International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Mobile Relay Arrangement in Wireless Sensor Networks

G. Dhana Sekhar[1], D. Pavan[2], A. Akill Kumar[2]

[1]Asst.Professor, MCA, Department of Computer Applications Svcet, Chittoor, Andhra Pradesh, India
[2]PG Scholar, Department of Computer Applications Svcet, Chittoor, Andhra Pradesh, India

ABSTRACT

Over the last few years, smart devices are able to communicate with each other and with Internet/cloud from short to long range. As a consequence, a new paradigm is introduced called Internet of Things (IoT). However, by utilizing cloud computing, resource limited IoT smart devices can get various benefits like offload data storage and processing burden at cloud. To support latency sensitive, real-time data processing, mobility and high data rate IoT applications, working at the edge of the network offers more benefits than cloud. In this paper, we propose an efficient data sharing scheme that allows smart devices to securely share data with others at the edge of cloud-assisted IoT. In addition, we also propose a secure searching scheme to search desired data within own/shared data on storage. Finally, we analyze the performance based on processing time of our proposed scheme. The results demonstrate that our scheme has potential to be effectively used in IoT applications.

Keywords: Secret Key Encryption And Public Key Encryption Searching Scheme, Key Generation, Data And Keywords Uploading, Data Sharing And Downloading And Data Searching And Retrieval.

I. INTRODUCTION

The Internet of things is that the network of physical devices, vehicles, home appliances and different things embedded with physical science, software, sensors, actuators, and property that allow these objects to attach and exchange knowledge. Internet of things (Iot1) is taken into account as a future internet that extends the association of the web to any or all types of real-world physical good devices. A estimates that by 2020 around fifty billion of such good devices are going to be connected to the web. By connecting these billions of good devices to the web, the IoT can offer developed good and autonomous cyber-physical environments within the space of good grids, good cities, good homes, good medical and health care systems, wearable technologies, transportation systems, etc. However, the bulk of those devices area unit a part of an outsized platform, hence, a large quantity of information area unit generated that needs high procedure capabilities for storage, processing, and analyzing functions in a very secure and economical manner. Generally, the good devices have restricted resources. On the opposite hand, cloud resources have virtually unlimited storage and process capabilities with measurability and on-demand accessibility anyplace. Therefore with the assistance of the cloud, the IoT good devices will relieve the burden of restricted resources.2 For IoT applications, good devices need low latency, high rate, quick knowledge access, and period knowledge analytics/processing with decision-making and quality support. Due to many drawbacks, the cloud cannot fulfill all the aforesaid needs. However, edge computing adds several benefit it's to cloud-assisted IoT3 and supports aforesaid needs by keeping processing, communications, and storage operation

