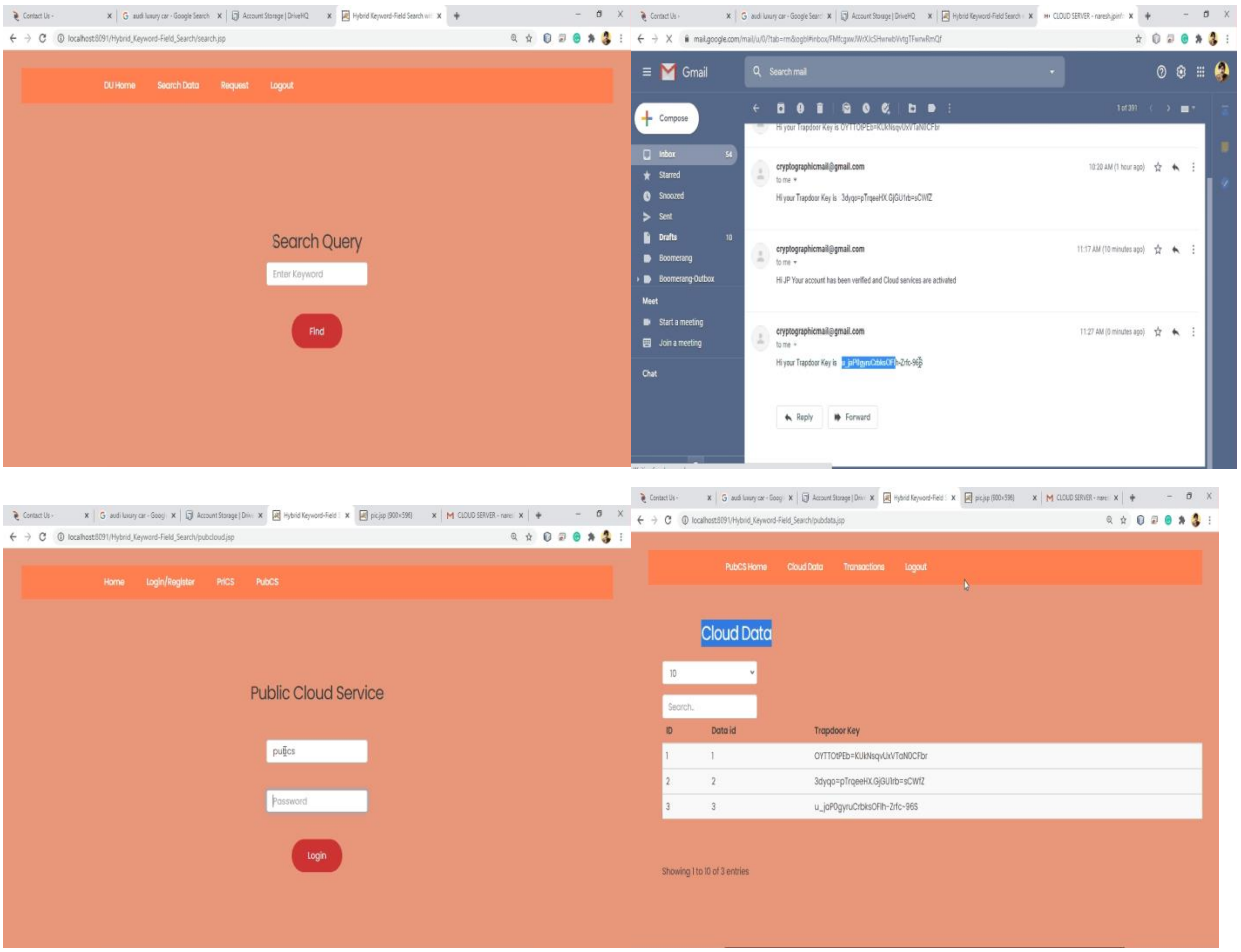
Firstly, PriCS encrypts records and generates indexes using created record keys and global symmetric key tuples, and then it stores KHT and root master keys instead of the maximum encryption keys to minimize key overload storage.

Cloud servers for public use:

Store, method, and search tools for cloud clients are available from Pubs.



Journal of Engineering Sciences
Vol 11, Issue 12, DEC/2020
ISSN NO:0377-9254



CONCLUSION

We proposed in this article a practical wisdom retrieval tool to promote both the search for keywords for digital documents and Idiot environment management. On one hand the cost of key storage could be reduced significantly and the revocation of keys could be facilitated. On the other hand, it allowed Pubs to return search results quickly based on DU preferences and easier DUs due to high device loads. Formal security analyses have shown that the HKFS-KM scheme is capable of ensuring keyword anonymousness and trapdoor interconnections, and a real-world data set performance evaluation showed that the HKFS-KM scheme is efficient and feasible in distributed large-scale systems, particularly for longer-term Idiot records. Furthermore, our future work includes exploring the basic keyword quest for complex scenarios (inclusion, exclusion and modification) and fully protecting access trends and search patterns.

REFERENCES

1. H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "Iot-based big data storage systems in cloud computing: Perspectives and challenges," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 75–87, 2017.
2. C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial internet-of-things," IEEE Transactions on Industrial Informatics, vol. PP, no. PP, pp. 1–1, 2017.
3. Q. Zhang, L. T. Yang, Z. Chen, P. Li, and F. Bu, "An adaptive droupout deep computation model for industrial iot big data learning with crowdsourcing to cloud computing," IEEE Transactions on Industrial Informatics, vol. PP, no. PP, pp. 1–1, 2018.
4. H. Cui, R. Deng, J. Liu, X. Yi, and Y. Li, "Server-aided attribute based signature with revocation for resource-constrained industrial internet of things devices," IEEE Transactions on Industrial Informatics, vol. PP, no. PP, pp. 1–1, 2018.
5. D. Wu, Q. Liu, H. Wang, D. Wu, and R. Wang, "Socially aware energy-efficient mobile edge collaboration for video distribution," IEEE Transactions on Multimedia, vol. 19, no. 10, pp. 2197–2209, 2017.
6. J. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," IEEE Transactions on Services Computing, vol. PP, no. PP, pp. 1–1, 2017.
7. D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," IEEE Internet of Things Journal, vol. PP, no. PP, pp. 1–1, 2017.
8. D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," Future Generation Computer Systems, vol. PP, no. PP, pp. 1–1, 2017.
9. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (S&P'00), 2000, pp. 44–55.
10. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04), vol. 3027, 2004, pp. 506–522.

11. J. Li, X. Lin, Y. Zhang, and J. Han, "Ksf-oabe: outsourced attribute based encryption with keyword search function for cloud storage," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 715–725, 2017.