Design of Improved Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things

P B V Rajarao¹ Dr N Srinivasu²

¹Assocate Professor, Dept of CSE BVCE, Odalarevu, Andhrapradesh, India
²Professor, K L University, Greenfields, Vaddeswaram, Andhrapradesh, India

Abstract- Cloud computing in addition to Internet of Things (IoT), two very different technologies, are actually both currently part of the life of ours. Their advantage of and massive adoption are anticipated to increase more, making them crucial parts of the Future Internet. A novel paradigm where IoT and Cloud are actually merged together is foreseen as disruptive as well as an enabler of a lot of application scenario. This paper proposes an effective data sharing system which allows for smart products to share secure data with other people at the edge of cloud assisted Internet of Things (IoT). We likewise suggest a protected searching scheme to data within own/shared data on storage space were desired by search.

Index Terms- Edge computing, Internet of Things (IoT), smart home and city

I. INTRODUCTION

Cloud computing has extremely transformed the way we live, job, and research since its inception around 2005 [1]. For instance, a software as a service (SaaS) instances, such as Flickr, Facebook, Twitter, and Google Apps, have been commonly used in the daily life of ours. Additionally, scalable infrastructures, as well as processing engines created to help cloud service, are also considerably influencing the way of managing the company, for example, Google File System [2], MapReduce [3], Apache Hadoop [4], Apache Spark [5], etc. Internet of Things (IoT) was first released to the neighborhood in 1999 for supply chain management [6], and next the idea of "making a computer sense data without the aid of human intervention" was broadly adapted to different fields for example healthcare, transports, environment, and home [7], [8]. Today with IoT, we are going to arrive in the post-cloud era, where there'll be a big quality of datageneratedby things which are immersed in the daily life of ours, and a lot of programs will additionally be used at the edge to ingest the data. By 2019, data produced by people, machines, and things are going to reach 500 zettabytes, as calculated by Cisco Global Cloud Index, nonetheless, the worldwide information center IP traffic is only going to attain 10.4 zettabytes by that moment [9]. By 2019, 45% of IoT-created details will be saved, prepared, examined, as well as acted upon close to, or perhaps at the edge of, the network [10]. There will Some IoT applications could require very quick response time, somemight involve private details, and some may generate a significant amount of information which may be a large load for networks. Cloud computing is not effective enough to help the applications. As shown in Fig. 1, both topics gained popularity in the last few years (Fig. 1a), and the number of papers dealing with Cloud and IoT separately shows an increasing trend since 2008 (Fig. 1b). On the other hand, a more recent and rapidly increasing trend deals with Cloud and IoT together. Following the indications reported, we adopt the research methodology schematically depicted in Fig. 2. We first provide a temporal characterization of the literature aiming at showing in a qualitative way the temporal behavior of the research and the common interest about the CloudIoT paradigm. Second, we provide a detailed discussion on the CloudIoT paradigm, highlighting the complementarity and the need for their integration. Third, we detail the new application scenarios stemming from the adoption of the CloudIoT paradigm. Fourth, jointly analyzing the CloudIoT paradigm and the application scenarios, we derive the hot topics and related issues for research. Fifth, we describe the main platforms (both commercial and open source) and research projects in the field of CloudIoT. Finally, thanks to the previous seven steps, we derive the open issues and future directions in the field of CloudIoT.
Fig. 1: Research and interest trends about Cloud and IoT.

An independent evolution has been seen by the 2 worlds of IoT and Cloud. Nevertheless, many mutual advantages deriving from their integration have been defined in literature and are actually foreseen down the road. On the one hand, IoT can easily gain from the virtually unlimited features and materials of Cloud to compensate its technological constraints (e.g., storage, processing, energy). Specifically, the Cloud can offer an effective solution to implement IoT service management as well as composition as well as applications that exploit the data or the things created by them. On the various other hand, the Cloud can easily benefit from IoT by extending the scope of its to cope with world things that are real in a much more distributed and powerful fashion, and for supplying brand new services in a big selection of real world scenarios. The complementary features of IoT and Cloud arising from the various proposals in literature and motivating the CloudIoT paradigm. Essentially, the Cloud acts as an intermediate level between the applications, and the things where it hides all of the complexity and also the functionalities needed to apply the latter. This framework will impact future program development, in which info gathering, new challenges will be produced by processing, and transmission to be resolved, also in a multi cloud environment.

II. BACKGROUND WORKS

Secret Key Encryption: In secret key encryption, the end user unit first creates a secret key. Then the information is encrypted with the key and is actually delivered to the recipient pc user device. By using exactly the same element, the recipient device is able to recoup the information from the encrypted type of information by decrypting with the secret key element. In order to keep the process secret, the solution is discussed with communicating devices using secure communication principals.

Public Key Encryption: In public crucial encryption, there are actually 2 types of keys: a public element and a secret element. Before sending, the data is actually encrypted with the recipient’s public key and after getting the data are actually decrypted by the recipient’s secret element to recover the data.

Searchable Secret Key Encryption: This mechanism is actually grounded on secret key encryption which enables searching certain details on outsourced storage-encrypted data via a generated trapdoor. The data owner device has to discuss the secret primary factor with all authorized products to create the trapdoor.

One-Way Hash Algorithms: After communicating, it’s essential to confirm the information aren’t altered in any way in between the sender as well as the receiver. This verification is actually called integrity checking. Generally, the integrity checking is completed by a hash feature. In case a publicly known hash function is actually put onto the information with a specified length, then the end result is actually known as the hash worth of the information. Nevertheless, this procedure is just one-way, it can’t recover the corresponding information from the hash value. The sender sends the information with its corresponding hash value. After receiving the information, the receiver inspections data integrity by the exact same way, implementing the hash feature to the received information; in case both hash values are actually the exact same, then the information has been proven to be candid.

