www.ijrream.in Impact Factor: 2.9463

INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING AND MANAGEMENT (IJRREM)

Efficient Key Management for Industrial Internet of Things

M. Manjurekha[1], Bhuvaneshwari. C[2], Shruthi. S[3], Aruna. S. P [4], Banu Priya. T [5]

[1]Assistant Professor & [2,3,4]UG Scholars – Dept. of Information Technology

Er. Perumal Manimekalai College of Engineering

ABSTRACT:

Equipped with the emerging cloud computing, clients prefer to outsource the increasing number of Industrial Internet of Things (IIoT) data to cloud to reduce the high storage and computation burden. However, existing Searchable Encryption (SE) schemes just apply to IIoT records containing textual keyword fields rather than both digital and textual keyword ones. Besides, the key management issue still impedes the practicality and availability of SE schemes due to high key storage overhead. To this end, we present an outsourced Hybrid Keyword-Field Search over encrypted data with efficient Keys Management (HKFS-KM) scheme by utilizing the relevance score function and keyed hash tree. Formal security analysis proves that the HKFS-KM scheme can achieve keyword privacy and trapdoor unlinkability in both known ciphertexts attack model and known background attack model. Experimental results using real-world dataset show its efficiency and practicality in practice.

Keywords *- Searchable encryption, textual keyword, digital keyword, multi-keyword search, keyed hash tree.*

I. INTRODUCTION

The emerging Internet of Things (IoT) technology, which is considered as a popular approach to extend the connections of internet to all kinds of smart devices, has been widely applied in industrial sectors (e.g. industrial process monitoring and management, machine health monitoring and fault diagnosis), thereby forming the Industrial IoT (IIoT). In a typical IIoT system, large amounts of data about industrial manufacturing (also called IIoT data) are first collected by the mobile devices or sensor nodes, then out sourced to cloud via Internet or

sensor network. Although the cloud can automatically control the industrial manufacturing processes and relieve the high storage and computation burden on resource- constrained IIoT devices locally, the privacy-sensitive IIoT data, (e.g. text, image, video) still suffer from privacy violations under various attacks. Although the encryption- before-outsourcing mechanism can guarantee the IIoT data privacy, it makes the data utilization over encrypted IIoT data extremely difficult. To solve the conflict between data confidentiality and searchability, exploring the emerging searchable encryption (SE) technology which enables data users to securely search and selectively retrieve records of interest over encrypted data according to user-specified keywords, is prime of importance in practice. Currently, a mass of SE schemes enriched with different functionalities have been proposed, such as single keyword search, multi-keyword search and fine- grained keyword search. Nevertheless, the single keyword search is still insufficient in practice as massive cloud clients tend to provide multiple keywords in a single search query.

Besides, aforementioned schemes separately focus on textual keyword fields (e.g. "Brand", "Model", "Color") or digital ones (e.g. "Length", "Width", "Height") of IIoT data. For example, Cao et al. First proposed the textual multi-keyword ranked search by utilizing inner product similarity, Wang et al. presented a new SE scheme supporting nearest neighbor digital keyword search over encrypted cloud data. However, existing multi-keyword search schemes still face some significant limitations, which make these schemes far from practice. Take the IIoT data records as an example, the data user (such as the sensors or smartphones in IIoT environment) may issue a search query "Brand = Jeep AND Length ∈ [4.1m,6.2m]", "Brand = BMW AND Length = 5.1m" in TABLE 1, while existing SE schemes cannot deal with such requests. Thus, how to develop a practical multi-keyword search scheme support-ing both textual and digital keyword fields is still an open issue. However, simply combining two kinds of keyword fields with two different key sets inevitably incurs huge computation burden on resource-limited IIoT devices. To further gain a broad range of applications, the practical SE schemes should support ranked search according to the relevance scores of textual keywords and range search

of digital keywords in records, without wasting the IIoT devices' bandwidth and computation resources..

