# High Security Data Sharing on Edge Servers by Internet of Things Users

**Jai Shree[1], Dr. Rekha Yadav[2]**

**1,2 Electronics and Communication Engineering Department**

**Deenbandhu Chhotu Ram University of Science and Technology, Sonipat**

**Abstract-** Due to the fast development of new technologies, new requirements are being imposed on a daily basis. The internet is a good illustration of this. The Internet of Things (IoT) is a new technology we've developed to make it even more sophisticated than it now is. A variety of smart devices may be connected to the internet using this technology. Take use of cloud computing in order to get additional benefits. The cloud stores all of the data that is generated, reducing the burden on smart devices. For communication and security purposes, edge servers are placed in close proximity to the linked devices. The goal of this paper is to use an edge server to speed up searches in a private cloud. Although all security features were maintained, there was an improvement in the time it took to complete an activity. User engagement and data interchange may be improved while keeping a high degree of security thanks to this. In addition, users may save time by searching for and downloading data from a secure server.

**Keyword-** IOT, Searching, Edge, Server

## Introduction

The term "next generation" is often used to describe the Internet of Things, or IoT. When Ashton came up with the concept in 1999, he was still an MIT student. The Internet of Things (IoT) will allow you to link any internet-capable smart gadget to the worldwide web. There is a lot of interest from a wide variety of businesses because of the various benefits it gives. Smart cities, health and fitness, smart vehicles, smart retail, and other areas of the economy will benefit greatly from this technology. In the years leading up to the year 2020, Cisco, a networking giant, anticipates that there will be fifty billion linked devices on the planet. When smart physical devices are employed in an Internet of Things setting, they generally generate a large quantity of data that may be used for analysis and processing, both of which need storage. Both of these operations need the use of storage space. As a result of its limited storage capacity, it is unable to support the creation of intelligent hardware devices. Because of this capacity's restrictions, this is the case. In order to solve this problem, the cloud was able to help us. It is possible to access one's data from almost anywhere at any time, and there is a vast array of storage solutions available thanks to the cloud. In the case of Internet of Things application devices, this is a particularly helpful feature since there is a very modest amount of storage space needed. Despite this, when these smart devices are used in Internet of Things (IoT) applications, the cloud is unable to meet all of the criteria for these devices. This includes support for high data rates and low latency, high-speed data access, real-time data processing, and other features. Edge servers may be used to ensure that the constraints described before are adhered to. An edge server is a network node that is only somewhat reliable, can operate independently, and must be kept physically close to intelligent physical things in order to function. This feature, when used in combination with an Internet of Things application, provides the remote access to smart devices that is needed. Confidentiality, honesty, and availability, all of which are critical to the CIA's activities, have been raised as a result of this data sharing. For the purposes of this discussion, data are considered secret if they cannot be read by anybody who is not explicitly authorised to make use of the data..

It's conceivable that an attacker is behind the problem if any of these are missing. There is a risk that this might lead to data breaches, deletions, theft, or manipulation. An enemy may be trying to launch an attack if any of these are missing. As a result, data transferred between smart devices is scrambled before being delivered. To ensure that only authorised devices may access encrypted data, each device already possesses the decryption key. The only way to guarantee that data may be accessed by authorised devices and only in a secure manner is to implement data retrieval methods. This is necessary for the reasons stated above. The Internet of Things device already has a lot of work to do, and this security component will just add to that burden..

## Implementation

Most Internet of Things devices need real-time networking for data transmission, and the volume of data is substantial. Cameras and lidar are used extensively in autonomous cars, which generates 1GB of data every second [1]. Data collected by IoT devices contain a large number of user privacy information, such as camera monitoring records, car driving records, account information, etc., and there is significant risk of privacy disclosure and malicious attacks like Bonet [3], DDoS [4], and Malware [6] for this personal privacy data. In sensor networks, key management, a broadcast authentication, has been used to offer greater security while using less storage space and energy. It was in 2003 when Akamai and IBM came up with the concept of "edge computing" that relied on edge services. In this paper, as part of improvement, added the cache memory concept; whenever a user issue query to the cloud server, then the cloud server performs a search operation on store data and sends the result back to the user. If a user issues the same query repeatedly, then the cloud server performs the same operation each time, resulting in high computation cost and waste of resources. To overcome this issue, maintain cache memory for all previous searches. Whenever the user issues the same query, the cloud server obtains results from cache memory instead of repeatedly searching computation. This technique can save computation cost and wastage of resources. In the following section, the system design mention in details through charts:

