JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhanced encryption Model in Fog Computing with Data Fragmentation

Manish Kumar
M. Tech. Student, GITAM, Jhajjar
(M. D. University, Rohtak)
kumar.manish1161997@gmail.com

Dr. Ritu Kadyan
Associate Professor, GITAM, Jhajjar
(M. D. University, Rohtak)

Abstract - **Data security in conventional applications was only available at the application layer. The package's security is guaranteed in the planned study. The necessity for a new security system emerged as a result of the shortcomings of existing security systems. Without authentication, there should be less chance of decryption. The establishment of decentralized security is necessary to fend off attacks from various networks. According to claims, the proposed encryption standard will enhance multilayer security. This technique divides the content into two pieces and offers a trustworthy transmission mechanism. Hackers cannot weaken the security system thanks to the system. To stop attackers, security was required in a cloud and edge environment. The two fish technique was created to improve data transmission security and dependability over various networks. Its security system has helped it withstand hacker or cracker attacks. The proposed article suggests a study on the security of slicing-based edge transmissions. To stop attackers from attacking from many networks, decentralised security must be developed. Layered security will also strengthen strong encryption standards. Computer security edge generators have been the subject of numerous investigations. Many of these have already been talked about. The suggested study divides the data into two pieces that are additionally encrypted at various levels in order to create a trustworthy transmission technique. Multilayer encryption has evolved, improving the security and dependability of data transmission via networks. By using this method, the security system became impervious to hacker and cracker attacks.**

Keywords— Edge computing, Data Security, Data Slicing, Two Fish Algorithm.

I. INTRODUCTION

The advantages of big data are becoming more and more apparent to businesses and governments. In actuality, efficient Big Data mining enables value and competitiveness to be increased in numerous areas. Big Data is primarily recognised for its 3Vs. Velocity, variety, and volume are the 3Vs. To prove that a significant data source is the source, all three of those characteristics must be present. In the absence of one of these three Vs, we are unable to discuss big data. Victory, Verification, Validation, Value, Complexity, and Immutability are additional Vs and traits that some big data firms have added to further define them. In addition, some believe that a large proportion of digital data sets are Big Data by definition since we can no longer access them effectively and analyze via existing technology and infrastructure.

Safety issues in the environment are the main topic of this chapter. To ensure the management of several information systems, we offer some technology, practises, and solutions. Big data security is similar to traditional information system security in many aspects.

However, stronger instruments, suitable methods, and advanced data processing technologies are required. It requires a new security management paradigm that manages both internal and external data simultaneously.

It requires a new security management paradigm that manages both internal and external data simultaneously. Several queries may be posed in connection to such issues: i)What techniques can I use to manage and analyse vast and unstructured data? ii) How are distributed systems with high performance safety measures integrated? iii) How can massive data streams be analysed without compromising privacy?

To make sure that data transfer is secure, a secure cryptographic mechanism is built. The study's findings suggested utilising data slicing to split the edge data [3] into two tiers for security concerns. As the data is separated into many sections for transmission, the relative chance of data loss during transmission is likewise decreased. Port numbers and IP addresses were provided during the investigation, and the suggested model also offers session-level security[4]. The historic and proposed works were contrasted as well. Splitting data into two sections was discovered to be helpful to lower the danger of losing the full data in single attempt transmission network during the comparison of several criteria including integrity, dependability, data security, confidentiality, path congestion in transmission networks, port number, and others. In terms of secure data transmission, this study will unquestionably be effective and valuable. The proposed strategy offered a more effective and narrowly targeted way to defend the data from attacks that are application level oriented. The suggested system was compared with an existing system during the research study based on many parameters. It has been shown that conventional security methods are less effective. The suggested model approach secures the data by separating, slicing, and encrypting it with a cutting-edge algorithm for cryptography that has a track record of success. In order to maintain security on multiple levels, this study explores numerous dangers that could arise [5,6]. The suggested

method divides the data into different pieces to secure it. Due to the shortcomings of the current conventional system, a brand-new system was necessary. The suggested system will work to meet the functional and security requirements for the current system.

II. Literature Review

The safety points that are crucial to a data transmission have been the subject of numerous research. Below, we've included them in brief summaries:

A secure, hierarchy-based cloud storage method depending on FOG Computing was presented by Jiyuan Zhou in 2017 [4]. In the foggy environment, the agreements as mentioned were crucial in preserving the data stored in the cloud. In our investigation, it was discovered that putting such a system into practise would be quite expensive and challenging.

