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

P B V Rajarao[1] Dr N Srinivasu[2]
[1]*Asssociate Professor, Dept of CSE BVCE,Odalarevu, Andhrapradesh, India*
[2]*Professor, K L University, Greenfields, Vaddeswaram, Andhrapradesh, India*

Abstract- **Cloud computing in addition to Internet ofThings (IoT), two very different technologies, are actually both currently part of the life of ours. Theirtake advantage of and massive adoption are anticipatedto increase more, making them crucial parts of the Future Internet. A novelparadigm where IoT and Cloud are actually merged together is forseenas disruptive as well as an enabler of a lot of application scenario.Thispaper proposes an effective data sharing system which allows for smartproducts to share secure data with other people at the edge of cloud assisted Internet of Things (IoT). We likewise suggest a protected searching scheme toData 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 asFlickr, 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 todifferent 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 ofprograms will additionally be used at the edge to ingest the data. By 2019, data produced by people, machines, andthings are going to reach 500 zettabytes, as calculated by Cisco GlobalCloud Index, nonetheless, the worldwide information center IP traffic is only going to attain 10.4 zettabytes by that moment [9]. By 2019, 45% ofIoT-created details will be saved, prepared, examined, as well as acted upon close to, or perhaps at the edge of, the network [10]. There willSomeIoT 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 topicsgained popularity in the last few years (Fig. 1a), and thenumber of papers dealing with Cloud and IoT separately showsan increasing trend since 2008 (Fig. 1b)1. On the other hand,a more recent and rapidly increasing trend deals with CloudandIoT together. Following the indications reported,we adopt the research methodology schematically depicted inFig. 2. We first provide a temporal characterization of theliterature aiming at showing in a qualitative way the temporalbehavior of the research and the common interest about theCloudIoT paradigm. Second, we provide a detailed discussionon the CloudIoT paradigm, highlighting the complementarityand the need for their integration. Third, we detail the newapplication scenarios stemming from the adoption of theCloudIoT paradigm. Fourth, jointly analyzing the CloudIoTparadigm and the application scenarios, we derive the hottopics and related issues for research. Fifth, we describethe main platforms (both commercial and open source) andresearch projects in the field of CloudIoT. Finally, thanks tothe previous seven steps, we derive the open issues and futuredirections in the field of CloudIoT.

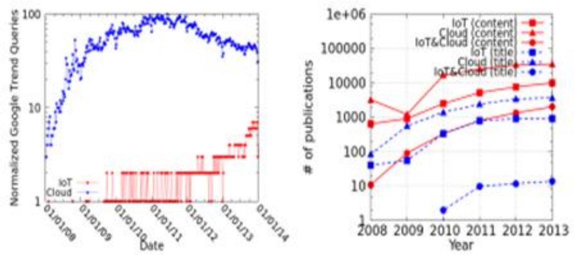


Fig. 1: Research and interest trends about Cloud and IoT.

An independent evolution has been seen by the 2 worlds of IoT and Cloud. Nevertheless, many mutual advantages deriving fromtheir integration have been defined in literature and are actually foreseen down the road. On the one hand, IoT can easily gain from thevirtually unlimited features and materials of Cloud to compensate its technological constraints (e.g., storage, processing,energy). Specifically, the Cloud can offer an effective solutionto implement IoT service management as well as composition as wellas applications that exploit the data or the things created by them. On the various other hand, the Cloud can easily benefit fromIoT by extending the scope of its to cope with world things that are real ina much more distributed and powerful fashion, and for supplying brand new services in a big selection of real world scenarios. Thecomplementary features of IoT and Cloud arising from the various proposals in literature and motivating the CloudIoTparadigm.Essentially, the Cloud actsas 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 impactfuture program development, in which info gathering,Brand new challenges will be produced by processing, and transmission tobe 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 withthe key and is actually delivered to the recipient pc user device. Byusing 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 usingsecure 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 publickey and after getting the data are actually decrypted by the recipient's secret ingredient to recover the data.

Searchable Secret Key Encryption:This mechanism is actually grounded on secret key encryptionwhich enables searching certain details on outsourced storage-encrypted data via a generated trapdoor. Thedata 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 theinformation 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 iscompleted by a hash feature. In case a publicly knownhash 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, thereceiver inspections data integrity by the exact same way, implementing the hash feature to the received information; in case bothhash 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 resourcelimited smart devices, we propose a lightweightcryptographic scheme so that IoT smart devices canshare data with others at the edge of cloud-assisted IoT wherein all security-oriented operations areoffloaded to nearby edge servers. Furthermore, although initially we focus on data-sharing security,we also propose a data-searching scheme to searchdesired data/shared data by authorized users on storage where all data are in encrypted form. Finally,security and performance analysis shows that ourproposed scheme is effcient and reduces the computation and communication overhead of all entitiesthat 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 consistsoffour main entities.