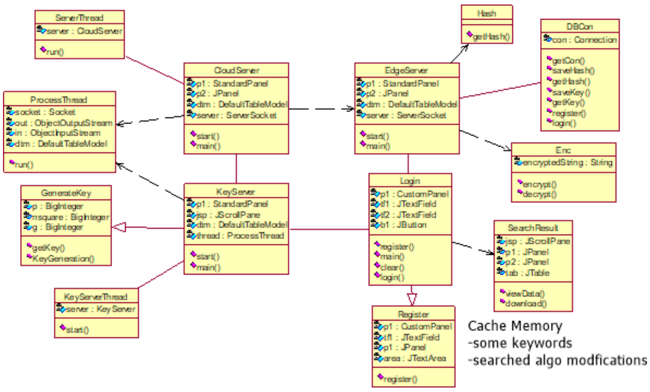
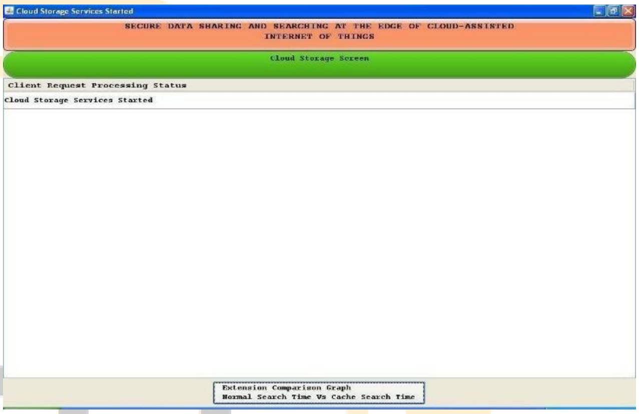


Figure 1: Class diagram of system design


Cloud Storage Services Started

SECURE DATA SHARING AND SEARCHING AT THE EDGE OF CLOUD-ASSISTED INTERNET OF THINGS

Cloud Storage Screen

Client Request Processing Status

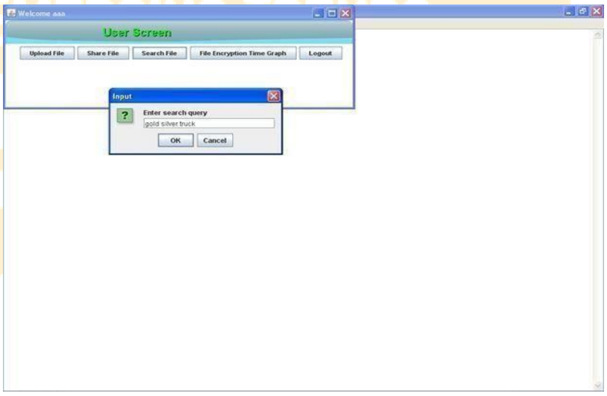
Cloud Storage Services Started

Extension Comparison Graph
Normal Search Time Vs Cache Search Time

Fig. 2: Screen for Cloud Storage Services.

Fig. 2 shows the Cloud server screen with a button to display the extension work graph.

See the below screen for a search operation in Fig. 3.


Welcome aaa

User Screen

Upload File | Share File | Search File | File Encryption Time Graph | Logout

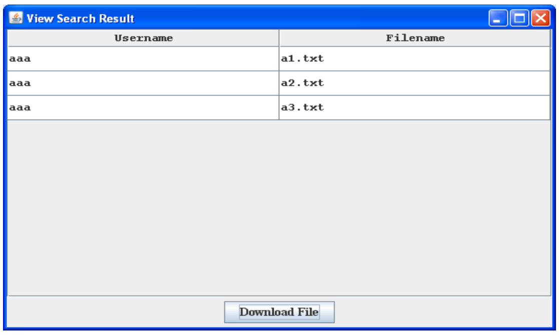
Input

Enter search query: gold silver truck

OK | Cancel

Fig.3: Search Query.

In above screen of Fig. 3 I gave the query as 'gold silver truck', and this query is not available in cache, so the cloud server will perform entire search computation and send the result back to user.

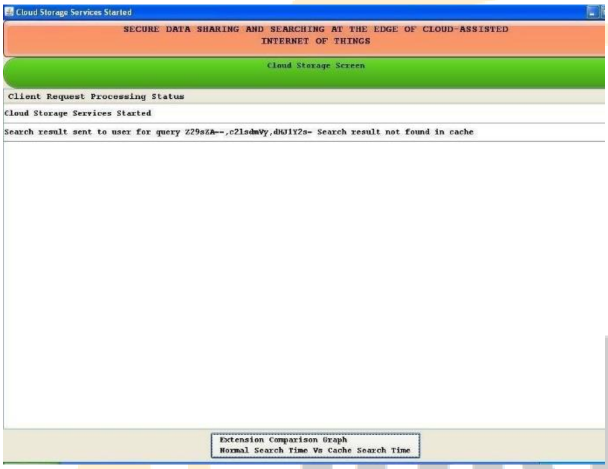


View Search Result

| Username | Filename |
|---|---|
| aaa | a1.txt |
| aaa | a2.txt |
| aaa | a3.txt |

Fig. 4: Search Results of search query.

