SPLITTER ASSOCIATED WITH CRYPTOGRAPHIC MODEL TO SECURE DATA TRANSMISSION OVER THE CLOUD

Chirag Mittal1, Ankur Gupta2, Deepak Goyal3, Pankaj Gupta3, Bijender Bansal4
1M.Tech Scholar, Dept. of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India
2Assistant Professor, Dept. of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India
3Professor, Dept. of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India
4Associate Professor, Dept. of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India
2ankurdjana@gmail.com

ABSTRACT
A secure cryptographic model has been proposed to secure the data transmission. In the proposed work, for security purpose data has been split in two layer cloud and fog using splitter. As the data is traveling on two layers, there are no chances of complete loss of data. In the research work, the IP address and port number has been specified, proposed model provide the security on session layer. In addition the comparison of tradition and proposed work has been made. In comparison the different factor such as Security, Reliability, Packet dropping, Congestion, Transmission path, Port etc. The splitting of data in two layers would be applicable to decrease the chances of complete data loss by one at attempt. In the research work both side the IP address and port number has been used which would provide the security to the system. The research would be beneficial by the point of view of security. At the application layer, the proposed solution has given a more secure method to protect data from active and passive attacks. The suggested model was compared to an existing security model in the research. When comparing packet dropping in conventional and suggested work, it was discovered that packet loss was less likely in proposed work. Traditional security methods were shown to be ineffective. By separating and encrypting data using sophisticated cryptographic mechanisms, the proposed method ensures data security. This system has a lower chance of packet loss and congestion. This study looked at active and passive attacks in order to offer network security at various layers. Security is given to packets in the proposed work by splitting them into several sections. The need for a new security system has arisen as a result of the limitations of conventional security methods.

Keywords: Cloud Computing, Fog Computing, IP Filter Splitter, Port Number, Mat Lab, Net-Beans.

I. INTRODUCTION

1.1 CLOUD COMPUTING
A cloud computing [1] environment is one in which computer system resources are made available on demand, especially grid computing (cloud storage) as storage capacity, without the need for the user to exert direct active control over the resources. Large clouds often have functions spread over many locations, each of which is a data center. Cloud computing [1, 2] depends on resource sharing to achieve coherence and scale economies. Cloud providers generally employ a "pay-as-you-go" approach, which may assist reduce capital costs but can also result in unanticipated operational fees for unsuspecting customers. With cloud computing, users may take advantage of all of these capabilities without having to possess significant expertise in almost all of them. With the cloud, clients may expect to save money while also being able to focus on their core business whilst being hindered by technological obstacles. Cloud computing is primarily enabled through virtualization, which is the main enabling technology. Virtualization software converts a physical piece of office furniture into one maybe more "virtual" computers that may be controlled and used to do computing [3, 4] tasks more easily. By using web browser virtual machines, it is possible to allocate and use idle computer resources more efficiently. Virtualization, in its
most basic form, provides a scalable system made up of several independent processing units. Virtualization provides the agility required to expedite IT operations while simultaneously reducing costs by increasing the use of existing resources. In autonomous computing, the process of providing resources on demand by the user is fully automated. Automation shortens the process, reduces labor costs, and minimizes the possibility of a human error by minimizing user contact with the system [5,6].

Cloud computing makes use of concepts from utility computing in order to provide metrics for the services that are used. Cloud computing [7] aims to solve the QOS (quality of services), reliability issues that plague previous grid computing technologies.

In cloud computing [8, 9], the transmission of data is done on a regular basis. This data is transmitted by means of the Internet. Due to this, it has become necessary to consider data security [10] in a cloud environment. Because they are utilizing the compromised cloud for data dissemination, many customers’ data may be impacted. The following are some of the security concerns raised by cloud computing:

- **Data integrity**: refers to instances in which human mistakes are made when entering data into a system. Errors may occur during the transmission of data from one system to another. Hardware failures, such as crashing hard drives, may cause errors.
- **Controlling data access**: In the absence of secure data and information access control, confidential information may be unlawfully taken.
- **Data theft**: Cloud computing [12, 13] employs an external data server to perform flexible and cost-effective activities. As a result, there's a chance that information may be stolen from an external server.
- **Data access control**: Consumers are unaware of the real location of data since it is kept concealed. Cloud computing [14] allows for a high degree of information mobility.
- **Data loss**: is considered as a significant cloud computing concern. If banking, business transactions, and R&D (Research and Development) ideas are all carried out online, unauthorized persons can collect data shared in the cloud [15].
- **Privacy concerns**: With cloud computing, the protection of user data is a top priority. Since many servers are external, the provider must ensure that the data is protected against unauthorized access.
- **Challenges at the user level**: It is essential for the user to ensure that there is no risk of data loss as a result of their own actions or the actions of other users sharing a shared cloud server [16, 17 and 18].
- **Security issues at the supplier level**: Cloud is the ideal choice if high security [12] is provided by the supplier.
- **The infected application**: To maintain and manage the server, the service provider must have administrative access to the server.
- **Account or service traffic hijacking**: An account may be hijacked if login credentials are stolen.
- **Insecure application program interface**: The application program interface will have control over third parties. It also confirms the identity of the user.
- **Denial-of-Service**: When millions of people seek a shared service, this is known as denial-of-service. In this instance, the hacker takes advantage of the situation.
- **Insiders with malicious intent**: It is carried out when someone has access to our login credentials.
- **Misuse of cloud services**: Hackers might breach security in less time [19, 20] if they used cloud servers.

