ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10 , Iss 2, Feb 2021

Secure Data Sharing and Searching At the The Edge of Cloud Assisted IoT

Rohan Kokate[1], Umesh Samarth[2], Mirza Moiz Baig[3], Chetan Singh Pandele[4]

[12]Assistant Professor, Department of Information Technology, J D College of Engineering & Management, Nagpur
[34]Student, Department of Information Technology, J D College of Engineering & Management, Nagpur

ABSTRACT
Smart gadgets can now communicate from close to a long distance with one another and with the Internet or cloud. As a result, the Internet of Things represents a brand-new paradigm (IoT).
However, by employing cloud computing, resource-constrained IoT smart devices can gain a number of advantages, such as offloading the burden of data processing and storage to the cloud.Working at the network's edge offers more advantages than using the cloud for IoT applications that require high data rates, mobility, and latency-sensitive real-time data processing.
We suggest a productive data-sharing system that enables smart devices to safely communicate data with others at the edge of cloud-assisted IoT .we analyze the performance based on processing time of our proposed scheme.
Because security-oriented operations will increase the heavy computational burden, IoT's resource-constrained smart devices cannot handle these computation-intensive operations.

KEYWORDS: Servers,Smart devices,Cloud computing,Internet of Things,Encryption,Public key,edge computing,extreme edge.

1. INTRODUCTION

The Internet of Things (IoT) is viewed as a future internet that will connect all different types of physical, smart objects in the actual world. On the other hand, cloud resources are scalable, on-demand, and nearly limitless in terms of storage and processing capacity.
IoT smart devices can therefore lessen the load of scarce resources with the aid of the cloud. Smart devices need low latency, high data rates, quick data access, real-time data analytics/processing with decision making, and mobility support in order to run IoT applications. The cloud is unable to satisfy the aforementioned standards due to a number of shortcomings. However, edge computing enhances cloud-as in many ways. The Internet of Things (IoT) will enable developed smart and autonomous cyber-physical environments in the areas of-smart grids,smart cities, smart homes, smart medical and healthcare systems, wearable technologies,transportation systems, etc.
By connecting these billions of smart devices to the Internet.
However, because the majority of these devices are a part of a vast platform, a significant amount of data is produced, necessitating strong computational capabilities for efficient and secure data storage, processing, and analysis. But keeping data processing, communications,

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 10 , Iss 2, Feb 2021

and storage operations on edge servers that are close to the devices at the edge of the networks.
IoT is persisted and fulfills the aforementioned needs the edge servers can act as a middleman for communications across large distances because smart gadgets have a restricted range of connectivity. Any personal or mobile device, standalone server, or network device that is hosted just one hop away from the end devices is considered an edge server. In addition, cloud servers and edge servers work together and have close connections. Data sharing is made available within cloud-aided IoT applications due to the rise in the number and accessibility of smart devices.
If the smart gadgets do not share data with other devices, the data are of limited utility. Smart devices can share data with lower latency, faster data access, and greater bandwidth thanks to data sharing at the edge. Such systems, where huge IoT smart devices are interconnected with high data rates at ultralow latency, will be crucial to the development of the fifth generation (5G) of wireless communications technology. In terms of latency and bandwidth, Yi et al. compare the performance of edge/fog servers with the cloud. The findings indicate that the uplink/downlink bandwidth for fog and cloud servers, respectively, is 83.723/101.918 Mbps and 1.785/1.746 Secure Data Sharing and Searching at the Edge of Cloud Assisted IoT Mbps, while the latencies when utilising fog and cloud servers are 1.416 and 17.989 ms, respectively.
Working at the network's edge offers more advantages than using the cloud for IoT applications that require high data rates, mobility, and latency-sensitive real-time data processing. In this research, we present an effective data sharing system that enables smart devices at the edge of cloud-assisted IoT to safely communicate data with others.
We also suggest a secure searching method to look for desired data among one's personal or shared data on storage. Finally, we evaluate the processing-time performance of our suggested approach.