Table 1 Example for IIoT data record

Brand	Model	Color	Length	Width	Height
BMW	Small	Red	5.1m	1.62m	1.45m
Buick	Compact	Blue	4.8m	1.68m	1.46m
Audi	Luxury	Silvery	4.6m	1.71m	1.58m
Ferrari	Compact	Purple	5.2m	1.76m	1.52m
Ford	Small	Black	4.4m	1.69m	1.48m
Jeep	Luxury	Yellow	4.9m	1.72m	1.50m

2. EXISTING SYSTEMS

Existing approaches on cipher texts retrieval either use the same encryption key to encrypt the data records or provide inefficient key storage mechanism, which become unsafe or unavailable when large amounts of IIoT data records are presented. For example, IIoT data in different sections (i.e., finance department, manufacturing department, etc.) are encrypted with various encryption keys to prevent unauthorized accesses, thereby bringing in high record keys management overhead. The defects of existing SE schemes are demonstrated in Fig. 1. When considering the large-scale distributed systems, the number of keys increases with the number of enterprise apartments, which are considered as the data owners in IIoT system. Besides, data users (i.e., management, staff, etc.) have different ac- cess permissions via the IIoT devices (e.g. mobile terminal- s, sensor nodes). Unfortunately, current key management schemes either have high key storage costs or are coarse grained. To address these problems, Atallah et al. [23] pro- posed a dynamic and efficient key management solution for hierarchical access control, Li et al. [24] demonstrated a Horcus scheme which can reduce key storage overhead and provide fine-grained security by leveraging Keyed Hash Tree (KHT), but these schemes do not effectively tackle the key revocation issue.

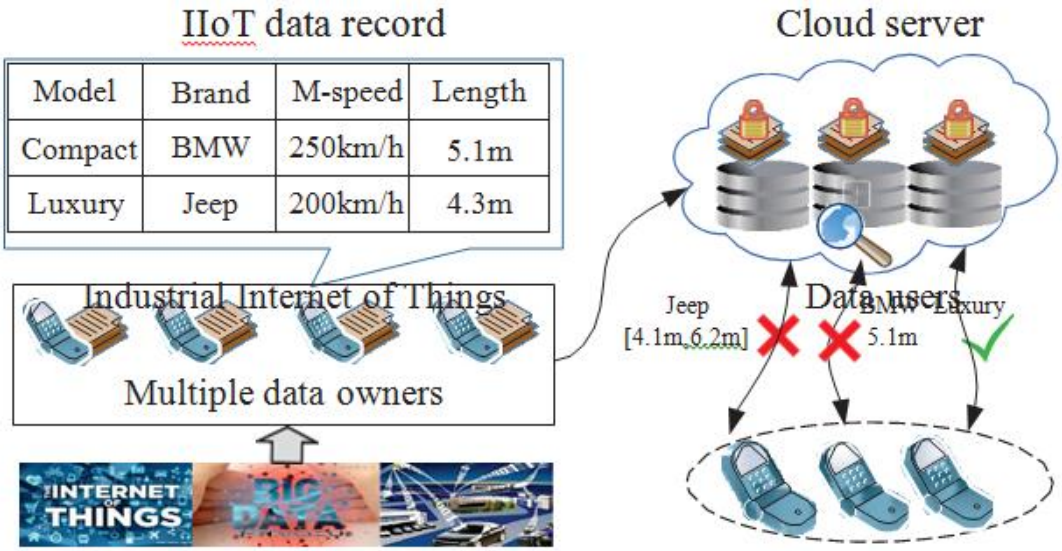

Figure 1: Existing defects in current SE Schemes

- **Hybrid Keyword - Field Search:** First, HKFS-KM enables data users to quickly locate the most relevant records by combining the vector space model and widely-used Term Frequency Inverse Document Frequency (TF IDF) for the textual keyword fields. Second, it further narrows down the search scope by specifying the range for each digital keyword field.
- **Efficient Key Management Mechanism:** HKFS-KM can greatly reduce the key storage overhead by just storing a root key in modified KHT rather than the whole key sets. Besides, it can effectively support key revocation without updating the original KHT.
- **Security and Efficiency:** Formal security analysis proves that HKFS-KM can resist the known cipher- texts attack and known background attack. Besides, partial key leakages do not compromise the security of remaining record keys. Experimental results us- ing real-world dataset demonstrate that HKFS-KM scheme is feasible and efficient in practice.

