International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 263-267
Published Online May 2020 in IJEAST (http://www.ijeast.com)

RESOURCE MANAGEMENT IN FOG COMPUTING BASED ON CLUSTERING

Ms. S. C. Nagavekar, Ms. S. S. Patil, Ms. V. V. Gathe, Mr. K. G. Malatkar, Ms. R.Y. Mulla
Department of Computer Science & Engineering
Sanjay Ghodawat Institute, Atigre, Kolhapur

Abstract: **Fog computing network is designed as an expansion of the cloud. In today's world security is main concern in the communication factor. To achieve the accurate perform in terms of security we need to use fog nodes over the network for accessing secured in cloud computing. Indeed, fog computing definitely meet various security and privacy risks. So we are proposing a security model that is based on cooperation between IoT and fog.**

Keywords: Fog Computing, Trust, Security, IoT network, Security, Access Control

I. INTRODUCTION

Cloud computing is used widely for handling large amount of the data. The main purpose of using cloud is for data storage. Here it does not need the active participation of the user. For handling the large amount of the data in distributed environments there is an effective solution known as cloud computing. As the cloud computing delivers centralized resources for data computation and storage, which may affect metrics delay and bandwidth [1]. Whereas fog nodes are distributed decentralized in nature. The fog is an extension of the cloud computing which consist the multiple edge nodes connected to the physical devices.

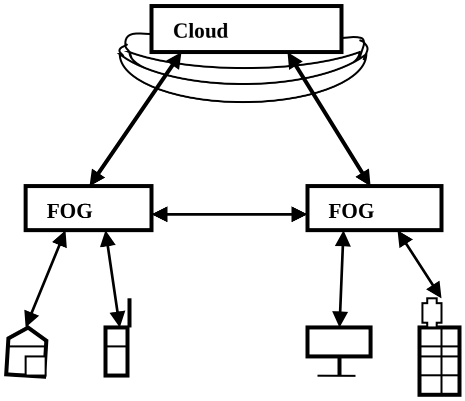


Fig 1. Interaction between Cloud, Fog, IoT

The fog computing is the mediator between hardware and remote servers. It regulates which information should be sent to users and which should be processed locally; a characteristic that reduces latency and establishes adjacent localized connections [5]. Fog computing is a standard with virtual or physical resources or horizontal resources that resides between end-devices and cloud or data centers. This standard supports latency sensitive applications by providing layered, scalable and distributed computing, storage, and network connectivity.

IoT utilizes capacities of fog computing for virtualizing tasks of IoT devices, which attains long delay and has restricted capability. As the primary goal of Fog computing is to achieve all tasks with high performance, the security features must be considered as part of the Fog system to guarantee the (CIA) that is Confidentiality, Integrity, and Authentication of all types of data. Fog computing or fog networking, is also known as edge computing or fogging. It is an architecture which uses one or more collaborative group of end-user or near-user edge devices to carry out a essential amount of communication and storage. Fog computing has been proposed to bring cloud services closer to IoT users [4].

By using wireless communications to interconnect nodes, system may affect by having attacks, such as sniffing, spoofing and Denial of Service attacks. We can achieve high security with the help of fog computing as data is processed by huge number of nodes in complex distributed system. The design of a combined wireless fog-cloud computing approach based IoT network becomes essential for resource management and network control security.

II. LITERATURE SURVEY

By having interaction between Cloud- IoT,-Fog, there is a huge amount of data that may need to be manipulated and executed. In such environment attacks may occur. Such attacks may occur due to inefficient and insufficient resource policies, as well as from a lack of monitoring of user activity.The main problem is poor implementation of the security can lead to security problems. Security schemes must be developed in the fog system for the reason that if it is not secure, its performance could possibly be reduced due to attacks such as misuse of resources, malware and so on [3]. In order to optimize the execution delay we need to propose the fog computing security strategies and resource management technique. Fog systems are effective for processing large amounts of data locally, and are fully portable, and can be installed on different hardware. These qualities make the Fog platform highly suitable for time.