### 1.2 NEED OF PROPOSED SYSTEM
To secure data transfer, a secure cryptographic paradigm has been developed. For security reasons, data in the proposed study was divided into two layers of cloud and fog [21] using a splitter. There is no risk of data loss since the data is spread over two levels. The IP address and port numbers were provided in the study effort, and the suggested model provides security [22] at the session layer. Furthermore, a comparison of traditional and suggested work has been performed [23]. When comparing various factors such as security, reliability, packet loss, congestion, transmission route, port, and so on. The partitioning of data into two layers might be useful in reducing the odds of total data loss by one at attempt. Both the IP address and the port number were utilized in the study effort to offer security to the system. The study would be helpful from the standpoint [24] of security. The suggested approach has provided a more secure way of protecting data from active and passive assaults at the application layer. In the study, the proposed model was compared to an existing security model. When packet loss in conventional and recommended work was compared [25], it was found that packet loss was less frequent in suggested work. Traditional security techniques have been shown to be useless. The suggested approach guarantees data security by isolating and encrypting data using advanced cryptographic methods. This system is less likely to experience packet loss and congestion [26]. This research looks at both active and passive threats in order to provide network security [27, 28] at many levels. The suggested approach secures packets by dividing them into multiple parts. The limits of traditional security techniques have necessitated the development of a new security system.

II. VARIOUS ATTACKS

While many methods and strategies for safe data [29, 30] transfer have been developed in the past, it is also true that new kinds of attacks are getting more effective and efficient at defeating a security system. Such assaults may include those mentioned below. Denial-of-service (DOS) and distributed denial-of-service (DDOS) attacks.

- Man-in-the-middle attack
- Phishing attacks
- SQL injection attack
- Malware attack
- Attack by Cross-site scripting
- Eavesdropping

III. LITERATURE REVIEW

There are several researches which considered the security factors that placed an important role in a transmission model. These are listed here such as

In 2017, Bushra Zaheer Abbasi [1] considered Security Issues, Solutions and Robust Practices in Fog computing. The perception of FC along with its architecture is explained in this article. It also enclosed the accomplishment of FC in different real life scheme. The major stress of paper was on recognizing architectural limitation & loopholes that could be exploited by attackers. The advertisement of significant protection features through which consistency of system is make sure is also done. The state of art work done by researchers to accomplish these security features is critically analyzed in order to expose lacking areas.

Nabil Abubaker [2] thought of the Privacy-Preserving Fog Computing Paradigm. It is necessary that the design goal of fog computing be disturbed in order to accomplish end-user or IOT device secrecy utilizing the given approaches. This is the first of two challenges. The second issue is that the end-location user’s is not kept hidden; it might be an accidental open closet to a fog node. The author puts these issues in the context of real-world situations and proposes a privacy-preserving fog computing paradigm to address them.

Yunguo Guan [3] focused on Data Security as well as secrecy in Fog Computing. The major issues in fog computing are mechanism utilized to cope with information security as well as privacy concerns.

Jiyuan Zhou [4] presented a Hierarchical Secure Cloud Storage mechanism depending on Fog Computing in 2017. Such schemes play an important role in safeguarding cloud storage in the fog environment. However, research indicates that implementing such a security system is very difficult.
In 2014, Mohamed Firdhous et al. [5] predicted that Fog Computing will be the future of cloud computing. They regarded cloud computing as the most recent computing paradigm, which makes computer resources available via the Internet on a utility pricing basis.

M. Georgescu [6] considered value of cloud computing in business environment. This can be done by proper utilization of resources. Without sustaining or storing technologies, the mentality of the cloud contains prospective of having access. This allows us to change the way in business conduction on a personal level as parallel to broadly transforming of purchase in decision-making.

S. Malkowski [7] addressed the Challenges as well as Opportunities in High Resource Utilization Consolidation. According to method, we can analyze and measure the resource utilizations directly. Author hasevaluated performance in case of two integrated n-tier application benchmark systems as well as request rates. It occurs in an enterprise-level computer virtualization atmosphere.

