

# A Secured Frame Work for Searching and Sharing of Data in Cloud Based Services using IoT

Dhanabal Thirumoorthy\*, Tucha Kedir, Rabira Geleta, Abdul Kadir

Lecturer, College of Informatics, Bule Hora University, Bule Hora, Ethiopia

\*Corresponding Author

**Abstract**— The internet technologies evolved many new innovations in communication technologies for searching and sharing data over the IoT. The importance of both software and hardware technologies became an important for the service providers and users as well. Searching and data sharing is contemporary task for the services providers because security aspects. Efficient searching and secured data sharing is an open issue till now. Information leakage costs more for the organizations. In this paper we propose an efficient frame work for secured cloud based services where the data can be shared among multiple devices of IoT. Our scheme allows all smart devices interact and share data among users in Internet of Things securely. We also attempted to develop a useful searching mechanism for having required data by the users over distributed storage domains to share. We conducted an abundant survey and study them in depth for better improvement of our work.

**Keywords**— IoT, cloud based services, AES, DES, key generation, SHA.

## I. INTRODUCTION

The Internet of Things is one of the internet revolutions which provide a platform for all real world smart devices to connect and use the internet for searching and data sharing among various users. Various studies tell that by the end of the 2020 there would be great improvement in the usage of internet through smart devices. One of the studies of the CISCO<sup>1</sup> reveals that more than 50 billion smart devices are going to share the internet through various smart devices. The challenge for this act is to provide compatible environment by the time with capable searching and secured mechanism. It further extends to smart grids, smart technologies in the domains of homes, cities, medicine, healthcare systems, transport systems etc.

These heterogeneous smart devices will establish a platform for generating large volumes of data. The generated data will be stored in cloud. To access the cloud data highly computational techniques are required for searching, processing the data in shared platform with an efficiency and security. There will be a contradiction, smart devices have limited capacity but cloud services are virtual i.e. unlimited capabilities hence by using IoT this can be resolved some extent. IoT services required low latency, high data rate, fast data access, and real-time data analytics/processing with decision-making and mobility support of smart devices. It is one more gap for

efficient searching and data sharing in cloud based services.

## II. RELATED WORK

The objective of this paper is to provide proper searching and sharing data among users over cloud based services using IoT. Many smart devices are available in the market and easy to connect internet to access required data from cloud. The main focus is sharing of data among multiple smart devices which leads compatibility and extensibility of their services for efficient searching techniques. The generation of internet technologies crossing rapidly like 2G to 5G etc there may be expected phenomenon for device technologies.

In this paper we tried to give some possible solutions for efficient searching and with secured data sharing over the smart devices in cloud based services using IoT. The existed encrypted and decrypted security mechanisms performed well and the same we are extending for the problem like symmetric, public key and homomorphic encryptions used. For the controlling of access control used control list and dynamic attributes are used. Key encryptions are used for searching data for IoT. This is an extra burden to the smart devices hence heavy computational process is required.

By considering all the mentioned limitations there may be a need of an alternative solution is required. Hence we proposed a lightweight cryptographic mechanism for

security issues for smart devices of IoT. Our mechanisms performed well while sharing of data with other smart devices in IoT. Data searching can control when allowed authorized users then performance of the devices also increased which reduced heavy computational and communication capabilities.

We focused on the

1. Implementation of secure data-sharing scheme for cloud connected IoT smart devices.
2. Development of efficient searching techniques for users required data with authorized users for reducing computational and communication capabilities.
3. Prosing of validation and verification process for user's retrieved data which increases the integrity and searching data efficiency well.
4. Finally performance analysis with our proposed methods for IoT applications.

### III. LITERATURE SURVEY

Dario Bruneo, Salvatore Distefano [1] explained about various IoT service ecosystem for Smart Cities of the SmartMEproject. In this paper given results oriented solutions after 2 years, we present the results from environmental monitoring to parking management.

K. Narendra Swaroop a, Kavitha Chandu in [2] given a health monitoring system for vital signs using IoT, this article presents the design of a real-time health monitoring system which can store a patient's basic health parameters. Panagiotis I. Radoglou Grammatikis in [3] given few measures for securing the Internet of Things: Challenges, threats and solutions.