Ensuring equivalent security in a different fog environment using the trust based access control approach would be a essential. Furthermore, authorization issues would occur as fog resources would be shared by various users. Without proper security measures, the network will be vulnerable to many threats and become easily compromised.Fog networks are examines as offloading to storage and computation.

In fog computing, fog nodes decide to either process the services using its available resource or send to the cloud server. The Fog system continuously manages personal data from end user to the cloud and vice versa. Here it supervises and detects abnormal network actions. Security efficient monitoring methods are applied by each fog system [1]. Fog provides storage locally and IoT data processing at IoT devices instead of sending them to the cloud. In contradiction to the cloud, the fog provides services with greater quality and faster response. Clustering involves the grouping of data points. Given set of fog nodes, get divided into small cells. The number of Fog node to use in each cell randomly selected. Then, each cell is managed by fog node manager that plays role of cluster head. When an IoT user tries to access a fog node the access request will be handled by this cluster head. In the fog computing system, the encrypted sensitive data may be transmitted to multiple fog nodes on the edge of a network for low latency; therefore, Implementation needs be done for fog nodes in order to a search over encrypted data as a cloud server. When sensitive data needs to be stored on fog nodes untrusted as public cloud platform, search over encrypted data and data encryptions are still preferred approaches for data confidentiality.

III. EXISTING WORK

The previous system was mainly focusing on the availability of servers processing in cloud or in fog. But an extra time for the procedure is needed due to the division procedure. Due to introduction of data combination, it can add a delay based overhead. Also from security point of view, they did not consider the risks of insider attacks in fog/cloud networks. It was difficult to process large number of requests due to limited resources.

The main problem is poor implementation of the security can lead to security problems. Security schemes must be developed in the fog system for the reason that if it is not secure, its performance could possibly be reduced due to attacks such as misuse of resources, malware and so on [3]. In order to optimize the execution delay we need to propose the fog computing security strategies and resource management technique. The Fog system continuously manages personal data from end user to the cloud and vice versa.

IV. PROPOSED SYSTEM

The proposed system is about resource management in fog computing based on clustering. Fog systems are composed of IoT devices and wireless sensors. If it is not hidden and secure, the attackers may interrupt and capture sensitive data. Thus we are going to propose the system which going to based on resource management and security strategies. The system is based on monitoring user’s activities and trust assessment where resource management strategy is integrated wireless fog in IoT networks to improve the resource utilization and reduce the transmission latency. We are mainly focusing on to optimize the execution delay and then minimize the total price of management in the system. The proposed scheme is the clustering, which involves the grouping of data points. Set of Fog Node is available, after that partitioning of that fog node cells into small cell is done. Firstly, the number of Fog Node to use in each cell is randomly selected. Then, Fog Node Manager manages the each cell and also it plays the role of cluster head. It mainly focuses on the security.The availability can be affected by failure of connectivity, hardware, or software matters. Hence, it must be guaranteed. The implementation of resource allocation and access control based priority scheduling approach in a highly distributed and different fog environment means that availability will be a challenge. In fact, the deployment of our resource allocation approach and the information exchanged between cluster heads from various Fog node cells increases the availability of the system; hence, the users are served with minimum introduced delay. Furthermore, the delivered authorization is used after the resource allocation procedure (its affectation to the Fog Node). In his next access to such a Fog Node in that small cell, this user doesn’t repeat the procedure of the access, since he/she has an authorization; quite simply, need to present it. Finally, we assure the availability of server in fog nodes to handle huge number of requested resources at any time, with considering guarantee of the satisfaction of Quality of Service and offering fast respond.

Here it supervises and detects abnormal network actions. Security efficient monitoring methods are applied by each fog system [2].Clustering involves the grouping of data points. Given set of fog nodes, get divided into small cells. The number of Fog node to use in each cell randomly selected. Then, each cell is managed by fog node manager that plays role of cluster head. When an IoT user tries to access a fog node the access request will be handled by this cluster head that is nothing but Fog Manager.