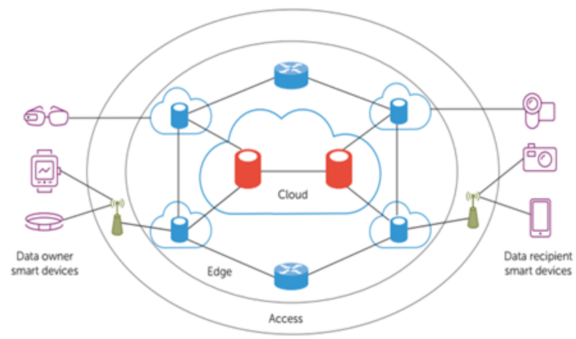


Figure 2.Cloud-assisted internet of things scenario

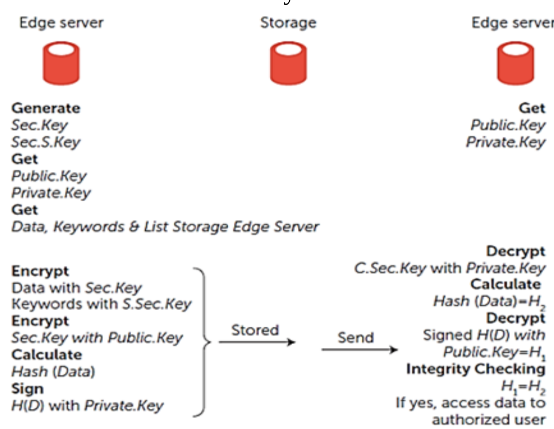
• Edge Servers
• Examples: Personal mobile devices, network devices hosted within onehop, stand-alone servers
• Provides data processing, communication, storage close to smart deviceswhile also connected with cloud servers
• Data Sharing for Smart Devices
• Data sharing between smart devices is essential component of IoT
• Sharing at edge instead of centralized cloud model creates faster dataaccess, 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 schemethat secures the sharing and searching of data atthe edge of cloud-assisted IoT. Before data sharingand searching, all users need to register with edgeservers by username and password to avail datasharing, downloading, desired data searching andretrieving.

1. Create secure data-sharing scheme that uses both secret keyencryption and public key encryption. Edge servers handle allsecurity operations
2. Create searching scheme for authorized users to search fordesired data stored on edge/cloud
3. Create verification process for shared data and data retrievalafter searching (proving data integrity)
4. Analyze performance of scheme to show efficiency and efficacyforIoT use

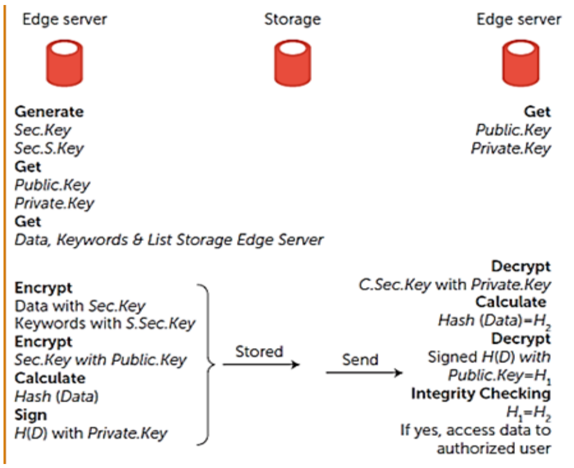
Encryption Concepts: The following things are to happen during the Encryption process
• Secret Key Encryption
• Public Key Encryption
• Searchable Secret Key Encryption
• Searching specific data on outsourced storage encrypted data via a generatedtrapdoor. The data owner device needs to share the secret key with allauthorized 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 generate two types of privatekeys on behalf of smart devices(differently and uniquely)256 bit keys randomly generated
1. Sec.key - Data Sharing
2. S.Sec.Key– Searching

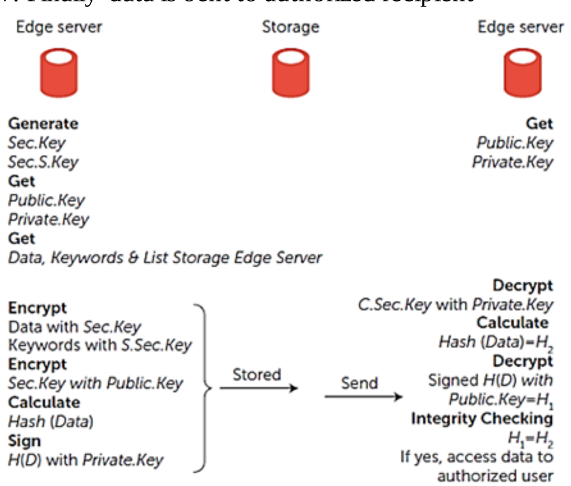


2. Data and KeywordUploading:
1. Edge Server (ES) stores username/password for data owner
2. IoT data is transferred to nearby ES
3. IoT sends keywords of data to ES for search
4. Key generation Server sends pair of keys to ES
5. ES encrypts data and keywords before uploading to cloud
6. CA issues digital certificate to verify ES
7. To ensure integrity, compute hash and signhash with private key
• H1 ← Compute hash (Data)
• Signed.H1 ← Sign (H1, Private.Key)

