International Journal for Research in Engineering and Emerging Trends (IJREET), Volume 7, Issue 1, JUNE, 2024
ISSN: 2545-4523 (Online)

A Review on Secure Authenticated Data Sharing using Cloud Computing

1. Anjali Maurya

(Research Scholar, Bhagwant Institute of Technology, Muzaffarnagar, UP, India)

2. Dr. Pushpneel Verma

(Assistant Director, Bhagwant Group of Institutions)

3. Dr. Ajay Singh

(HOD-CSE, Bhagwant Institute of Technology, Muzaffarnagar, UP, India)

Abstract- Most current gadgets have gained the ability to interact with one another as well as with the Internet/cloud across short to long distances in the past few of years. Because of this, the term "Internet of Things" is used to characterise the phenomena (IoT). Using cloud computing to store and process data, IoT smart devices with limited resources may benefit from a variety of benefits, including shifting data storage and processing burden to a distant site (cloud). Instead of relying on the cloud for latency-sensitive and real-time data processing applications, working at the edge of the network offers additional benefits such as increased mobility and high data rates for Internet of Things applications. One of the objectives of this research is to provide a cost-effective data sharing technique that will allow smart devices to securely share data with others at the edge of cloud-assisted IoT while staying cost-effective. Additionally, effort is required to provide a secure searching strategy to search for requested data inside own/shared data on storage that is both efficient and secure to use in order to locate requested data. Finally, assess the overall performance of the proposed system based on the amount of time it takes to process the information it contains. A successful demonstration of the method's potential for use in Internet of Things applications should follow as a natural result. The strategies for safe data exchange using cloud computing are discussed in this study.

Keywords- IOT, Cloud, Sharing, Edge Server

Introduction-

The edge servers may also function as mediators for communications that must take place over long distances, which is advantageous since smart devices have a restricted range of connectivity. [1-5] Those personal computers or mobile devices, as well as stand-alone servers and network devices, that are placed within a one-hop distance of the end devices are included in this category of edge servers [6-8]. Aside from that, the edge servers collaborate closely with cloud servers and keep a close connection with them as well. It is becoming increasingly usual for data to be shared through cloud-based Internet of Things applications, as the number and availability of smart devices continues to expand. [9] The fact that smart devices linked to the Internet of Things (IoT) interact with other devices increases the risk of data leakage, manipulation, integrity compromise, and unauthorised access. Therefore, even when data is shared at the edge, it is vital that the confidentiality, integrity, and access control of such shared information be maintained to avoid data leakage. For approved devices to search for and retrieve information that has been shared with them, it is also necessary to provide a secure data searching method. [14] The difficulties of secure data sharing and searching in cloud settings are now addressed by just a few solutions, which are currently limited in number. To ensure shared data confidentiality, systems based on symmetric key, public key, and homomorphic encryption-based mechanisms are currently being used. [15] Who has access to what is controlled via the use of access control lists and dynamic attributes, which are used in conjunction with access control rules. It is vital to utilise searchable encryption, which is based on symmetric and public keys, in order to locate the required information. [16] All of these systems, in terms of data security, have the bulk of security-oriented processing performed by the device that the user is currently using on the network. This includes encryption, decryption, and access control methods, amongst other things. Because security-oriented operations will place a substantial amount of computing strain on the devices in the Internet of Things, smart devices with limited capabilities would be unable to handle these computation-intensive activities. [18]

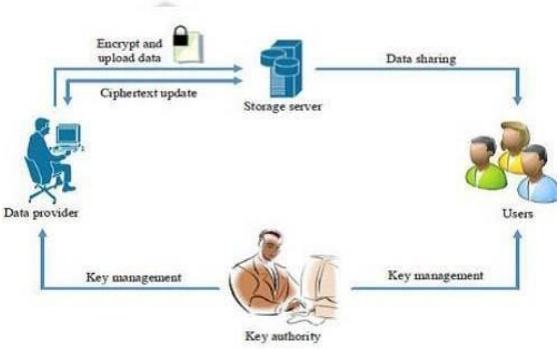

Figure 1. Secure Data Sharing Method [4]