Abbasi Bushra Zaheer 2017 saw [5] take into account the flaws, reliable techniques, and fixes in fog computing. This article does a wonderful job of describing fog computing's architectural design and execution. Additionally, it demonstrated how fog computing was being used globally in various real-time systems. The paper's main goal was to identify architectural constraints and weaknesses that could be exploited by hackers to damage the system. Further investigation revealed that, according to the most recent sophisticated security domain tools, some sections of the research done by researchers to accomplish security features are missing. K. Shenoy began researching fog computing in 2015 in relation to the future of cloud computing [9]. Cloud service companies deal with numerous challenges. The privacy and security of stored user data is one such issue. The ongoing rise in data breach attacks makes it a concern. Fog computing allows for the monitoring of users. As a result, user data security must be offered to maintain organisational compliance standards.

The future of cloud computing, according to Mohamed Firdhous and others in 2014 [10], will revolve around fog computing. They did take into account that the cloud computing paradigm, which is the most recent in computing, will make resources available for computation, storage, etc. over the Internet is based on pay per use basis.

In 2017, [11] Leonard Dervishi and Nabil Abubaker developed a new fog computing paradigm that supported privacy protection. The end user or IoT device should be able to be reached in fog computing, and using the normal methods, confidentiality should be provided. This was the initial problem. The public availability of the end user was the second problem. The researcher positions these problems in relation to the requirements of the real world and offers a fog computing system that resolves them.

Data security and fog computing confidentiality were both emphasised by Jun Shao and Yunguo Guan [12]. Mechanisms needed to handle information security and privacy issues are the main Fog computing problems.

In the framework of cloud computing, H.S. Guruprasad and B.H. Bhavani [13] investigated resource provisioning techniques. In most systems, there are numerous options for resource allocation. However, static and dynamic are the two main categories. Every allocation scheme has advantages and disadvantages.

M. Georgescu [14] investigated cloud computing from a business standpoint. Profits can be produced by using these resources in the right way. With the aid of storage technologies, cloud installation enables easy access from anyplace, enabling us to modify the Business based on capacity and requirements, along with significantly enhancing decision-making abilities.

The architecture of the load balancing mechanism in the FOG computing environment was highlighted by N.Bhardawaj and M. Verma [15]. It is crucial to improve the portability of such services across the various platforms because fog computing devices are geographically dispersed across several platforms. The traffic light control system is one example of a real-world issue that edge computing can resolve. Independent edge nodes can establish a direct connection with the cloud or a client.

P. Pazowski conducted a thorough investigation in 2013 [16] to identify the best IS/IT system for use with cloud computing. During the investigation, he presented the conventional strategy using an IT supply chain management system in a SaaS format. It was completed within the constraints of the ownership cost. After establishing TCO, the author can use cloud computing and analyse financial ratios like capital value, return on investment, and payback duration.

S. Malkowski [17] discussed the difficulties and possibilities of the consolidation of excessive resource use. Depending on the approach, we can evaluate and quantify resource utilisation directly. The author assessed the results for two integrated n-tier application benchmark systems as well as request rates in an environment of enterprise level computer virtualization technological system.

III. Objectives Of Research Study

The proposed work's goal is to provide security against various application layer threats, which occur when a user interacts with the network directly. The most used protocols at the application layer include HTTP, TELNET, FTP, and others. The primary goal of research is to develop an application layer system that is more effective and efficient in terms of time.

The proposed work aims to offer defence against different application layer assaults, where the user interacts with the network directly. The three most popular application layer protocols are HTTP, TELNET, and FTP. The creation of a time- and safety-effective system is the study's principal objective. The following are the overall goals of this study:

- To learn more about various risks, such as active and passive attacks.
- Providing network security through the use of cryptographic methods.
- The creation and application of a secure technique to protect user data at the application layer from active and passive threats.
- Using data slicing to separate the data into pieces and offer data security during transmission and upon receipt.
- Comparing observable details of the proposed system under consideration with those of the current system to demonstrate why the proposed system will be easier to operate.

IV. Proposed Work

The proposed effort aims to identify a more narrowly focused method to strengthen the protection of data from a variety of assaults, including active and passive attacks, at the application layer. The proposed work and the security techniques that are currently in use were compared

throughout this investigation. Traditional security measures proved to be less effective. By adopting a tried-and-true, hack-proof cryptographic methodology to slice and convert data into cypher text, the proposed method strengthened the defence of data.

The planned study also looked at how active and passive threats could improve security at different tiers. The need for such a system was necessary because traditional security systems had their limits. Here, the IP filter is used to reject and disregard unauthenticated requests for data transmission from the cloud server and edge node to the client system. On top, an enhanced encryption mechanism works to fortify the defence. By breaking up the data and encrypting each piece, the suggested technique achieves data security. The procedure for securing data during transmissions is detailed below:

When a request for data is received by an edge node, the edge node will perform the following actions:

Input the plaintext.