In this paper, by considering the aforementioned limitations of current solutions for resource-limited smart devices, we propose a lightweight cryptographic scheme so that IoT smart devices can share data with others at the edge of cloud-assisted IoT wherein all security-oriented operations are offloaded to nearby edge servers. Furthermore, although initially we focus on data-sharing security, we also propose a data-searching scheme to search desired data/shared data by authorized users on storage where all data are in encrypted form. Finally, security and performance analysis shows that our proposed scheme is efficient and reduces the computation and communication overhead of all entities that are used in our scheme.

III. PROPOSED LIGHTWEIGHT CRYPTOGRAPHIC SCHEME
In our scheme, we consider a model of IoT data sharing and searching at the edge system that consists of four main entities.

![Edge Servers Diagram](image)

**Figure 2. Cloud-assisted internet of things scenario**

- **Edge Servers**
  - Examples: Personal mobile devices, network devices hosted within onehop, stand-alone servers
  - Provides data processing, communication, storage close to smart devices while also connected with cloud servers
- **Data Sharing for Smart Devices**
  - Data sharing between smart devices is essential component of IoT
  - Sharing at edge instead of centralized cloud model creates faster data access, higher bandwidth, lower latency
  - This creates potential security issues
  - Risks: Data leakage, data modification, integrity, unauthorized access
  - Essentials: Confidentiality, integrity, access control
  - IoT devices cannot handle typical computation-intensive operations form security

In this section, we present our proposed scheme that secures the sharing and searching of data at the edge of cloud-assisted IoT. Before data sharing and searching, all users need to register with edge servers by username and password to avail data sharing, downloading, desired data searching and retrieving.

1. Create secure data-sharing scheme that uses both secret key encryption and public key encryption. Edge servers handle all security operations
2. Create searching scheme for authorized users to search for desired data stored on edge/cloud
3. Create verification process for shared data and data retrieval after searching (proving data integrity)
4. Analyze performance of scheme to show efficiency and efficacy for IoT use

**Encryption Concepts:** The following things are to happen during the encryption process

- **Secret Key Encryption**
- **Public Key Encryption**
- **Searchable Secret Key Encryption**
- **Searching specific data on outsourced storage encrypted data via a generated trapdoor. The data owner device needs to share the secret key with all authorized devices to generate the trapdoor.**
- **One-way Hash Algorithms**
- **Verify data has not been modified with integrity checking via hash functions**
- **Digital Signature**
  - Key pair, digital cert ensures identity of user or entity

1. **Key Generation:** Edge Server generates two types of private keys on behalf of smart devices differently and uniquely
   - 256 bit keys randomly generated
2. **Data and Keyword Uploading:**
   - Edge Server (ES) stores username/password for data owner
   - IoT data is transferred to nearby ES
   - IoT sends keywords of data to ES for search
   - Key generation server sends pair of keys to ES
   - ES encrypts data and keywords before uploading to cloud
   - CA issues digital certificate to verify ES
   - To ensure integrity, compute hash and sign hash with private key
     - \( H_1 \leftarrow \text{Compute hash (Data)} \)
     - Signed.\( H_1 \leftarrow \text{Sign (H1, Private.Key)} \)
   - ES uploads tuple to a table under username
     - (Encrypted data, encrypted key, signed hash, sig)
3. Data Sharing and Downloading:
1. Access Data: authorized IoT requests data from ES with username/password
2. ES downloads tuple under username
   1. (Encrypted data, encrypted key, signed hash, sig)
   2. (C.Share || C.Sec.Key || C.KW.Search || Signed.H1 || Dig.Cert)
3. ES checks digital cert
4. Decrypts private key (fails if not authorized)
5. ES decrypts data
   • Data ← Decrypt (C.Share, Sec.Key)
6. Verifies data with hash function
   • H2 ← Calculate hash (Data) H1 ← Decrypt (Signed.H1, Public.Key)
   Check (H1=H2)
7. Finally data is sent to authorized recipient

4. Data Searching and Retrieval:
1. To search for data, auth user sends keyword to ES after login
2. ES receives secret key to generate trapdoor
3. Trapdoor sent to storage server with request to search
4. Storage server searches encrypted keywords under username, sends tuple back to edge server on success
5. ES checks digital certificate
6. Decrypts secret key and then decrypts to get data
7. ES verifies with hash function, sending data to device on success

For AES, we used the cipher block chaining mode. The performance of our scheme is evaluated based on processing times. Therefore, we tested the processing time of data encryption/decryption with AES by 256-bit key size and different data size (10 to 500 Mbyte). We also tested key generation time, secret key encryption with RSA by key size of 1024 bit, hash value generation, and signing- and verification-processing times for both downloading and uploading sides. As discussed earlier, in our proposed scheme, all security-oriented operations of smart devices are executed at nearby edge servers; we focused on calculating the total processing time on edge servers.

IV. CONCLUSION
Nowadays, a growing number of solutions are actually pressed from the cloud to the advantage of the network since processing details at the edge is able to guarantee shorter response time as well as much better reliability. Moreover, bandwidth may also be protected in case a bigger part of information might be managed at the edge instead of uploaded to the cloud. With this paper, we show a proposed data sharing and searching scheme to discuss and search information securely by IoT bright products at the edge of cloud assisted IoT. The overall performance
analysis demonstrates that the scheme of ours is able to achieve much better efficiency in the terminology of processing period compared with existing cloud-based systems. In future work, we intend on authenticating and accessing management issues in this specific place.

REFERENCES