Figure 1 shows the data sharing basic block diagram. The previous author propose a lightweight cryptographic scheme that overcomes the limitations of current solutions for resource-constrained smart devices, allowing IoT smart devices to share data with others at the edge of cloud-assisted IoT, with all security-related operations being offloaded to nearby edge servers. [19] While the initial focus is on data-sharing security, the authors also propose a data-searching approach that enables authorised users to search for necessary data/shared data on storage devices where all data is kept in encrypted form, in addition to the data-sharing security method. Last but not least, our proposed solution is efficient and, according to our security and performance analysis, reduces the computation and communication overhead of all entities that are participating in our system. [20]

Literature Review

It is possible that the Internet of Things paradigm may totally revolutionise authorship's way of life and work with the introduction of an avalanche of new services based on flawless interactions between enormous numbers of heterogeneous devices, as described in this paper. Since the conception and development of the Internet of Things began decades ago, a vast array of communication technologies has progressively emerged in recent years, reflecting the broad diversity of application sectors and communication requirements that exist. In part due to the diversity and fragmentation of the connection environment, the full implementation of the Internet of Things idea is presently delayed by the presence of a number of key integration difficulties that must be addressed. This is why the introduction of 5G cellular systems, which will provide truly ubiquitous connectivity at the same time as being dependable, scalable, and cost-efficient connectivity at the same time, is seen as a significant potential driver for the global Internet of Things, which is still in its early stages and has not yet emerged. The author of this paper delves into the prospects of 5G technologies for the Internet of Things, taking into consideration both the technical and standards aspects of the technology. An examination of the present condition of the Internet of Things (IoT) connectivity environment, as well as the major 5G enablers for the IoT, is provided by the author. Finally, the author demonstrates how a strong interaction between IoT and 5G has the potential to cause significant business disruptions in the operator and vendor ecosystems.

With superior Radio Resource Management (RRM) algorithms working in tandem, the global coverage delivers a degree of stability and reliability that is unsurpassed by any other competing technology now available on the market. [1]

Figure 2. Cloud Data Sharing Registrations and Process

Figure 2 shows the cloud sharing processes and there is a need to add security in the above method for processing. The author employs a variety of scenarios to evaluate the effectiveness of LPCF in identifying processing task assignments, the results of which are subsequently presented. The author also discusses a variety of challenges that may have an impact on the real-world deployment of the Edge-Fog cloud, including but not limited to: [2]

The Internet of Things anticipates a future in which physical goods that are now not connected to the internet will be able to be connected to the internet in the near future. In the future, there will be an extraordinarily large number of internet-connected devices, much more than the number of human people on the world, all of which will be producing data at the same time at the same rate. These data will be acquired and transmitted to the cloud for analysis, with the purpose of uncovering meaningful information that can then be utilised to take appropriate action in response to the findings. However, in order to increase privacy, respond to people in a timely manner, and reduce the use of network and storage resources, it is preferable that the data be reviewed locally. It is possible that distributed data analytics will be supplied in order to acquire and analyse data at the edge or in fog devices, as well as in the cloud, to solve these concerns. This research's authors argue that a hybrid strategy should be used to construct successful IoT data analytics, which means that both network level

processing and cloud level processing should collaborate in order to overcome their respective limitations and capitalise on their respective advantages. The author acquired raw data locally and retrieved features using data fusion techniques on the data collected on resource limited devices in order to reduce the data size. The recovered features were then uploaded to a cloud for further processing, which was then finished. The accuracy and data consumption of the network were investigated by the author, and the findings show that it is feasible to increase privacy while keeping accuracy while reducing the amount of data sent.