Sahitya Roy, Dr. Rajarshi Ray, IoT in [4] described the advanced technologies like Big Data Science & Analytics, Cloud Computing and Mobile App based Hybrid System for Smart Agriculture domain.

Andrea Zanella in [5] gave clear clarity about building of smart cities using IoT Internet.

Shahid Mumtaz, Guest Editorial in [6] drafted the summary of a special issue on 5G and Beyond-Mobile Technologies and Applications for IoT.

Mohamed Kheir in [7] drafted a special issue on Intrinsic Hardware Security for Internet of Things Infrastructure.

Liuqing Yang in [8] explained about IoT on the move: Enabling Technologies and Driving Applications for Internet of Intelligent Vehicles (IoIV).

Jasmin Guth in [9] tells about a detailed analysis of IoT platform architectures: Concepts, Similarities, and differences, [http://dx.doi.org/10.1007/978-981-10-5861-5\\_4](http://dx.doi.org/10.1007/978-981-10-5861-5_4).

We conducted an intensive survey from which we drafted the required things to use and modify technologies to improve our work. The survey is useful to us to take make and decisions about our work to select things required. All the existed works explained well in many aspects but little back on explanation of searching and security aspects.

The rest of the paper is organized as follows. In the fourth section, we present the proposed work, section five explains data sharing and searching, section six given the performance analysis of the work, section seven describes various cryptographic mechanisms that are used in our proposed scheme. We then analyse the performance and compare it to related works. Finally, we conclude our paper by drafting the conclusion.

### IV. PROPOSED WORK AND SECURITY ASPECTS

The proposed work concentrates various cryptographic techniques used and how they contributed to perform an efficient searching with security for shared data over the smart devices of IoT.

Cryptographic Technique	Description
Secret Key Encryption	By using secret key the user will send and receive secured data. Devices using secure communication principals.
Public Key Encryption	It is a two key mechanism, public key and a secret key. Public key can be used before sending data and secret key is used for decrypting the data.
Searchable Secret Key Encryption	It uses secret key by using trapdoor for authorized user devices only.
One Way Hash Algorithms	It is used for integrity check with hash functions i.e. if any data is modified between sender and receiver.
Digital Signature	Public and secret key are operated by the authorized users with digital signatures.

Our proposed work also explains the required overall architecture of the system for efficient searching and secured data sharing for cloud based services for IoT. The architecture is made up with the following entities shown in the below table.

Entity Type	Description
Smart Devices	Allow authorized devices to share searching data.
Server	Smart devices given privilege to

Technologies	connect to the servers must be located comfortably. Self oriented secured encryption and decryption can be done by the smart devices.
Certificate Authority	The certificate authority is fully trusted and is responsible for issuing certificates to edge servers.
Key Generation Mechanism	The public and secret keys can be generated by the third party servers to have security.

Here we focus on the various threats while sharing data among smart devices of IoT. Implicit threats generated by the system itself because of malicious functioning and explicit threats are generated by the unauthorized users using devices and is one more issues.

## V. SECURE DATA SHARING AND SEARCHING FOR IoT

Here we perform efficient searching and secured data sharing for smart device of cloud based services via IoT by using our proposed scheme.

### Algorithm Design Steps

Step1: All users must register and will be given user name and password  
 Step2: Allow the devices to download required data  
 Step3: Efficient searching for required relevant data  
 Step4: Then key generation for security aspects i.e encryption/decryption  
 Step5: Uploading of data and keywords for efficient searching  
 Step6: Allow devices to share and download data  
 Step7: Perform data retrieval and searching  
 Step8: Use digital signatures for data integrity  
 Step9: Safe searching and download for good performance by the authorized users  
 Step10: Controlling threats generations

Key Generation: The server will generate two secret keys first one is randomly generated secret key (256bit) and

second one is Sec.Key (for data sharing) and S.Sec.Key (for data searching) from devices side uniquely.