2. LITERATURE SURVEY

1. Internet of Things in the 5G Era: Enablers, Architecture and Business Model
Authors: L. Xu, X. Wu, and X. Zhang, :CL-PRE
With its wealth of new services built on the seamless interactions between numerous heterogeneous devices, the Internet of Things paradigm holds the potential to ompletely transform the way we live and work. After decades of conceptual development, the Internet of Things (IoT) has recently emerged in a wide variety of communication technologies, reflecting a wide range of application domains and communication requirements. Due to a number of difficult integration challenges, the heterogeneity and fragmentation of the connectivity landscape are currently impeding the full realization of the IoT vision.In this context, the introduction of 5G cellular systems is seen as a potential key enabler for the yet-to-emerge global IoT due to the availability of a connectivity technology that is simultaneously truly ubiquitous, reliable, scalable, and cost-effective. In the current study, we thoroughly examine the potential of 5G technologies for the Internet of Things while taking both the technical and standardized aspects into account. We examine the current state of IoT connectivity as well as the key 5G IoT enablers.

2. Edge-Fog Cloud: A Distributed Cloud for Internet of Things

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved, Journal Volume 10 , Iss 2, Feb 2021**

Authors: A.N. Khan, M.M. Kiah, S.A. Madani, M. Ali, and S. Shamshirband.
Computations The Internet of Things typically entails a sizable number of intelligent sensors that gather data from their surroundings and transmit it to a cloud service for processing. Fog and Edge Secure Data Sharing and Searching at the Edge of Cloud Assisted IoT computing are two architectural abstractions that have been suggested to localize certain processing close to the sensors and away from the main cloud servers. We suggest an Edge-Fog Cloud that distributes task processing across the network's participating cloud resources. In order to assign processing tasks to nodes that offer the best processing time and nearly ideal networking costs, we design the Least Processing Cost First (LPCF) We assess LPCF in several contexts and show that it is efficient in determining the processing task allocations. In this study, we presented the Edge-Fog cloud, a decentralized cloud architecture for managing computation-based, large-scale, and distributable data, such as that produced by the Internet of Things.

3. A Hybrid Approach for Data Analytics for Internet of Things
Authors: S. H. Seo, M. Nabeel, X. Ding, and E. Bertino.
The goal of the Internet of Things is to provide internet connectivity for physical objects that aren't already linked. There will be far more internet-connected devices than there are people on the planet, and they will all be creating data in much greater quantities. These data will be gathered and sent to the cloud for processing, primarily with the goal of discovering actionable information. To increase privacy, provide quick responses to individuals, and utilise less network and storage resources, the data should ideally be evaluated locally. Distributed data analytics might be suggested to gather and analyse the data in edge or fog devices in order to address these issues.we examine a hybrid method, which entails that network level and cloud level processing should collaborate to provide efficient IoT data analytics in order to overcome their individual limitations and utilise their unique strengths. We specifically collected raw data locally, applied data fusion techniques to the data to decrease the data, and then extracted features, sending the features to the cloud for processing. The creation of analysis techniques that can be disseminated and used effectively on low power devices has been mentioned as one important piece of work in the findings section. Exploring the trade-off
between analysis using small (local) data sets and the accessibility of a global perspective will be a significant tactic in this case

4. Security Issues for Cloud Supported IoT
Authors:H. Li, D. Liu, Y. Dai, T.H. Luan, and X. Shen
A popular system paradigm for achieving connections across physical, digital, and social environments is the internet of things. Security concerns emerge when interactions between the internet of things, so it is important to build improved solutions for security measures. Through the use of cloud computing principles, the IoT ideal of open data exchange is realized. IoT has three layers, namely the perception, transportation, and application layers, and because it is based on the Internet, IoT security issues will also surface there. This paper discusses the application layer's security problems, technologies, and solutions. The idea of object security, which introduces security into the application payload, is the foundation of this system. Think of distinct trust domains for authenticity and confidentiality. In order to provide capability-based access control and a defense against communication eavesdropping,

IJFANS International Journal of Food And Nutritional Sciences
Official Publication of International Association of Food and Nutrition Scientists

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10 , Iss 2, Feb 2021

confidentiality is used. This paper discusses the application layer's security concerns and technological solutions. The technique for data security protection at the application layer and a comparison of several data security protection approaches are the major topics of this paper.