This study proposes a hybrid approach in which data is fused in the fog before being transmitted to the cloud, with the goal of reducing data transmission over the network. The results reveal that this architecture is successful in terms of minimising the cost of data transmission over a network while maintaining the accuracy of future decision-making processes to a significant degree. The author has offered the proposed approach, as well as the associated methodology, for consideration. In addition, the author made use of the WISDM dataset to assess our concept. Future research will build on the promising findings presented in this paper in order to improve (or at least maintain) accuracy while simultaneously reducing data communication. This will be accomplished by developing different features and algorithms for better data aggregation and, as a result, further reducing data communication. Among the significant pieces of work mentioned in the results section is the development of analytic algorithms that can be distributed and operate efficiently on low-power devices, which is an essential step forward. One strategy that will be useful in this circumstance is the identification of the ideal balance between the study of limited (local) data sets and the availability of a comprehensive picture of the situation, which will be important. In addition, future research will involve an analysis of energy consumption as well as consideration of the positive impact on privacy that may be gained as a result of this technology. [3]

With the Internet of Things (IoT), we will see an explosion in the number of endpoints, but there will be other benefits as well. As a result, there are many unfavourable repercussions.

According to the author, use cases that demonstrated the need for Fog were investigated, with the relevance of Fog being highlighted in a number of industries within the Internet of Things and Big Data arenas. A high-level overview of Fog's software architecture was also provided by the author, who emphasised the many technological components that are necessary in order to complete the objective of Fog [4] Concerns about the security of cloud-based Internet of Things systems

It's no secret that the internet of things is swiftly becoming a popular system paradigm when it comes to creating connections across physical, electronic, and social domains. Security problems become increasingly prevalent during the interactions between internet-connected devices, and it is necessary to build more powerful security protection solutions to address these concerns. The Internet of Things concept of open data exchange is brought to fruition via the use of cloud computing technologies. For this reason, and since the Internet of Things is built on top of it, the security vulnerabilities that have plagued the Internet will present themselves in the IoT, which is divided into three layers: the perception layer, the transportation layer, and the application layer. This article examines the security challenges, technologies, and solutions that are important to the application layer at the network layer, as well as the application layer at the application layer.

The security architecture and issues associated with the Internet of Things (IoT) have been investigated, and the IoT has been divided into three layers: the perception layer, the transportation layer, and the application layer. A description of each layer's features and security concerns has been given, as well as information on the common treatments for these difficulties. There is a concern with the security of end-to-end connections in the Internet of Things. On the concept of object security, it is based, and while the programme is being performed, it provides security to the payload of the programme. Consider separating the trust domains for secrecy from the trust domains for legitimacy. In order to provide capability-based access control as well as protection against eavesdropping while a communication is in progress, confidentiality is used in conjunction with other security measures. This article examines the security concerns and technology solutions that apply to the application layer of the network, as well as the implications of these solutions. Data Security Protection methods for the application layer, as well as comparisons between various Data Security Protection methodologies, are the key topics covered in this article.[5]

Cloud computing has seen remarkable growth in recent years as a consequence of its ability to provide consumers with elastic, adaptive, and on-demand storage and processing services, among other benefits. A key component of the cloud-based storage concept is the fact that the data is stored by a third party, referred to as cloud service providers, and that the data owner does not have total control over his or her own data (CSP). In the cloud, when a data owner shares his or her own data with another person, known as a data sharer, data security becomes a challenging problem to handle. Fortunately, there are solutions. There have been

several attempts to tackle this issue via the use of cryptography, which includes a number of encryption techniques that allow for the secure transfer of information over the internet. According to this paper, the author proposes a system model for secure data sharing on the cloud, with the goal of ensuring data confidentiality, access control of shared data, removing the burden of key management and file encryption/decryption on users, supporting dynamic changes in user membership, and requiring the owner to be online at all times when a user requests access to the data.