Above the screen, it is showing the search result in Fig. 4.



Cloud Storage Services Started

SECURE DATA SHARING AND SEARCHING AT THE EDGE OF CLOUD-ASSISTED INTERNET OF THINGS

Cloud Storage Screen

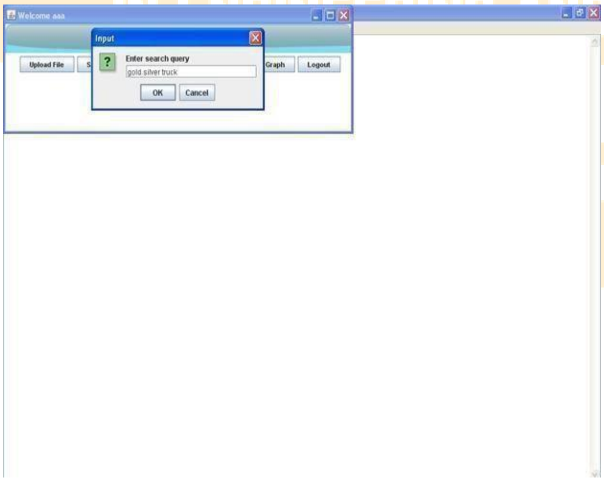
Client Request Processing Status

```
Cloud Storage Services Started
Search result sent to user for query Z29sZA--,c2lsdmVy,dHJ1Y2s- Search result not found in cache
```

Extension Comparison Graph
Normal Search Time Vs Cache Search Time

Fig. 5: Search Results.

In the above screen, Fig. 5 at the cloud side showing status as search not found in cache If I execute the same query again, then Cloud will obtain the result from cache seen in Fig. 6.



Welcome aaa

Input

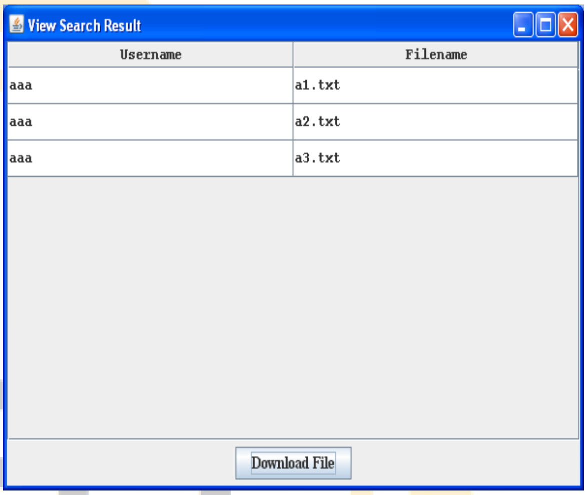
Enter search query: gold silver truck

Fig. 6: Search Again with Cache.

## Results

This is the most important metric, since it measures how long it takes the edge server to search. Cache RAM was added to the edge server to do this. Memory for previously saved data will be created, and the speed of keyword processing will be boosted. Servers benefit greatly when a large text file is uploaded. The first work includes a hash algorithm and a key agreement procedure to provide security as an additional outcome parameter. The improvement shown in the Fig. 8 is compared to the current approach.

Below is a search screen for the result with cache memory saving in Fig. 7.

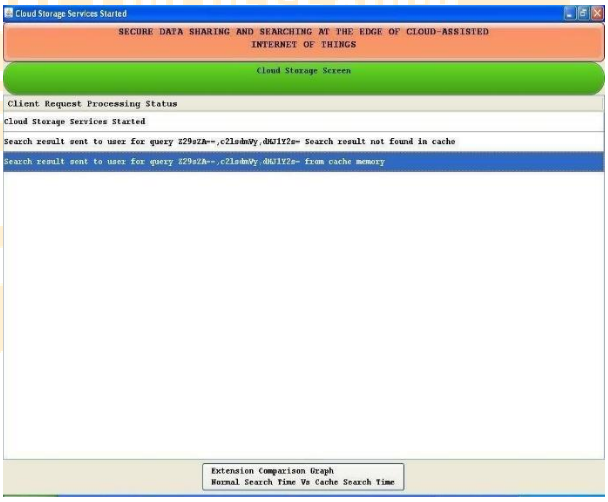


View Search Result

| Username | Filename |
|---|---|
| aaa | a1.txt |
| aaa | a2.txt |
| aaa | a3.txt |

Fig. 7: Results for search from Cache.