- Utilising the validation code, perform the XOR transformation, and then store and provide the output to another module.
- To create encrypted data using information from the preceding operation, initialization vector, and symmetric key, follow these steps:
- Generate Initialization Vector
- Generate a Symmetric Key
- Apply the Two Fish Algorithm.
- The data slicing module is then given the cypher text.
- The cipher text will be split into two halves by the data slicing function.
- • Send a portion to the cloud server and a portion to the client immediately.

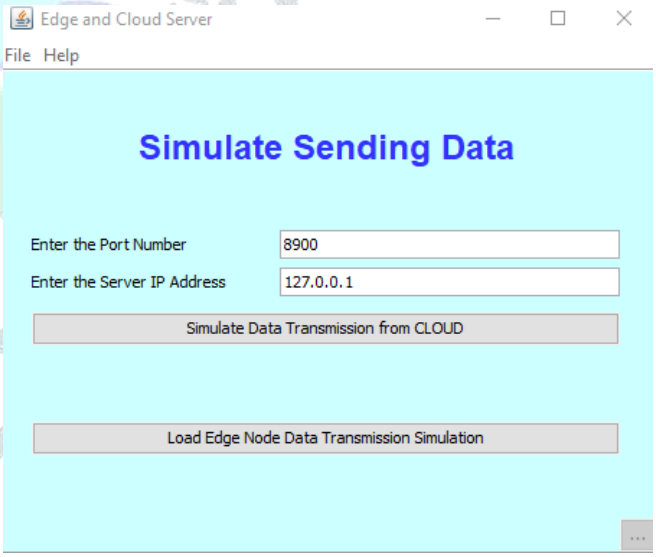
At the client site the following procedure is followed-

- Download the file that was transferred from the cloud server.
- Take the file that was transferred from the edge node.
- Combine the content of the two files.
- Obtain the symmetric key and initialization vector explicitly.
- Use the Two Fish algorithm to decode the data after it has been combined, passing the initialization vector and the symmetric key together with the cypher text.
- After that, the result is given to an XOR-based transform function utilising the explicit authentication code.
- In this manner, the ciphertext can be used to create the plaintext.

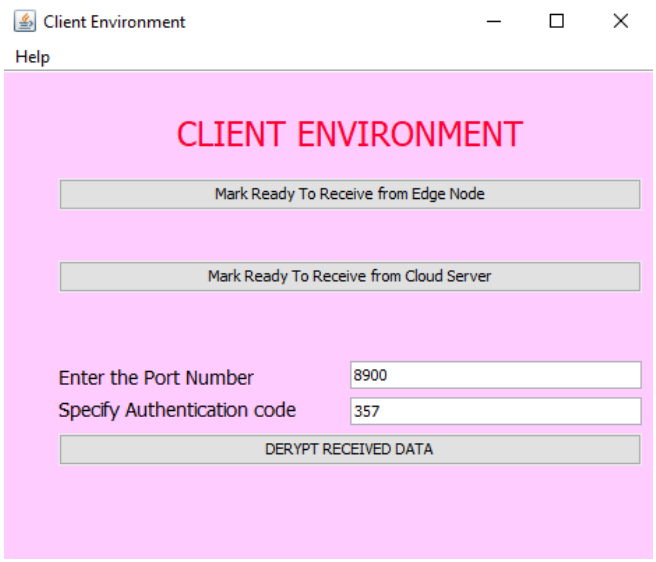
V. Implementation And Results

(Fig. - Data Slicing Module)

(Fig.- Simulate Data Sending from Edge Node)



(Fig.- Simulate Data Sending from Cloud Server)



(Figure – To generate original Plain Text from Cipher Text at the Client End)

Factors	Traditional Model	Proposed Model
Support for FOG	Do not support FOG integration.	The work uses FOG integration.
Congestion	Chances of congestion are high.	Chances of path congestion are low because the data is transmitted by two paths.
Reliability	Less reliable	More reliable
Port number	Static defined ports	User defined ports
Security	Uses only SSL which is also vulnerable to attacks like BEAST, BREACH, FREAK and Heartbleed etc.	Uses multilayer security including the Two Fish Algorithm which has no vulnerability and is quantum safe too.