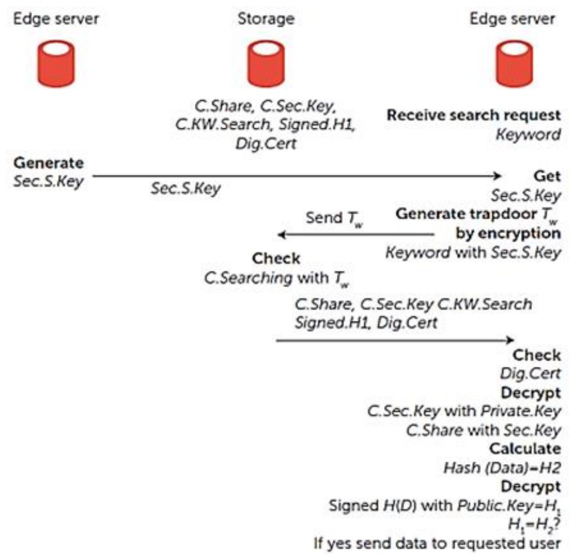
ES uploads tuple to a table under username
(Encrypted data, encrypted key, signed hash, sig)



3. Data SharingandDownloading:
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 andRetrieval:
1. To search for data, auth user sends keywordto ES after login
2. ES receives secret key to generate trapdoor
3. Trapdoor sent to storage server with requestto search
4. Storage server searches encrypted keywordsunder username, sends tuple back to edgeserver on success
5. ES checks digital certificate
6. Decrypts secret key and then decrypts to getdata
7. ES verifies with hash function, sending datato device on success



For AES, we used the cipher block chaining mode. The performance of ourscheme is evaluated based on processing times.Therefore, we tested the processing time of dataencryption/decryption with AES by 256-bit key sizeand different data size (10 to 500 Mbyte). We alsotested key generation time, secret key encryptionwith RSA by key size of 1024 bit, hash value generation, and signing- and verifcation-processing timesfor both downloading and uploading sides. As discussed earlier, in our proposed scheme, all securityoriented operations of smart devices are executed atnearby edge servers; we focused on calculating thetotal 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

[1] M. Armbrust et al., “A view of cloud computing,” Commun. ACM,vol. 53, no. 4, pp. 50–58, 2010.

[2] S. Ghemawat, H. Gobioff, and S.-T.Leung, “The Google file system,”ACM SIGOPS Oper. Syst. Rev., vol. 37, no. 5, pp. 29–43, 2003.

[3] J. Dean and S. Ghemawat, “MapReduce: Simplified data processingon large clusters,” Commun. ACM, vol. 51, no. 1, pp. 107–113, 2008.

[4] K. Shvachko, H. Kuang, S. Radia, and R. Chansler, “The hadoop distributed file system,” in Proc. IEEE 26th Symp. Mass Storage Syst.Technol. (MSST), Incline Village, NV, USA, 2010, pp. 1–10.

[5] M. Zaharia, M. Chowdhury, M. J. Franklin, S. Shenker, and I. Stoica,“Spark: Cluster computing with working sets,” in Proc. 2nd USENIXConf. Hot Topics Cloud Comput., vol. 10. Boston, MA, USA, 2010,p. 10.

[6] K. Ashton, “That Internet of Things thing,” RFiD J., vol. 22, no. 7,pp. 97–114, 2009.

[7] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, “Vision andchallenges for realising the Internet of things,” vol. 20, no. 10, 2010.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet ofThings (IoT): A vision, architectural elements, and future directions,”FutureGener. Comput.Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[9] “Cisco global cloud index: Forecast and methodology, 2014–2019white paper,” 2014.

[10] D. Evans, “The Internet of Things: How the next evolution of theInternet is changing everything,” CISCO White Paper, vol. 1, pp. 1–11,

[11] H. Li, D. Liu, Y. Dai, T.H. Luan, and X. Shen,“Enabling Effcient Multi-Keyword RankedSearch over Encrypted Mobile Cloud DataThrough Blind Storage,” IEEE Trans. Emerging Topics in Computing, vol. 3, no. 1, 2015, pp.127–138.

[12] H. Li, D. Liu, Y. Dai, and T.H. Luan, “Engineering Searchable Encryption of Mobile CloudNetworks: When Qoe Meets Qop,” IEEE Wireless Communications, vol. 22, no. 4, 2015, pp.74–80.

[13] L. Xu, X. Wu, and X. Zhang, :CL-PRE: A Certifcateless Proxy Re-Encryption Scheme For Secure Data Sharing with Public Cloud,” Proc. 7thACM Symposium on Information, Computer andCommunications Security, 2012, pp. 87–88.

[14] A.N. Khan, M.M. Kiah, S.A. Madani, M. Ali,and S. Shamshirband, “Incremental Proxy ReEncryption Scheme for Mobile Cloud Computing Environment,” J. Supercomputing, vol. 68,no. 2, 2014, pp. 624–651.

[15] S.K. Pasupuleti, S. Ramalingam, and R. Buyya,“An Effcient and Secure Privacy-Preserving Approach for Outsourced Data of Resource Constrained Mobile Devices in Cloud Computing,”J. Network and Computer Applications, vol. 64,2016, pp. 12–22.