3. RELATED WORK

To achieve data availability in cloud computing or IIoT environment, many data sharing schemes focusing on data privacy protection have been proposed. Since Song et al. [9] achieved the search- ing functionality without any loss of data confidentiality, more efficient and secure searches over encrypted cloud data have motivated a series of studies focusing on system security and efficiency in different environments (e.g. cloud computing, IoT, IIoT). For example, He et al. proposed a certificate less public key authenticated encryption with keyword search scheme to achieve privacy-preserving data retrieval in IIoT environment; Zhou et al. [26] presented a novel file-centric multi-key aggregate keyword searchable encryption system for the IIoT data in the file-centric frame- work; Yang et al. proposed a lightweight break-glass access control system in healthcare IoT environment. To meet more practical search demands, available SE schemes should support multi-keyword search since single keyword search is far from satisfactory by returning many irrelevant records. Besides, data users prefer to quickly locate the relevant results in a relevance-based order. Thus, Li et al. [31] presented a more secure ranked search scheme by leveraging blind storage. However, the types of keyword fields in practical scenarios may be not only textual but also digital.

4. PROBLEM FORMULATION

4.1 System Model

In this paper we consider an IIoT data storage scenario involving four main entities, namely Public Cloud Server (PubCS), Data Owner (DO), Data User (DU) and Private Cloud Server (PriCS), as illustrated in Fig. 2. Multiple DOs first outsource plaintext IIoT records to PriCS (Step 1), then PriCS generates the IIoT data encryption keys and global symmetric key tuple before sending the encrypted records and indexes to PubCS (Step 2). Notice that the IIoT data collected by DO (such as enterprise) via sensors or smart devices are finally sent to PubCS with the help of PriCS. When a certain DU (i.e., sensors, smartphones, etc.) wants to issue a search query (Step 3), he submits a plaintext search query to PriCS, then PriCS returns the search token (or trap- door) to PubCS (Step 4). PubCS matches the trapdoor with

the indexes, and then returns the relevant encrypted records to PriCS (Step 5). PriCS first computes the corresponding IIoT data encryption keys according to KHT and root key, then sends the plaintext results to DU (Step 6). It is worth noticing that the PriCS not only guarantees the key security but also eliminates the computation and storage burden on resource-constrained IIoT devices. However, the HKFS- KM scheme does not incur much computation and storage overhead on PriCS due to one-time operation and efficient key management mechanism. The specific role of each entity is shown as follows:

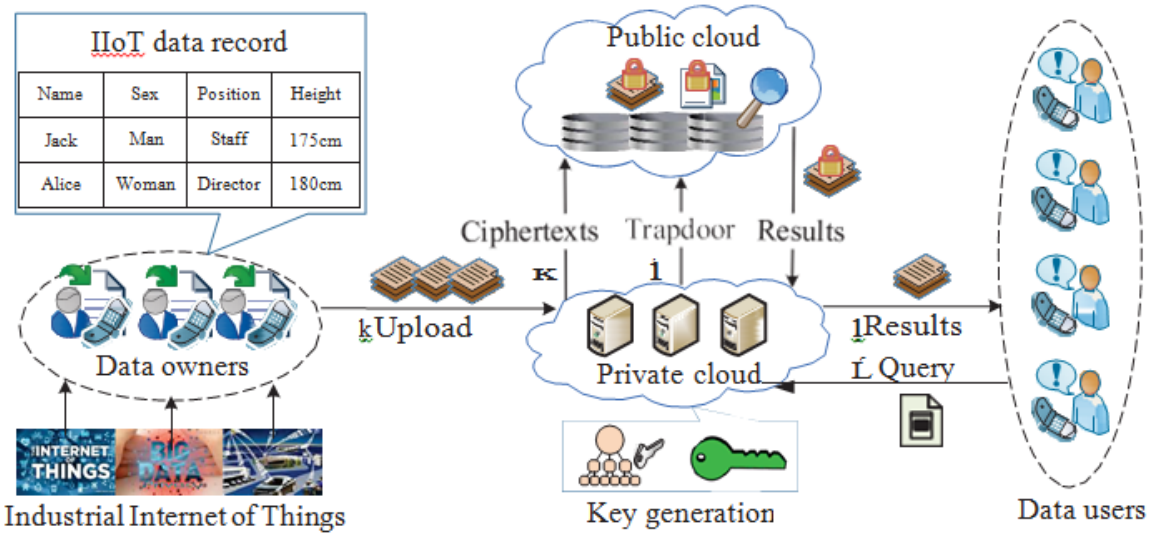

Figure: 2 System model of HKFS-KM scheme

- **Data Owner:** Multiple resource-limited DOs out- source abundant IIoT records to PubCS to alleviate the local computation and storage burden.
- **Data User:** DU can issue hybrid keyword-field search query including both textual and digital keywords, but search query encryption is conducted by PriCS.
- **Private Cloud Server:** PriCS first encrypts records and builds indexes by utilizing the generated record keys and global symmetric key tuple, then it just stores KHT and root master key rather than the whole record encryption keys to reduce key storage overhead, finally it computes the record decryption keys to obtain plaintext results.

- **Public Cloud Server:** PubCS can provide storage, computation and search services for cloud clients.

4.2 Threat Model

For the threat model, PubCS is assumed to be an honest- but-curious entity which honestly executes the designed protocols but may curiously deduce some sensitive infor- mation about records, indexes or trapdoors. Based on what information PubCS has gained, we mainly consider the following two threat models [18], namely known ciphertexts attack model and known background attack model. Note that the PriCS and authorized DUs are considered to be fully trusted.

- **Known cipher text attack model:** In this model, we assume that PubCS only knows the encrypted records and indexes CT = (C, I), which are out-sourced by the PriCS.
- **Known background attack model:** Compared with above known ciphertext model, PubCS is supposed to learn much more information in this stronger model. When gaining the correlation relationship of multiple trapdoors (or search tokens) and the dataset related statistical information, the PubCS may de- duce the potential keywords in the search queries.

5. PROPOSED HKFS-KM SCHEME

In this section, we first give some notation descriptions in TABLE 3, then demonstrate the concrete construction of our HKFS-KM scheme involving with six main phases, namely initialization, key management, ciphertexts generation, trapdoor generation, cipher texts search and cipher- texts decryption. In the system initialization phase, the PriCS outputs the global symmetric SK and root key α of KHT. In order to reduce the key storage overhead for vast amounts of records, in the key management phase the PriCS constructs an efficient KHT by using α and distributes a unique encryption key for each record. The DO (e.g. mobile terminals, sensor nodes) first collects large amounts of IIoT records from IIoT scenarios, then outsources them to PriCS. To guarantee record privacy and improve search efficiency, in the ciphertexts generation phase the PriCS first encrypts each record with

distributed record encryption key in KHT, then builds index for each record according to the hybrid keyword fields and SK, finally uploads the record ciphertexts and indexes to PubCS. To achieve search queries over encrypted IIoT records, a DU (e.g. mobile devices or sensor nodes) must submit a plaintext search query to PriCS. Aiming to protect search query privacy, the PriCS first encrypts the plaintext search query as trapdoor in trapdoor generation phase, then sends the trapdoor to PubCS. To retrieve the encrypted IIoT data, the PubCS matches the trapdoor with the indexes and then returns the corresponding results to PriCS in cipher texts search phase. To decrypt the search results in ciphertexts decryption phase, the PriCS first computes the related record decryption keys according to the KHT, then returns the plaintext search results to DU.

6. CONCLUSION

In this paper, we proposed a practical information re- trieval system to support both digital and textual keywords search as well as key management in IIoT environment. On the one hand, it could greatly reduce key storage costs and efficiently support keys revocation. On the other hand, it allowed PubCS to quickly return the top-k search results according to DUs' preferences and eased DUs from the high computation burden. Formal security analysis proved that HKFS-KM scheme could guarantee keyword privacy and trapdoor unlinkability, and the actual performance evalua- tion using real-world dataset demonstrated that HKFS-KM scheme was efficient and feasible in large-scale distributed systems, especially for IIoT records with longer length. In addition, exploring expressive keyword search for dynamic scenarios (record insertion, deletion and modification) and fully guaranteeing the privacy of access pattern and search pattern are parts of our future work.

REFERENCES:

1. H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "Iot-based big data s- torage 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 industri- al 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 Trans- actions 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 indus- trial 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. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for out- sourced decryption in attribute based encryption," IEEE Transac- tions 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.