Process of moving from cloud to fog would reduce the network bandwidth usage. As a result, system would decrease network communication overhead by using clustering method in fog domain. Hence, our proposed strategy has led to the optimization of distribution of large data in the fog. Proposed System continuously monitors the user till user’s end activity.

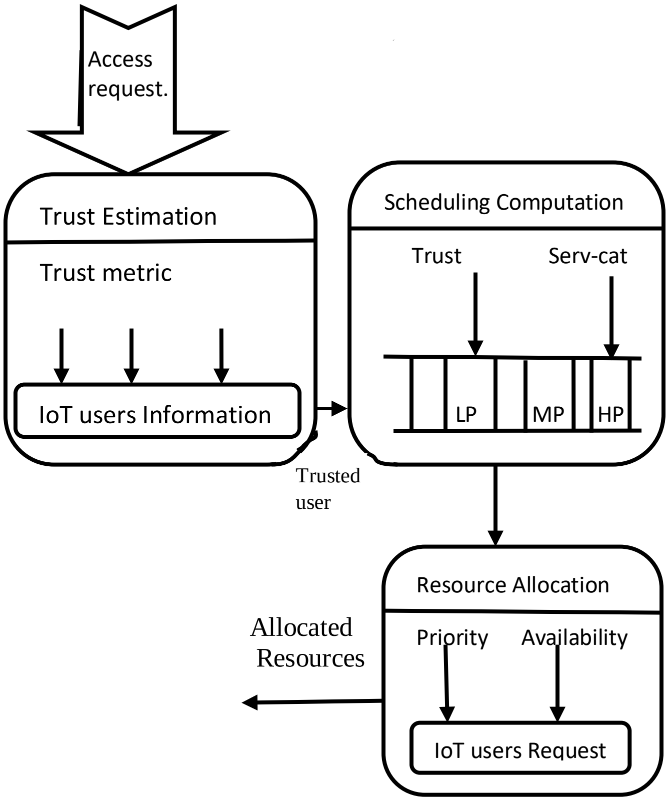


Fig 2. Process of Proposed System solution

Here we maintain the log records of each user by monitoring user's activities. User gets blocked if any abnormal activity done by the user gets noticed. Mainly focuses on detection of attacks, for that we are going to work on authentication and bootstrap attacks. Thus the cluster head handles the request when the IoT user tries to access Fog Node.

In the proposed system we are providing the security by detecting the attacks occurred in the system and accordingly providing according for the system. By this method, not only system but also we will be providing security to each user.

A. Advantages:

1. Ensuring homogeneous security in a heterogeneous fog environment using the trust based access control approach would be a necessity.
2. The monitoring process is functioning continuously, even after the gain of permission from the user.
3. The user's information is vulnerable to network failures mostly at the Edge level (fog, IoT).
4. The availability can be affected by failure of connectivity, hardware, or software matters.
5. The moving of the processing from cloud to fog would reduce the network bandwidth usage.

B. Methodology:

- **Access control management:**

Here the first task is to control the access of the new IoT user which is done by the Fog Node manager. When the user request the access at that time trust level get computed. User's trust is assigned according to the behaviour of each user. On the basis of the trust level authorization is allocated to the every user that is assessed by the cluster head. After the resource allocation procedure authorization is used. Once the authorization has allocated to the user, in his next access he doesn't repeat the procedure to access Fog Node in that small cell.