3. PROPOSED SYSTEM

We propose a lightweight cryptographic scheme in this paper that allows IoT smart devices to share data with others at the edge of cloud-assisted IoT, where all security-oriented operations are offloaded to nearby edge servers, taking into account the aforementioned limitations of current solutions for resource-limited smart devices. Additionally, even though our initial focus is on the security of data-sharing, we also offer a data-searching scheme to enable authorised users to look for required data or shared data on storage where all data are in encrypted form.

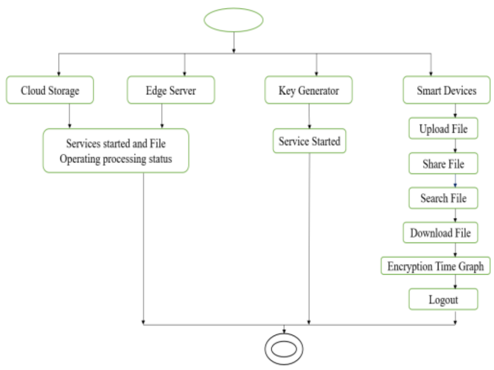

Fig 3.1 Block Diagram

4. SCREEN SHOTS:

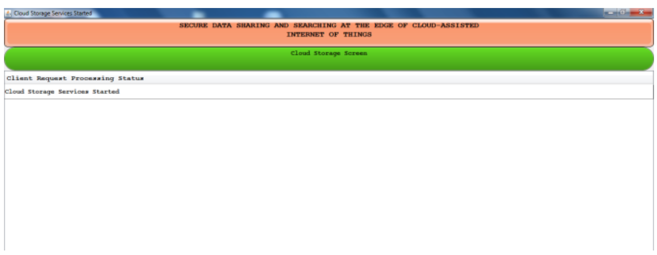

Fig 4.1 Cloud Server

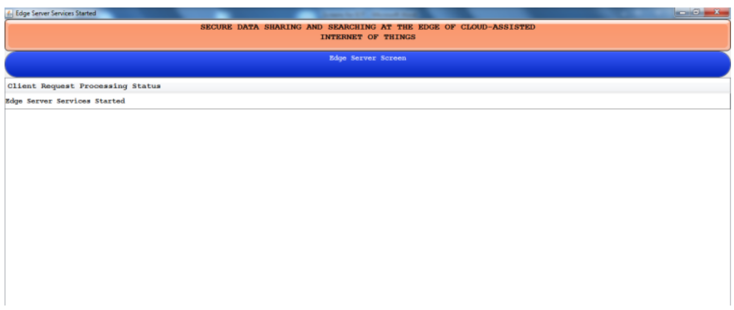

Fig 4.2 Edge Server

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10 , Iss 2, Feb 2021

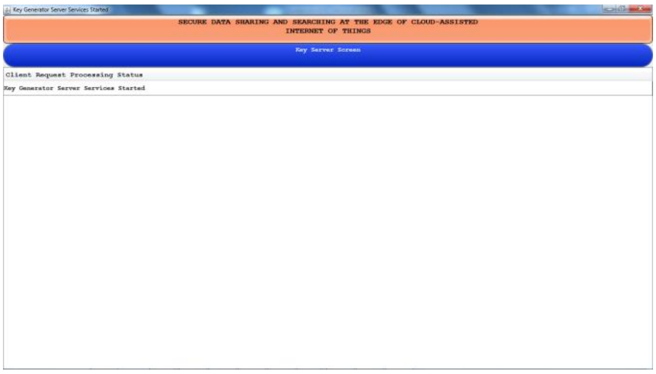

Fig 4.3 Key Generator Server

Fig 4.4 Smart Device Application

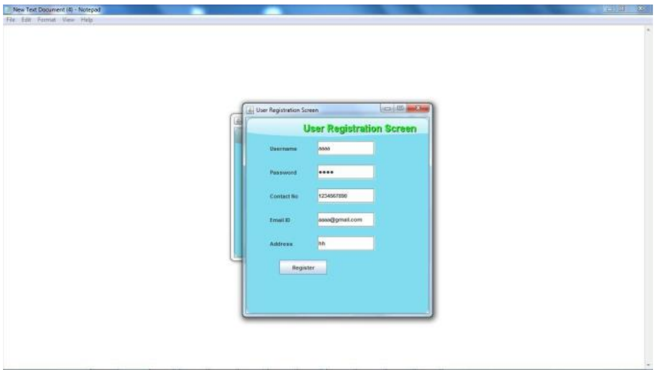

Fig 4.5 Click On Register for User Registration

Fig 4.6 Login as Registered User

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, Journal Volume 10 , Iss 2, Feb 2021

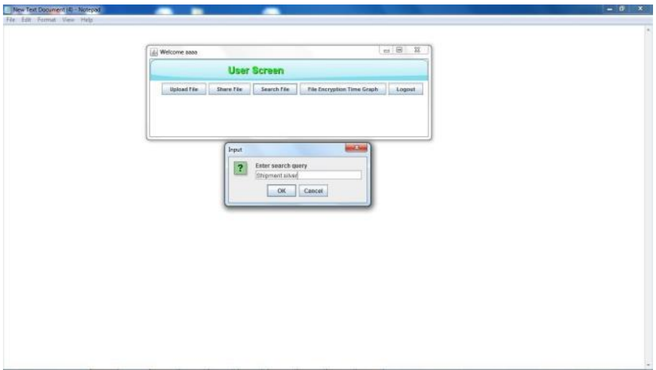

Fig 4.7 User Search Query Screen

5. CONCLUSION

In this work, we present a proposed data-sharing and -searching scheme to share and search data securely by IoT smart devices at the edge of cloud-assisted IoT. The performance analysis demonstrates that our scheme can achieve better efficiency in terms of processing time compared with existing cloud-based systems. In future work, we plan on authenticating and accessing control challenges in this area.