Data and Keywords Uploading: Every smart device is given user name and password to login into the server then data searching, sharing and transferring data among devices and servers is possible. List uploaded keywords are useful to the authorized users to search easily. While uploading data into the server storages devices must be encrypted with respective keys for data integrity. Then works based on the table 1.

Data Sharing and Downloading: Authorized users are allowed to access the data from cloud to reduce the bottleneck and increase the performance. Authorized user can be given user name and passwords through which they connect to the server through their smart devices from various locations. Then the server checks the user authentication using its digital signatures. Then using keys data can be had by performing encrypted and decrypted techniques and unauthorized users will get rejected. It is compulsory to perform an integrity action for checking received data. If data was found or matched then users can download or share it.

Data searching and retrieval will also follow the above steps but use trapdoors for generating keys to an efficient search for every device.

## VI. PERFORMANCE ANALYSIS

We used various encryption (AES, RSA and SHA-256) and decryption algorithms to generate secret key, public key and hash function development along with cipher chaining mode with respect to the processing time. The processing time was estimated for data decryption and encryption for various memory sizes of data (10 to 500MB) and calculated time process for key generation, data uploading, data downloading and searching and retrieval was given in the table 1. Data integrity was done in terms of valuation and verification of the transferred data in smart devices.

### Results Table

Table.1. Time processing of various techniques

Time For (ms) / Techniques	Encryption	Decryption	Digital signature	Total Processing
Key Generations	0.4	0.5	0.3	1.4ms
Data Uploading	1.6	2.0	1.2	4.8 ms
Data Downloading	1.2	1.8	0.7	3.7 ms
Data Searching and Retrieval	5.5	6.5	1.01	13.01 ms

We observed that the time factor is almost negligible irrespective of memory sizes, techniques used and other comparatively.

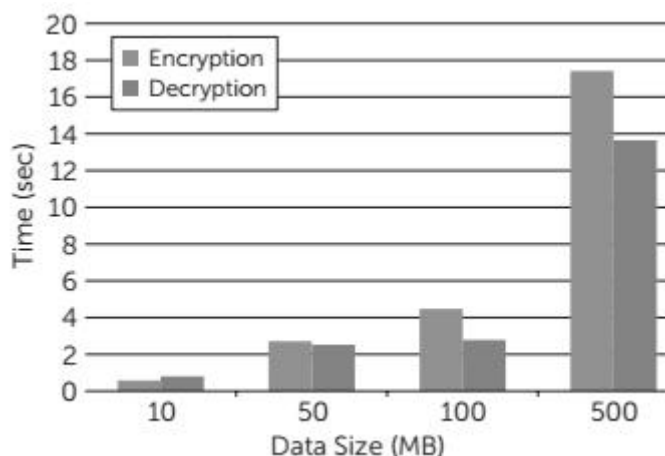


Fig.1. Processing time of encryption and decryption of AES.

## VII. RELATED WORKS AND COMPARATIVE ANALYSIS

This section we performed comparative study with respect to the other works. We have gone through the various papers related this work in terms of consumption of time processing in [6,7] developed a certificate less proxy re encryption using symmetric and public key techniques.

Table.2. Comparative study of the existed works

Author Work	Comparative study
S.H. Seo in [10]	used certificateless scheme for data sharing but without bilinear pairing
Mohamed Kheir in [7]	The cloud is responsible for both secure data storage and public/private key pair generation.
Baqer Mollah In [13]	The data can be encrypted with the secret key and then the secret key is further encrypted with public key finally send to cloud server.
Khan in [6]	Utilized an incremental cryptography based data sharing scheme where the data are divided into several blocks and these blocks are then incrementally encrypted.
Jasmin Guth in [14]	A trusted third party is used as a proxy for key generation, re-encryption, and access control purposes.
Ali in [15]	A secret key-based encryption and access control list for secure data sharing where a trusted third party is engaged in encryption/decryption, key management, and access control rather than the user's device itself is utilized.

Table.3. Comparison of total uploading time in seconds.