P. Pazowski [8] provided a case study for a novel IS/IT implementation ideal in cloud computing. The study compares the conventional approach of managing the IT supply chain to the SaaS model. It happens in the context of the Total Cost of Ownership. Following the establishment of TCO, author may analyses financial metrics such as net present value, return on investment, and payback and are using them to invest in cloud computing.

B. H. Bhavani [9] investigated resource providing methods in the cloud computing context. There are many ways for allocating resources. There are two types: static and dynamic. Each has its own set of advantages and disadvantages, as well as its own set of difficulties.

In 2015, K. Shenoy etc. al. did research on Fog Computing considering it future of Cloud Computing [10]. Cloud service providers have been facing a serious problem. The issue is the security of information of user. This is due to continuous increasing number of theft attacks of information. By fog computing user’s behavior could be monitored. Hence security is provided to user data. It is developing latest techniques so that issues of insider information robbery attacks might be solved in a cloud.

M. Verma et al. focused on Architecture in case of Load balancing mechanism in Fog Computing Environment [11]. Many devices of fog computing are circulated geographically over various platforms. It is essential to optimize Service portability diagonally platforms. Fog computing concept could assist Traffic light control. Fog devices which are independent might consult directly with Cloud.

IV. OBJECTIVES OF PROPOSED WORK
The goal of the study is to offer security against attacks at the application layer, where the user interacts directly with the network. FTP, TELNET, and HTTP are the most often used protocols at the application layer. Major objective of research is to create a more efficient and time-consuming system at the application layer that is consisting following:

1. To learn about various types of attacks, such as aggressive and passive attacks.
2. To offer network security at various layers via the use of cryptographic techniques.
3. Developing and implementing secure mechanism for the safety of data from active and passive attacks at the application layer.
4. Applying a Splitter to divide data and offer data security on both layers.
5. To conduct a comparison study of the proposed model and the current security model in order to demonstrate that the suggested model is superior.

V. PROPOSED MODEL
The proposed solution has given a more secure method to protect data at the application layer from active and passive types of attacks. The suggested model was compared to the current security model in the research. When comparing packet drops in conventional and suggested work, it was discovered that the proposed work had a lower likelihood of packet loss. Traditional security methods were discovered to be ineffective. The proposed
method protects data by separating and encrypting it using sophisticated cryptographic mechanisms. This system has a lower chance of packet loss and congestion.

This study investigated active and passive attacks in order to offer network security at various layers. In the proposed approach, packet security is achieved by splitting them into numerous pieces. Because of the limitations of conventional security methods, a new security system is required. Here IP filter has been used to reject unauthenticated transmission of packets from server to client. If packet is valid then enhanced AES ENCRYPTION module works. Here the process flow of data transmission has been proposed.

At sending hand, following steps are followed such as

- TAKE PLAIN TEXT (256 bits)
- APPLY ROUND KEY and set counter=1
- if counter is less then N-1 (Here N would be number of iteration)
- Process sub byte.
- Perform Shift row
- Mix columns
- counter=counter+1;
- other wise
- process sub bytes
- shift rows
- Apply round key
- Cipher text would be generated (256 bits)

At receiver end, following steps have been followed

- TAKE CIPHER TEXT (256 bits)
- APPLY ROUND KEY and set counter=1
- if counter is less then N-1
  - a)Process Inverse shift row.
  - b)Perform inverse sub byte
  - c)Inverse Mix columns
  - d)Counter=counter+1;
- other wise
  - a)Inverse shift rows
  - b)Inverse sub byte
  - c)Apply round key
- Plain text would be generated (256 bits)
The objective of the research is to provide protection against assaults on the app level, where the user directly interacts with the network. The protocols used at the application layer include FTP, TELNET, and HTTP. Research's main goal is to develop a more time consuming and efficient application layer system. Research has focused on learning about many kinds of assaults, including aggressive and passive attacks and the application of cryptographic methods to provide network security on different levels. In addition, the work being suggested is aimed at designing and implementing a safe data security mechanism against active and passive application layer threats. The suggested approach applies a Splitter to split data into two levels and provide data protection. Finally, research is carried out in order to show that the proposed model and the existing security model are better.

![Diagram of data security mechanism](image)

**Fig 1** Process flow of proposed work

**VI. RESULTS AND DISCUSSION**

The implementation and result of the proposed work has been stated here

**FILE SPLITTER**

The FILE splitter would divide the data into two separate files, one for the cloud and the other for the fog. The file's name and security code are provided, and the file is split and distributed in two locations, one for cloud and another for fog. This improves the security and reliability of transmission.
GUI INTERFACE FOR CLIENT
This is file transmitter interface, which would send data to the server. User ID, password, port number, IP address, file path to be sent, security token, and AES CODE are all entered here.

GUI INTERFACE FOR SERVER
This is file transmitter interface, which is used to transfer data to server. Port number, AES CODE, and file path to be received, as well as the security token are considered during transmission.