As a result of the ease with which services may be provided and dispersed while requiring the least amount of administrative work or service provider interaction for the services that consumers seek, cloud computing is quickly becoming the dominant paradigm. Data confidentiality, access control, scalability, user revocation, and the ability to rejoin a group after being ejected are all requirements for cloud-based data sharing security. Therefore, the author proposed a system architecture for safe data sharing on the cloud that ensures data confidentiality, access control of shared data, relieves users of the burden associated with key management and file encryption/decryption, supports dynamic changes in user membership, and is simple to implement. When a friend seeks access to a data set, the owner should not be online at the moment the request is made. [6]

For the safe sharing of sensitive information and data in public cloud settings, the authors are proposing a mediated certificate-less encryption system that does not need pairing procedures and does not require the use of certificates. With mediated certificate-less public key encryption, the solution to the key escrow problem that occurs in identity-based encryption, as well as the certificate revocation problem that exists in public key cryptography, is offered (mCL PKE). For their part, existing multichannel symmetric key exchange (mCL-PKE) encryption systems are either inefficient owing to the use of expensive pairing procedures or vulnerable due to the use of expensive pairing operations. For the purpose of describing the performance and security challenges, the author has first supplied a mCL PKE scheme that does not need the usage of pairing processes in order to accomplish this task. The authors are now working on developing a practical solution to the issues involved with transferring vital and secret information in public clouds, which will make use of our mCL PKE approach. The cloud is used to store security information and generate keys, which are both important functions. By encrypting his sensitive data before uploading it to the cloud and using the cloud-generated users' public key, which is based on the cloud's access monitoring restrictions, the data owner ensures that his sensitive data is safeguarded by a powerful encryption method. Users who have been successfully authorised have their sensitive data partially decrypted in the cloud after the completion of the successful authorization process. In order to decrypt the data in its entirety, the user will need to apply the private key that has been handed to him. As a second benefit, our superior approach allows for a single encryption of every data item for a large number of users who are all subject to the same access control limitations, thereby decreasing the overall load on the data owner. [7]

Currently available technologies have limitations when it comes to delivering high efficiency and accuracy when it comes to providing analytic services for encrypted data over a cloud platform; nevertheless, models have been created to address these limitations.

Cloud computing technology has a number of benefits, but it also has a number of drawbacks that must be considered before using it. We're talking about a computer architecture in which both data storage and data processing take place outside of the mobile device when we say "cloud computing." An introduction to Internet of Things Technology, as well as an explanation of how it works and how it is utilised, are provided in this article by the author. In addition, the author covers the key aspects of cloud computing, as well as its advantages and disadvantages, in detail. Data storage and processing take happen outside of a mobile device while using cloud computing, which is a word that refers to an infrastructure that uses cloud computing. Furthermore, the Internet of Things (IoT) is a new technology that is rapidly gaining root in the field of telecommunications, notably in the present sector of cellular telecommunications, as well as in several other disciplines, including the medical profession. As a group, rather than as individuals, the interaction and cooperation of objects and products that communicate across wireless networks serves the main function of achieving the objective that has been defined for them rather than as individuals. Furthermore, as a result of developments in wireless network technology, both Cloud Computing and the Internet of Things are evolving at a rapid rate. A look into the Internet of Things (IoT) and Cloud Computing is provided in this article, with a special focus placed upon some of the security issues involved with both technologies. The author also mixes the two technologies mentioned above (Cloud Computing and IOT) in order to study the parallels and contrasts between them, in addition to uncovering the benefits of integrating the two technologies together. [8]

A general trust management paradigm was designed by the author of this research with the purpose of supporting agents in judging the trustworthiness of their partners. In this part, the author undertakes a

simulation with the purpose of providing an example of food nutrition analysis. It illustrates how depending on confidence may reduce the amount of analytical mistake that is produced