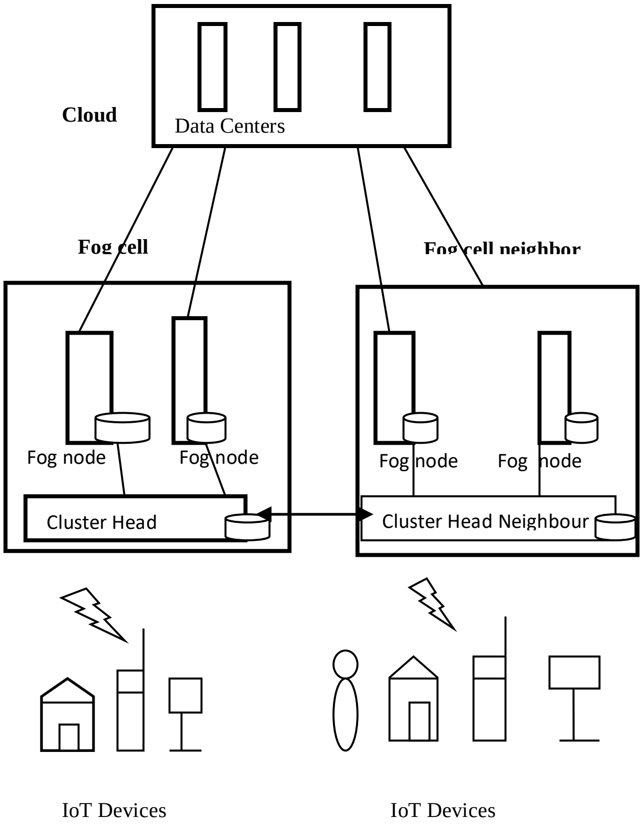
- **Monitoring process:**

The monitoring process is functioning continuously, even after the gain of permission from the user. Moreover, a deactivating function is triggered when detecting abnormal activities and reporting them .Here the Fog Node Manager monitors the whole system to supervise the user's activities. The overall traffic between cloud and fog computing also get supervised by the Fog Node manager. In this monitoring process, it detects the malicious behaviour of connected users and reports alerts that is shared between different fog nodes in the same small cell.

- **Resource management:**

Here the Fog Node Manager has to perform the resource classifier by knowing the amount of the resource available. To meet the quality of service requirements the resource allocation process needs to dynamically adjust. The classifier allocates the communication and the computing resources to each user if and if user is trusted. Also it is responsible for the user's priority which will be benefited by the requested resources and to allocate the resources to the users.

C. System Architecture



The architecture of the system is shown above, it contains different IoT users requesting for the access to the Fog Node cell to gain computing services. The proposed system architecture contains two layers: IoT layer and the fog layer. The fog layer has several fog nodes. The data services are available independently by fog nodes with reduced latency.

D. Algorithms:

The algorithms implemented in the proposed system are:
1. Assigning Priority
2. Access Decision and Scheduling

1. Assigning priority based on trust level:

- Calculating trust value:

$$\text{Trust} = \sum_{i=1}^{n} w_i x_i.$$

.... [1]

Where,

W= weight vector
X= input vector

We have considered, input vector as 1 which constant and weight vector gets change for each user.

In this algorithm we are going to assign priority on the basis of trust level.

```
{
   if (Trust == 1)
   {
         if SC ==H or M)
               Assign HPri to the ac-reqi
         if SC ==L)
                Assign MPri to the ac-reqi
    }
    if (Trust ==2 )
    {
          if SC ==H)
                Assign HPri to the ac-reqi
          if SC ==M or L)
                 Assign MPri to the ac-reqi
    }
    if (Trust == 3)
   {
         if SC ==H or M)
                 Assign MPri to the ac-reqi
         if SC ==M)
               Assign LPri to the ac-reqi
    }
    if (Trust == 4)
         if SC ==H or M or L)
                 Assign LPri to the ac-reqi
   }
```

Where,

ac-reqi – access request from user i
Pr: Priority
SC - Service category
H, M, L: High, Medium, Low
HPri: high priority
MPri: medium priority
LPri: low priority

2. Access Request and Scheduling:

- Access Decision:

$$\text{Ac\_Des} = \begin{cases} 1 & \mathit{if} \sum_{i=1}^{n} w_i x_i \geq \theta \\ 0 & \mathit{else} \end{cases}.$$

… [1]