We hope that our proposed scheme is practical to be deployed and opens a new door in edge-oriented security research for cloud assisted IoT applications

6. REFERENCES

1. L. Xu, X. Wu, and X. Zhang, :CL-PRE: A ertificateless 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.
2. A.N. Khan, M.M. Kiah, S.A. Madani, M. Ali, and S. Shamshirband, "Incremental Proxy Re- Encryption Scheme for Mobile Cloud Computing Environment," J. Supercomputing, vol. 68, no. 2, 2014, pp. 624–651.
3. 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.
4. L. Wang and R. Ranjan, "Processing Distributed Internet of Things Data in Clouds," IEEE Cloud Computing, vol. 2, no. 1, 2015, pp. 76–80.
5. 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.
6. 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.
7. 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.

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 10 , Iss 2, Feb 2021

8. H. Li, D. Liu, Y. Dai, and T.H. Luan, “Engineering Searchable Encryption of Mobile Cloud Networks: When Qoe Meets Qop,” IEEE Wire-less Communications, vol. 22, no. 4, 2015, pp. 74–80.
9. F. Li, Y. Rahulamathavan, M. Conti, and M. Rajarajan, “Robust Access Control Framework forMobile Cloud Computing Network,” Computer Communications, vol. 68, 2015, pp. 61–72.
10. 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.
11. H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, “Secure Data Analytics for Cloud Integrated Internet of Things Applications,” IEEE Cloud Computing, vol. 3, no. 2, 2016, pp. 46–56