nervy servers that area unit near the devices at the sting of the networks. Moreover, attributable to good devices' restricted vary of property, the sting servers will function intermediaries for communications over long distances. These edge servers area unit any personal device or mobile device, complete servers, or network devices that area unit hosted at intervals one hop far from the tip devices. Additionally, the sting servers also work and connect powerfully with cloud servers. Internet of things (Iot)1 is taken into account as a future internet that extends the association of the web to any or all types of real-world physical good devices. By connecting these billions of good devices to the web, the IoT can offer developed good and autonomous cyber-physical environments within the space of good grids, good cities, good homes, good medical and health care systems, wearable technologies, transportation systems, etc. However, the bulk of those devices area unit a part of an outsized platform, hence, a large quantity of information area unit generated that needs high procedure capabilities for storage, processing, and analyzing functions in a very secure and economical manner. Generally, the good devices have restricted resources. On the opposite hand, cloud resources have just about unlimited storage and process capabilities with measurability and on-demand accessibility anyplace. Therefore with the assistance of then cloud, the IoT good devices will relieve the burden of restricted resources.2 For IoT applications, good devices need low latency, high rate, quick knowledge access, and period knowledge analytics/processing with decision-making and quality support. in this paper, we tend to propose a light-weight crypto logic theme so IoT good devices will share knowledge with others at the sting of cloud-assisted IoT whereby all security-oriented operations area unit offloaded to near edge servers. what is more, though ab initio we tend to concentrate on data-sharing security, we tend to conjointly propose a knowledge-searching theme to look desired knowledge/shared data by approved users on storage wherever all data area unit in encrypted type. Finally, security and performance analysis shows that our proposed theme is efficient and reduces the computation and communication overhead of all entities that area unit employed in our theme. First, we tend to propose a secure data-sharing theme at the sting of cloud connected IoT good devices that utilize each secret key encoding and public key encoding. During this theme, all security operations area unit offloaded to near edge servers, thereby, greatly reducing the process burden of good devices. Next, we tend to propose a looking out theme to look desired knowledge firmly by authorized users at intervals encrypted, stored, shared knowledge in edge/cloud while not leaking keyword, secret key, and data, thereby reducing each computation and communication overhead throughout search and knowledge retrieval. Then, we tend to show the verification method of the shared knowledge similarly as knowledge retrieval once looking out. Hence, our planned theme attains the integrity of shared knowledge and looking out resultant knowledge. Finally, we tend to analyze the performance of our planned theme and prove that our theme is economical and may be employed in IoT applications. The key contributions of our work area unit summarized as follows: one. First, we tend to propose a secure data-sharing theme at the sting of cloud connected IoT good devices that utilize each secret key encoding and public key encoding. During this theme, all security operations area unit offloaded to near edge servers, thereby, greatly reducing the process burden of good devices. 2. Next, we tend to propose a looking out theme to look desired knowledge firmly by approved users at intervals encrypted, stored, shared knowledge in edge/cloud while not leaking keyword, secret key, and data, thereby reducing each computation and communication overhead throughout search and knowledge retrieval. 3. Then, we tend to show the verify ion method of the shared knowledge similarly as knowledge retrieval once looking out. Hence, our planned theme attains the integrity of shared knowledge and looking out resultant knowledge. 4.

Finally, we tend to analyze the performance of our proposed theme and prove that our theme is efficient and may be employed in IoT applications.

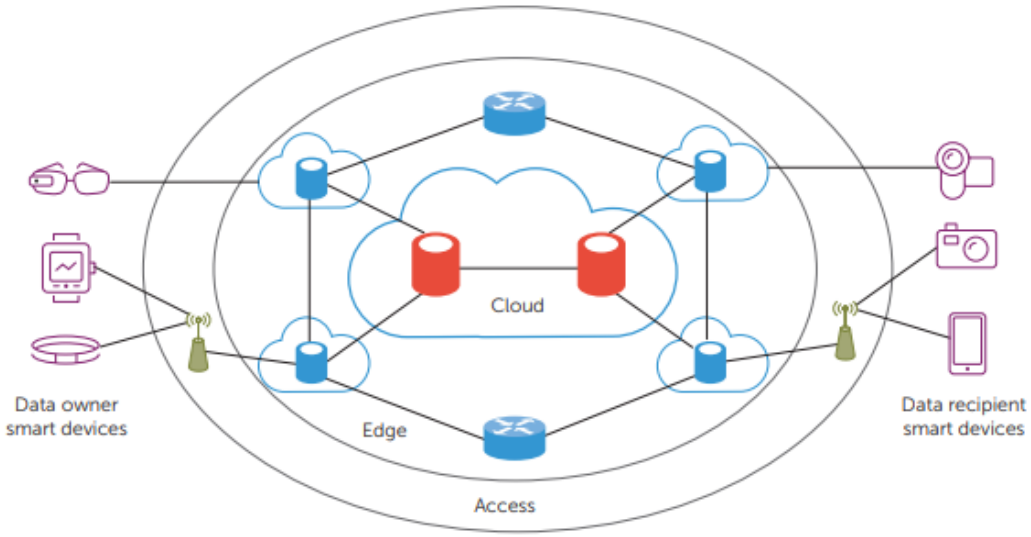

Figure 1.. Cloud-assisted Internet of Things scenario.

Secret Key Encryption

In secret key encryption, the user device first generates a secret key. Then the data are encrypted with the key and is sent to the recipient user device. By using the same key, the recipient device can recover the data from the encrypted form of data by decrypting with the secret key. To keep the process secret, the key is shared with communicating devices using secure communication principals.

Public Key Encryption

In public key encryption, there are two kinds of keys: a public key and a secret key. Before sending, the data are encrypted with the recipient's public key and after receiving the data are decrypted by the recipient's secret key to recover the data.