Data (MB)	Ref.9	Ref.11	Ref.10	Ref.12	Ref.13	Our Work
10	5.43	12.04	13.95	14.13	0.5612	0.4812
50	9.01	53.68	58.56	60.37	2.7162	2.1350
100	17.37	99.69	112.41	155.15	4.0213	3.9156
500	33.24	369.72	492.09	872.09	17.4262	16.9401

Table.4. Comparison of total downloading time in seconds.

Data (MB)	Ref.9	Ref.11	Ref.10	Ref.12	Ref.13	Our Work
10	6.48	9.91	9.90	10.45	0.8057	0.6037
50	10.24	33.45	35.57	35.90	2.5237	2.0273
100	20.68	57.14	59.14	61.59	2.7937	2.1806
500	39.25	215.3	229.81	400.21	13.6537	12.5637

## VIII. CONCLUSION

Our work presents a novel approach for efficient data sharing and searching scheme for cloud based services using IoT. We have gone through the various encryption and decryption techniques used in our work. When we compared the work we feel that our work gives better performance than others. The processing time can be calculated based on the searching, data sharing and other parameters of the work. It is observed that when all the smart devices connected to the server will get bottleneck

gradually performance will decrease where as the performance analysis in section six and demonstrated results are tabulated in table 2 and table 3. We feel some reformations are required related to authentication and access control challenges in this area to achieve data integrity. We hope that our proposed scheme is deployed an efficient performance and opens a new era to cloud based service using IoT secured applications.

## REFERENCES

- [1] Dario Bruneo, An IoT service ecosystem for Smart Cities: The #SmartMEproject, *Internet of Things* 5 (2019) 12–33, © 2018 Elsevier.
- [2] K. NarendraSwaroop, A health monitoring system for vital signs using IoT, *Internet of Things* 5 (2019) 116–129, © 2019 Elsevier.
- [3] Panagiotis I. RadoglouGrammatikis, Securing the Internet of Things: Challenges, threats and solutions, *Internet of Things* 5 (2019) 41–70, © 2018 Elsevier.
- [4] Sahitya. Roy, IoT, Big Data Science & Analytics, Cloud Computing and Mobile App based Hybrid System for Smart Agriculture, 978-1-5386-2215-5/17 © 2017 IEEE.
- [5] Andrea Zanella, Internet of Things for Smart Cities, *IEEE INTERNET OF THINGS JOURNAL*, VOL. 1, NO. 1, FEBRUARY 2014.
- [6] Guest Editorial, Special Issue on 5G and Beyond—Mobile Technologies and Applications for IoT, *IEEE INTERNET OF THINGS JOURNAL*, VOL. 6, NO. 1, FEBRUARY 2019.
- [7] Guest Editorial, Special Issue on Intrinsic Hardware Security for Internet of Things Infrastructure, *IEEE INTERNET OF THINGS JOURNAL*, VOL. 6, NO. 1, FEBRUARY 2019.
- [8] Guest Editorial, Special Issue on IoT on the Move: Enabling Technologies and Driving Applications for Internet of Intelligent Vehicles (IoIV), *IEEE INTERNET OF THINGS JOURNAL*, VOL. 6, NO. 1, FEBRUARY 2019.
- [9] 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.
- [10] 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.
- [11] L. Xu, X. Wu, and X. Zhang, “CL-PRE: A Certificateless Proxy Re-Encryption Scheme For Secure Data Sharing with Public Cloud,” *Proc. 7<sup>th</sup> ACM Symposium on Information, Computer and Communications Security*, 2012, pp. 87–88.
- [12] Jaiswal, Manishaben. “Cloud Computing and Infrastructure”. *International Journal of Research and Analytical Reviews*, vol 4, no. 2, 2017, pp. 742-746., doi:10.6084/m9.doi.one.IJRAR19D1251.
- [13] 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.
- [14] Muhammad Baqer Mollah, Cloud-Assisted Internet of Things, 2325-6095/17 © 2017 IEEE.
- [15] Jasmin Guth, A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences, *Institute of Architecture of Application Systems*, © 2018 Springer-Verlag.
- [16] AdilaMebrek, Efficient Green Solution for a Balanced Energy Consumption and Delay in the IoT-Fog-Cloud Computing, 978-1-5386-1465-5/17 © 2017 IEEE.