At cloud side, can see search status in the below screen in Fig. 8



Cloud Storage Services Started

SECURE DATA SHARING AND SEARCHING AT THE EDGE OF CLOUD-ASSISTED INTERNET OF THINGS

Cloud Storage Screen

Client Request Processing Status

```
Cloud Storage Services Started
Search result sent to user for query Z29sZA--,c2lsdmVy,dHJ1Y2s- Search result not found in cache
Search result sent to user for query Z29sZA--,c2lsdmVy.dHJ1Y2s- from cache memory
```

Extension Comparison Graph
Normal Search Time Vs Cache Search Time

Fig. 8: Result in Cloud Server for search from Cache.

By clicking on the 'Extension Comparison Graph' button, one can see execution time for both cloud complete search and cache search in the visual graph in Fig. 9.

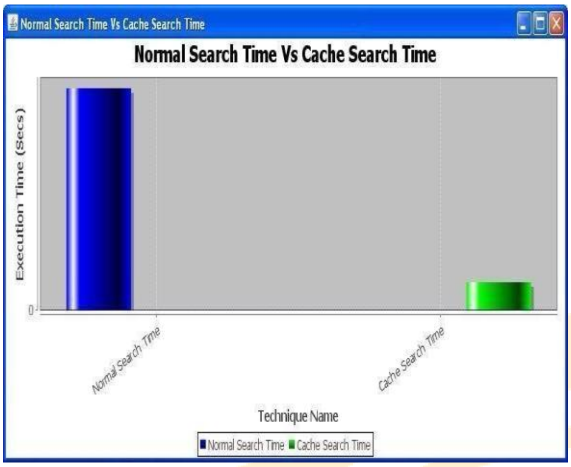


Fig. 9: Result Graph for Faster Speed.

In above graph shows that normal search took from execution time compared to cache search.

## Conclusion

This paper proposes a lightweight cryptographic and speedier framework for IoT-enabled smart phones to exchange data on the cloud's highest level. All security-related tasks are delegated to PCs on the outside of the city. This paper examines the current choices for asset-restricted shrewd gadgets in light of the conditions outlined above. Despite early concerns regarding information sharing security, a data search architecture was developed to find the essential data/sharing data by approved buyers in encrypted databases. Additionally, the security and speedier execution study shows that the proposal is realistic and reduces all companies' expenditures in our framework for count and communication. Encryption has been implemented successfully in all cloud storage types.

## References

[1] Sivannarayana Nerella, G.Sateesh “Confederate Process Key Agreement Scheme for Cloud Assisted Vehicular Internet of Things” International Journal of Research in Advent Technology, Special Issue, March 2019 E-ISSN: 2321-9637.

[2] C. Pravallika, P. Sukanya “Secure Data Sharing and Searching at the Edge of CloudAssisted Internet of Things” International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-8, Issue- 4),2019.

[3] Hind Bangui, Said Rakrak, Said Raghay and BarboraBuhnova “Moving to the Edge- Cloud-of-Things: Recent Advances and Future Research Directions" Electronics 2019, 7, 309

[4] L. Minh Dang, Md. JalilPiran, Dongil Han, Kyungbok Min and Hyeonjoon Moon “A Survey on Internet of Things and Cloud Computing for Healthcare”Electronics 2019, 8, 768.

[5] Sampath Kumar Y R and Champa H N “An Extensive Review on Sensing as a Service Paradigm in IoT: Architecture, Research Challenges, Lessons Learned and Future Directions”International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 6 (2019) pp. 1220-1243.

[6] Sukhpal Singh Gilla, Peter GaDr.K. Praveen Kumarrraghan, RajkumarBuyy “Fogenabled cloud based intelligent resource management approach for smart home IoT devices” Institute of Electrical and Electronics Engineers 2019.

[7] FaguiLiu ,Zhenxi Huang and Liangming Wang “Energy-Efficient Collaborative Task Computation Offloading in Cloud-Assisted Edge Computing for IoT Sensors” Received: 22 January 2019; Accepted: 26 February 2019; Published: 4 March 2019.

[8] ShreshthTulia,b , RedowanMahmuda, , ShikharTuli c, RajkumarBuyya “FogBus: A Blockchain-based Lightweight Framework for Edge and Fog

Computing" International Research Journal of Engineering and Technology (IRJET), Received 2 October 2018 Revised 13 March 2019 Accepted 12 April 2019 Available online 13 April 2019.

[9] FanBi, SebastianStein et al.,"A Truthful Online Mechanism for Allocating Fog Computing Resources"AAMAS 2019, May 13-17, 2019, Montréal, Canad.

[10] Igor Leão dos SantosA, Flávia C. DelicatoB, Paulo F. Pires B, Marcelo PitangaAlvesC, Ana OliveiraD, Tiago SalvianoCalmonD "Data-Centric Resource Management in Edge-Cloud Systems for the IoT "Open Journal of Internet of Things (OJIOT) Volume 5, Issue 1, 2019 ISSN 2364-7108.