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

Smart Devices

The smart devices, connected with the physical world, are entities that have a large amount of data to be shared with other devices or stored in edge/storage servers. The authorized smart devices are allowed to decrypt/download the shared data and also retrieve desired data after searching from encrypted storage.

Edge Servers

The edge servers are semi trusted and secure entities located at the proximity of smart devices that are capable of sharing data with a number of smart devices. It is responsible for security-oriented operations such as secret key generation and management, encryption, and decryption. The edge servers are maintained by clouds. Moreover, the edge servers provide data storage and processing of the smart devices.

Certificate Authority

The certificate authority is fully trusted and is responsible for issuing certificates to edge servers.

Key Generation Server

The key generation server is also a trusted third party that is responsible for generation of public and secret key pairs. As shown in Figure 1, the data owner and

recipient smart devices are connected to each other by edge servers and edge servers are interconnected with each other so that data are shared and searched within the IoT scenario.

II. ALGORITHM

Key Generation

In our scheme, the edge servers generate two kinds of secret keys on behalf of data owner smart devices as follows: 1) 256 bit keys are randomly generated, and 2) two kinds of keys, Sec.Key and S.Sec.Key, are assigned that are used for data-sharing and -searching purposes, respectively. With the help of the list uploaded by the data owner smart device, the edge server generates both secret keys differently and uniquely.

Data and Keywords Uploading

The data owner first puts the username and password to login into a nearby edge server from a smart device. After collecting the data from the physical systems, the data are transferred from the smart device to nearby edge servers. In addition, the data owner sends some related keywords of the data so that any authorized users can search the data and a list of recipient users that are authorized to access the data. Before uploading the data from edge server to storage, the data and its associated keywords are encrypted. And finally, to verify data integrity, the encrypted data are signed. Therefore, after receiving the data, keywords, and list, the edge server works as follows: Encrypt the data with secret key for sharing as C.Share ← Encrypt (Data, Sec.Key) Next, by using secret key for searching, the keywords are encrypted as C.KW.Search ← Encrypt (Keywords, S.Sec.Key) The edge server receives pair of keys from key generation server such as public key Public.Key and private key Private.Key on behalf of the data owner and every recipient smart device with the help of list provided by the data owner's smart device. Moreover, the edge server is issued a digital certificate Dig.Cert from certificate authority that guarantees the validity of the edge server and contains its identification information. To share securely with authorized devices, the secret key is encrypted with authorized recipients' public keys as C.Sec.Key ← Encrypt (Sec.Key, Public. Key) To ensure integrity, the edge server computes the hash value of encrypted form of the data by collision resistant hash function as H1 ← Compute hash (Data) Then, the edge server signs the hash value with the data owner's private key as Signed.H1 ← Sign (H1, Private.Key) Finally, the edge server uploads the tuple (C.Share || C.Sec.Key || C.KW.Search || Signed.H1 || Dig.Cert) to the edge storage or cloud as per requirements under the username. After verifying Dig.Cert, the tuple is stored in storage. The data structure of uploading data from smart device to edge server under a username and from the edge server to storage under different usernames.

Data Sharing and Downloading

When an authorized smart device wants to access the data, it requests the nearby edge server after the login using the username and password. Then, the edge server works as follows: The edge server downloads and stores the tuple (C.Share || C.Sec.Key || C.KW.Search || Signed.H1 || Dig.Cert) under the data owner username from storage. The edge server checks the digital certificate Dig.Cert as Check (Dig.Cert) Then, first it decrypts the encrypted form of secret key as Sec.Key ← Decrypt (C.Sec.Key, Private.Key) If the requested user is not authorized, it cannot decrypt. After getting the secret key, the edge server decrypts the encrypted data and gets the data. Data ← Decrypt (C.Share, Sec.Key) To verify the integrity of decrypted data, the edge server works as H2 ← Calculate hash (Data) H1 ← Decrypt (Signed.H1, Public.Key) Check (H1=H2) If matched, then data integrity is verified. Finally, the data are sent to the authorized recipient.