The author uses two measures to evaluate trustworthiness and confidence: the measure of trustworthiness (m) and the measure of confidence (c) (c). Through the use of measurement theory, we may develop a paradigm that regards agents' trust evaluations and interactions as measurements. Furthermore, the author argues that agents can appraise one another through engaging with them in a variety of circumstances, which is consistent with previous research. Also included is a list of several hypothetical circumstances and qualities that might impact trust relationships in Internet of Things systems, which the author believes are important to consider. In order to be applicable to a broad variety of Internet of Things applications, our trust management architecture has been intended to be generic and scalable. The author utilises a food nutrition analysis in the context of diabetes treatment as an example to show the usefulness of our trust management technique in order to better elucidate this. Several studies have shown that patients may benefit from trust in order to filter out erroneous information or reduce the consequences of receiving incorrect information. Also included are illustrations of two other types of attacks by the author. Through the demonstration of these two different types of attacks, the author can explain how critical it is for Internet of Things systems to choose and weight their settings correctly. [9-10]

Conclusion

In this article, the works from the previous year that were connected to cloud computing, the internet of things, and security based on these topics are evaluated. The article has been examined, and it has come to the conclusion that there is a present need for the development of cloud sharing and security of IOT-based solutions. Given that smart devices linked to the Internet of Things (IoT) transmit data with other devices, there is the chance that information may be compromised, such as via data leakage, manipulation, integrity, or unlawful access. Therefore, even when data is shared at the edge, it is vital that the confidentiality, integrity, and access control of such shared information be maintained to avoid data leakage. For approved devices, it is also necessary to provide a secure data-searching mechanism that allows them to search for and retrieve data that has been shared with them. The difficulties of secure data sharing and searching in cloud settings are now addressed by just a few solutions, which are currently limited in number. Currently, encryption-based procedures such as symmetric key, public key, and homomorphic encryption are often used to ensure the privacy of shared data.

Table 1 Review of Previous Work

S.NO	AUTHOR	PROBLEM	AREA OF APPLICATION	FINDINGS	FUTURE RESEARCH
1.	Athanasios Vasilakos, Md. Abul Kalam Azad, Muhammad Baqer Mollah[4]	security issue while searching and sharing of data by the smart devices	secret key encryption and public key encryption	provides better efficiency in case of processing time	work on access control and authenticating issues
2.	Hai Jin, Peng Xu, Ye Tao[11]	leakage of data in CECS due to safety issue in cloud and edge servers	public and private key pair and SE encryption	ensures confidentiality and reduces computing overhead	Not Addressed
3.	C. Pravallika, I. Bhanu Prakash, P. Sukanya[6]	security of data at the edge of cloud supported IOT	implemented CTAC model	assured security achieved with the model	compairtive analysis of presented CTAC model
4.	Dhanabal Thirumoorthy, Tucha Kedir, RabiraGeleta, Abdul Kadir[12]	framework required to provide security in Datain Cloud based services using IOT	encryption and decryption algorithms	better performance achieved and gadgets attached to the servers slowly get bottleneck	Not Addressed
5.	Jorge Bernal Bernabe, Antonio F. Skarmeta Gomez, Jose Luis Hernandez Ramos[2]	need for reliable communication and adaptable mechanism between multiple devices	Architectural Reference Model	considerable performance achieved in trust values	proceed further to measure the accuracy
6.	Quin Li, Shanhe Yi, Zhengrui Qin, Zijiang Hao[14]	facing challenges in using cloud	Fog computing architecture	low latency and high bandwidth	plan for imposing full fog platform
7.	Abdulatif Alabdulatif, Zahir Tari, Ibrahim Khalil, Heshan Kumarage,Xun Yi[3]	requirement for security cloud supported data analytics system for IOT	homomorphic encryption	capable of performing analysis on ciphertext	nature of data processing models and analysis tasks
8.	Athanasios V. Vasilakos, Revathi Dhamotharan, Sameer U. Khan, Albert Y. Zomaya, Keqin Li,Mazhar Ali, Eraj Khan[1]	threats to the cloud storage which leads to leakage of data	SeDaSC	access controls for malicious insiders, confidentiality	extended by limiting the trust level

References

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

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

[3] M. Satyanarayanan, P. Simoens, Y. Xiao, P. Pillai, Z. Chen, and K. Ha, "Edge Analytics for the Internet of Things," IEEE Pervasive Computing, vol. 14, no. 1, 2015, pp. 24–31.