In this algorithm we are going to the give access by checking the user's trust against the threshold value.

```
if ( Trust<=Threshold)
   Accept the access-request;
else
   Reject the access-req;
```

Priority is assigned by the classifier by calling the scheduler module which is based on the availability of the resources in Fog Node cell, service scheduling happens as follows:

```
(Pr) = Assign-priority (Trust, SC)
{
     For each user i having High Priority or Medium
     Priority, or Low Priority


     Resource availability get checked by classifier.

          if ( resources are available)
                    Schedule the ac-reqi for the service and
                    initiate the service for user i
  }
```

V. CONCLUSION

The cooperation between this standard requires a robust security system to manage with expected attacks. An efficient resource management strategy to improve the performance of the system is also needed. Here we proposed a clustering algorithm for security and resource allocation based on priority. We provide access control scheme based on user's trust assessment and monitoring process in order to ensure high security level. The result of the efficient resource deployment for network environment. From the simulation results, we proved the impact of the implementation of our algorithm in the Fog paradigm towards solving the problem of latency that is a critical factor in IoT applications.

ACKNOWLEGGEMENT

The presented paper is an outcome of motivation received from "TACRM: Trust Access Control and Resource Management mechanism in Fog Computing" by Widen Ben Daoud, Mohammad S. Obaidat. We tried to partially implement Fog Computing System for Resource Management as a part of UG student projects to learn Fog Computing and to work with new technologies.

VI. REFRENCES

[1] Daoud Widen Ben, Obaidat Mohammad S., Medded-Makhlouf Amel, Hsiao Faouzi Zarai,Kuei-fang (2019): TACRM:Trust Access Control and Resource management mechanism in fog computing, doi:10.1186/s13673-019-0188-3

[2] Guan Z, Zhang Y, Wu L, Wu J, Li J, Ma Y (2019) :APPA-An anonymous and privacy preserving data aggregation scheme for fog enhanced IoT. J Netw Comput ,(pp.82–92)

[3] Tanwar S, Kumar N, Tyagi S, Obaidat MS (2019): Tactile internet-based ambient assistant living in fog environment. Future Gener Comput Syst ,(pp.635–649)

[4] Bangui H, Rakrak S, Raghay S, Buhnova B (2018) : Moving to the Edge-Cloud-of-Things:recent advances and future research directions.Electronics, doi: 10.3390/electronics7110309

[5] Riad K (2018): Secure storage and retrieval of IoT data based on private information retrieval. Wirel Commun Mob Comput , doi: 10.1155/2018/5452463

[6] Ben Daoud W, Meddeb-Makhlouf A, Zarai F (2018):A model of role-risk based intrusion prevention for cloud environment.In:2018 14th international wireless communications & mobile computing conference(IWCMC),doi:10.1109/ IWCMC.2018.8450466

[7] Puthal DD, Obaidat MS, Nanda P, Prasad M, Mohanty SP, Zomaya AY (2018) : Secure and sustainable load balancing of edge data centers in fog computing. IEEE Commun Mag. ,(pp.60–65)

[8] Ni J, Zhang K, Lin X, Shen XS (2018): Securing fog computing for Internet of Things applications: challenges and solutions. IEEE Commun Surv Tutor ,(pp.601–628)

[9] Xiao M, Zhou J, Liu X, Jiang M (2017) :A hybrid scheme for fine-grained search and access authorization in fog com- puting environment. Sensors (Switzerland) ,(pp.1–22)

[10] Mahmud R, Ramamohanarao K, Buyya R (2017): Latency-aware application module management for fog computing environments. ACM Trans Embed Comput Syst ,(pp. 1–21)

[11] Alrawais A, Alhothaily A, Hu C, Cheng X (2017) : Fog computing for the Internet of Things: security and privacy issues.IEEE Internet Comput,(pp.34–42)

[12] Choudhari T, Moh M, Moh TS (2018):Prioritized task scheduling in fog computing. In: Proceedings of the ACMSE (pp. 1–8)