Data Searching and Retrieval

To search a desired data on encrypted data on storage, the authorized user sends the keyword to the edge server after login. The edge server then works as

follows: The edge server receives the requested authorized user's secret key and generate trapdoor as Tw ← Encryption (Keyword, S.Sec.Key) Then Tw is uploaded to the storage server with a request to search. Next, the storage server searches for the matched encrypted keywords under the username based on the trapdoor as Check (C.KW.Search, Tw) If found, the corresponding tuple (C.Share || C.Sec.Key || C.KW.Search || Signed.H1 || Dig.Cert) is sent to the edge server. The edge server checks the digital certificate Dig.Cert as Check (Dig.Cert) Then, first it decrypts the encrypted form of secret key as Sec.Key ← Decrypt (C.Sec.Key, Private.Key) If the requested user is not authorized, it cannot decrypt. Then, the edge server decrypts to retrieve the data as Data ← Decrypt (C.Share, Sec.Key) To verify the integrity of decrypted data, the edge server works as H2 ← Calculate hash (Data) H1 ← Decrypt (Signed.H1, Public.Key) Check (H1=H2) If matched, then data integrity is verified. If verified, the data are sent to the requested authorized device. As searchable secret keys are generated for every smart device, there is no possibility of matching any data that is not shared with the requested device or does not belong to the device.

III. CONCLUSION

In this paper, 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. First, we propose a secure data-sharing scheme at the edge of cloud connected IoT smart devices that utilize both secret key encryption and public key encryption. In this scheme, all security operations are offloaded to nearby edge servers, thereby, greatly reducing the processing burden of smart devices. Next, we propose a searching scheme to search desired data securely by authorized users within encrypted, stored, shared data in edge/cloud without leaking keyword, secret key, and data, thereby reducing both computation and communication overhead during search and data retrieval. Then, we show the verification process of the shared data as well as data retrieval after searching. Hence, our proposed scheme attains the integrity of shared data and searching resultant data. Finally, we analyze the performance of our proposed scheme and prove that our scheme is efficient and can be used in IoT applications.

IV. REFERENCES

[1]. M.R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, et al., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," IEEE J. Selected Areas in Communications, vol. 34, no. 3, 2016, pp. 510–527.

[2]. L. Wang and R. Ranjan, "Processing Distributed Internet of Things Data in Clouds," IEEE Cloud Computing, vol. 2, no. 1, 2015, pp. 76–80.

[3]. M. Satyanarayanan, P. Simoens, Y. Xiao, P. Pillai, Z. Chen, K. Ha, et al., "Edge Analytics in the Internet of Things," IEEE Pervasive Computing, vol. 14, 2015, pp. 24–31.

[4]. S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog Computing: Platform and Applications," 2015 3rd IEEE Workshop Hot Topics Web Systems and Technologies (HotWeb), 2015, pp. 73–78.

[5]. J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for CloudSupported Internet of Things," IEEE Internet of Things J., vol. 3, no. 3, 2016, pp. 269–284.

[6]. M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A.V. Vasilakos, K. Li, et al., "SeDaSC: Secure

Data Sharing in Clouds," IEEE Systems J., vol. 99, 2015, pp. 1–10.

[7]. S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Trans. Knowledge and Data Engineering, vol. 26, no. 9, 2014, pp. 2107–2119.

[8]. H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, "Secure Data Analytics for CloudIntegrated Internet of Things Applications," IEEE Cloud Computing, vol. 3, no. 2, 2016, pp. 46–56.

[9]. J.B. Bernabe, J.L.H. Ramos, and A.F.S. Gomez, "TACIoT: Multidimensional Trust-Aware Access Control System for the Internet of Things," Soft Computing, vol. 20, no. 5, 2016, pp. 1763–1779.

[10]. F. Li, Y. Rahulamathavan, M. Conti, and M. Rajarajan, "Robust Access Control Framework for Mobile Cloud Computing Network," Computer Communications, vol. 68, 2015, pp. 61–72.

[11]. H. Li, D. Liu, Y. Dai, T.H. Luan, and X. Shen, "Enabling Efficient Multi-Keyword Ranked Search over Encrypted Mobile Cloud Data Through 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 Cloud Networks: 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 Certificateless Proxy Re-Encryption Scheme For Secure Data Sharing with Public Cloud," Proc. 7th ACM Symposium on Information, Computer and Communications 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 Efficient 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.