Time Comparison	Testing System RAM – 4 GB		
Plain text (in KB)	AES (in ms)	Two Fish (in ms)	Proposed (in ms)
111	491	316	348

Size Comparison	Testing System RAM – 4 GB		
Plain text (in KB)	AES (in MB)	Two Fish (in KB)	Proposed (in KB)
111	148	108	108

VI. Conclusion

Compared to previous implementations, the proposed approach ensures a better safeguard approach to preserve and protect the data from a variety of application-layer attacks. The proposed security model was also put up with existing security model during the research. The proposed system used advanced cryptographic mechanisms to segregate and encrypt data to safeguard it whose details are described and discussed above. The proposed system proved to be reducing the possibility of path congestion and a data security breach. The study of various potential threats was done for making sure that the security on various different levels maintains and continues. In particular, the proposed method successfully shielded and fortified the data security by multilayer encryption and dividing the data into parts for transmission through different paths in an edge computing environment.

VII. Future Scope

A fully holistic security solution has yet to be developed to satisfy all the required security mechanisms that can work on a wide range of objects in the domain of Edge or IoT devices. To add new devices, their safety in each part must be ensured in different day to day applications. The key issue in the edge computing system is to decentralize security.

Although a lot of solutions are in developmental phase, but using Blockchain with the proposed work can prove to be a good candidate for the optimal overall solution addressing various issues including the proper security in the Edge Computing Environment.

References

[1] Mahmud, R., Kotagiri, R., & Buyya, R. (2018). Fog computing: A taxonomy, survey and future directions. In *Internet of everything* (pp. 103-130). Springer, Singapore.

[2] Kunal, S., Saha, A., & Amin, R. (2019). An overview of cloud-fog computing: Architectures, applications with security challenges. *Security and Privacy*, *2*(4), e72.

[3] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*, *6*(1), 1-22.

[4] Dolui, K., & Datta, S. K. (2017, June). Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

[5] Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., Morrow, M. J., & Polakos, P. A. (2017). A comprehensive survey on fog computing: State-of-the-art and research challenges. *IEEE communications surveys & tutorials*, *20*(1), 416-464.

[6] Vishnu S.N. , Kavitha P.B. , N.M. murthy , P. Kasana , 2016, A research study on the fog computing for data security, ISSN 2394-1537 Vol. 5,Specail Issue No.01, pp. 221-227, February 2016

[7] Zhou, J., Wang, T., Bhuiyan, M. Z. A., & Liu, A. (2017, November). A hierarchic secure cloud storage scheme based on fog computing. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 470-477). IEEE.

[8] Abbasi, B. Z., & Shah, M. A. (2017, September). Fog computing: Security issues, solutions and robust practices. In *2017 23rd international conference on automation and computing (ICAC)* (pp. 1-6). IEEE.

[9] Shenoy, K., Bhokare, P., & Pai, U. (2015). Fog computing future of cloud computing. *International Journal of Science and Research*, *4*(6), 55-56.

[10] Firdhous, M., Ghazali, O., & Hassan, S. (2014). Fog computing: Will it be the future of cloud computing?.

[11] Abubaker, N., Dervishi, L., & Ayday, E. (2017, October). Privacy-preserving fog computing paradigm.

In *2017 IEEE Conference on Communications and Network Security (CNS)* (pp. 502-509). IEEE.

[12] Guan, Y., Shao, J., Wei, G., & Xie, M. (2018). Data security and privacy in fog computing. *IEEE Network*, *32*(5), 106-111.

[13] H.S. Guruprasad and B.H. Bhavani 2014, Resource provisioning techniques in clòud computing environment: Á survey, International Journal of Research in Còmputer and Còmmunication Technology, vol.3, no.3, pp. 395--401, 2014

[14] Georgescu, M., & Matei, M. (2013). The value of cloud computing in the business environment. *The USV Annals of Economics and Public Administration*, *13*(1 (17)), 222-228.

[15] Verma, M., & Yadav, N. B. A. K. (2015). An architecture for load balancing techniques for fog computing environment. *International Journal of Computer Science and Communication*, *8*(2), 43-49.

[16] Pazowski, P., & Pastuszak, Z. (2013). Cloud computing–a case study for the new ideal of the IS/IT implementation. *Make Learn*.

[17] Malkowski, S., Kanemasa, Y., Chen, H., Yamamoto, M., Wang, Q., Jayasinghe, D., ... & Kawaba, M. (2012, June). Challenges and opportunities in consolidation at high resource utilization: Non-monotonic response time variations in n-tier applications. In *2012 IEEE Fifth International Conference on Cloud Computing* (pp. 162-169). IEEE.

[18] Mohanta, B. K., Jena, D., & Sobhanayak, S. (2020). Multi-party computation review for secure data processing in IoT-fog computing environment. *International Journal of Security and Networks*, *15*(3), 164-174.