From the sender's end, the following file would be transmitted to the recipient. It might be a notepad file.
At the recipient end, the following file would be received. The file's content would be the same as the file transmitted from the sender's end.

**Fig 6 File Received**

**ENCRYPTED FILE**

During transmission, the file's content was shown here. It's encrypted text, and it's unreadable. If someone were to hack that information, he would be unable to comprehend it.

**Fig 7 Encrypted file**

The transmitter module would deliver data from cloud to end user. Authentication code would be used to encrypt the data. The port on the sender side would be the same as the port used by the end user. The end user's IP address would be provided here.

The following diagram depicts the design of a data transmitter module for the cloud. There are three boxes for input. The first input box would receive a port number, the second a server IP address, and the third an authentication code to encrypt data to be transmitted.
IMPLEMENTATION OF FOG

The transmitter module would convey data from the FOG to the end user. Authentication code would be used to encrypt the data. The port on the sender side would be the same as the port used by the end user. The end user's IP address would be provided here. The design of the data transmitter module for FOG is shown in the picture below.

The end user module is split into three sections.

1. **Ready to receive from fog**: This part opens the fog port and enables data to be collected from the fog side. The port should be accessible from both sides. The shared authentication code would be the same so that data transmitted from the fog side could be decrypted.

2. **Ready to accept data from the cloud**: This step opens the cloud port and enables data to be collected and transmitted from the cloud side. The port should be accessible from both sides. The shared authentication code would be the same so that data transmitted from the cloud side could be decrypted.

3. **Merge and Decode**: In this phase, incoming data is merged and decoded based on the authentication code.
Table 1: Comparison of Tradition work and Proposed work

<table>
<thead>
<tr>
<th>Comparison Factors</th>
<th>Tradition work</th>
<th>Proposed work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration to Fog</td>
<td>Traditional work does not make use of Fog</td>
<td>Proposed work make use of fog</td>
</tr>
<tr>
<td>Level of Security</td>
<td>Traditional work is less secure</td>
<td>Proposed work is more secure as split data is transferred from two different locations.</td>
</tr>
<tr>
<td>Reliability</td>
<td>Traditional work is less reliable</td>
<td>Proposed work is more reliable.</td>
</tr>
<tr>
<td>Security at multiple layer</td>
<td>Tradition layer provided security on the application layer only.</td>
<td>Proposed work is providing security at multiple layers.</td>
</tr>
<tr>
<td>Packet dropping</td>
<td>The probability of packet dropping is more</td>
<td>There is less probability of packet dropping.</td>
</tr>
<tr>
<td>Congestion</td>
<td>There are more chances of congestion.</td>
<td>There are fewer chances of congestion.</td>
</tr>
<tr>
<td>Transmission path</td>
<td>Only a single path would be chosen to transmit data</td>
<td>Data would travel through multiple paths.</td>
</tr>
<tr>
<td>Port</td>
<td>Predefined</td>
<td>User Defined</td>
</tr>
</tbody>
</table>

Table 2: Comparative Analysis of Packet Dropping in Traditional and Proposed Work

<table>
<thead>
<tr>
<th>Factors</th>
<th>Traditional</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>200</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>300</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>400</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>500</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>600</td>
<td>18</td>
<td>8</td>
</tr>
<tr>
<td>700</td>
<td>30</td>
<td>12</td>
</tr>
<tr>
<td>800</td>
<td>40</td>
<td>23</td>
</tr>
</tbody>
</table>
VII. CONCLUSION

Compared to previous implementations, the proposed approach provides a more secure method to protect data from both active and passive types of attacks at the application layer. The suggested security model was compared to an existing security model in the course of the investigation. While comparing packet dropping in traditional and proposed work it has been observed that in proposed work there has been less probability of packet loss. It was observed that traditional security systems. This system protects data by separating and encrypting it using sophisticated cryptographic mechanisms, which are described in detail below. The likelihood of packet loss and congestion is decreased with this arrangement. The investigation of possible threats has been carried out in order to ensure network security at various layers throughout the investigation. Specifically, in the proposed method, packet security is achieved by segmenting them into several sections. Because of limitation of traditional security mechanisms there has been requirement of new security system.

VIII. FUTURE SCOPE

The use of cryptographic technique would be beneficial for the security of data transmission. In case of traditional work, there has been data protection only at application layer. The splitting of data in two layers would be applicable to decrease the chances of complete data loss by one at attempt. In the research work both side the IP address and port number has been used which would provide the security to the system. Security is given to packet in proposed work. This mechanism would provide a security system immune against of different attacks.

REFERENCES

3. Yingsuo Guan, Jun Shao, Guiyi Wei, Data Security and Privacy in Fog Computing, 0890-8044/18/$25.00 © 2018 IEEE