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

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

[6] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A.V. Vasilakos, and K. Li, "SeDaSC: Secure Data Sharing in Clouds," IEEE Systems Journal, vol. 99, no. 1, 2015, pp. 1–10.

[7] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption Protocol for Secure Data Sharing in Public Clouds," IEEE Transactions on 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 Cloud-Integrated IoT Applications," IEEE Cloud Computing, vol. 3, no. 2, 2016, pp. 46–56.
[9] TACIoT: Multidimensional Trust-Aware Access Control System for the Internet of Things, J.B. Bernabe, J.L.H. Ramos, and A.F.S. Gomez, Soft Computing, vol. 20, no. 5, 2016, pp. 1763–1779.
[10] F. Li, Y. Rahulamathavan, M. Conti, and M. Rajarajan, "A Robust Access Control Framework for a Mobile Cloud Computing Network," Computer Communications, vol. 68, no. 1, 2015, pp. 61–72.
[11] Arun K Mani, Shreevani D, Samra said, M. Gokilavani, and Unnikrishnan K N, "A Review: IoT And Cloud Computing For The Future Internet," International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, Volume: 06 Issue: 05 | May 2019.
[12] Sabeen Javed, Hammad Afzal, Muhammad Babar, and Fahim Arif, "An Attack-Resilient Cloud-Assisted IoT System." IEEE Access, 10.1109/ACCESS.2019.2897095, Institute of Electrical and Electronics Engineers.
[13] P. Har I Naveen, K. Viswaprasad, "Secure Data Sharing and Search at the IoT's Cloud-Assisted Edge" DECEMBER/2018 International Standard Serial Number (ISSN)
[14] Soujanya, A.V., Budur Dr.Aradhana.D,Shruthi.P,Sushmitha.P.T,Naveen Kumar Reddy "With The Aid Of The Internet Of Things, Reliable Data Sharing And Searching At The Cloud's Edge" Volume 10 / Issue 1 / MAY 2018. International Journal Of Professional Engineering Studies.
[15] Sneha Sureddy, K. Rashmi, R. Gayathri, and Archana S. Nadhan Sneha Sureddy, K. Rashmi, R. Gayathri, and Archana S. Nadhan "Flexible Deep Learning for Edge Computing in the Internet of Things" International Journal of Pure and Applied MathematicsVolume 119, Issue 10 (October 2018), pp. 531-543.
[16] Abhishek Jaiswal, Mohit Kumar Nayak, "Reducing the Computational and Communication Costs of IoT Smart Devices Using a Lightweight Cryptographic Scheme" Volume 7, Issue XI of the International Standard Serial Number (ISSN), November 2018.
[17] [PawaniPorambage "Analysis of Multi-Access Edge Computing for the Realization of the Internet of Things" IEEE,
[18] GopikaPremsankar, Mario Di Francesco, and TarikTaleb, "Edge Computing for the Internet of Things: A Case Study," Institute of Electrical and Electronics Engineers, 2018, IEEE.2805263.
[19] G. DhanaSekhar, D. Pavan, and A. Akill Kumar, "Mobile Relay Configuration in Wireless Sensor Networks."
IJSRCSEIT | Volume 3 | Issue 4 | ISSN: 2456-3307 | International Journal of Scientific Research in Computer Science, Engineering, and Information Technology | 2018 IJSRCSEIT
[20] "A Survey on Edge Computing for the Internet of Things" by Wei Yu, Fan Liang, Xiaofei He1, William Grant Hatcher1, Chao Lu, Jie Lin, and Xinyu Yang. Accepted November 18, 2017, date of publishing November 29, 2017, date of current version March 9, 2018. Received October 20, 2017, accepted November 18, 2017, date of publication November 29, 2017, date of current version March 9, 2018.