SECURE DATA QUERY ON FOG AND CLOUD COMPUTING

SUNANDA NALAJALA¹, B LAKSHMI LIKHITA², K SANDEEP², L RAVI KIRAN², VNSV JAGADEESWAR²

¹Assistant Professor, Department of computer Science &Engineering, Koneru Lakshmaiah Education Foundation, Guntur. sunanda@kluniversity.in
²Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Guntur. vjagadeeswar111@gmail.com

ABSTRACT

Fog computing especially wants to process an outsized amount of data created by terminal devices. As fog nodes are the closest spotters to the terminal devices, the processed data could also be tinkered with or illegally captured by some dangerous nodes while the info is transferred or piled up. When some applications need to require a real-time process with high security, cloud service may represent some data from fog service to check final results. The suggested system is a secure data query structure for both fog and cloud computing. We use cloud service to see queried data from the fog network when the fog network furnishes queried data to users. In the framework, the cloud server pre-assign a few facts aggregation topology trees to the fog community, then the fog community might also additionally spot associated facts from fog nodes constant with one the various pre-assigned facts aggregation trees. Moreover, some fog nodes are allocated as sampled nodes which will feedback related data to the cloud server. Based on the safety requirements of fog computing, we inspect the safety of our proposed framework. The Proposed framework not only assures the reliability of essential data but also effectively guards data against a man-in-the-middle attack, single node attack, and collusion attack of dangerous users. Also, the experiments show our framework is powerful and methodical.

I. INTRODUCTION

With the fast development of network, cloud computing has become an awfully vital application service in several alternative business fields, like web of Things (IoT). However, a lot of and a lot of terminal devices square measure connected to IoT, which can turn out huge and numerous knowledge on a daily basis. So, the model of cloud computing is troublesome to satisfy the necessities of IoT for responding quickly, high quality, geographical distribution, location awareness, low latency so on. The Cisco Company projected a brand new computing idea known as fog computing, that moves computing, storage and alternative functions of cloud computing from the middle to the sting of network wherever all functions square measure nearer to terminal users. Fog computing provides a system-level horizontal design. Fog computing is additionally a virtualized service computing design, which can give computation, storage and networking services between terminal devices and back-end cloud services.
As Associate in Nursing extending paradigm of cloud computing, fog computing naturally inherits a number of the protection and privacy problems from cloud computing. Some issues are often solved mistreatment some existing solutions or technologies. However, fog computing has non-uniformity, mobile request, big range of node distribution and lack of observation of fog nodes. Thus, as fog devices square measure measure the nearest acquirers to the terminal devices, several of fog devices square measure measure terribly liable to some attacks from malicious nodes, like device meddling, man-in-the middle attack and privacy run. What is more, as some effective protection ways for fog devices square measure measure lacked, the processed knowledge is also simply tampered with or lawlessly captured by some malicious nodes in storage and transmission. As an example, as fog servers square measure deployed at the sting of network, the information in fog servers square measure straightforward to be attacked or tampered with, then the compromised fog servers will give an outsized quantity of false knowledge to users.

II. LITERATURE SURVEY

Many present strategies were studied with the aid of using the researchers primarily based totally on stable facts outsourcing to cloud storage, few of them are mentioned below.


As the explosive boom of properly gadgets and so the appearance of the numerous any new programs, visitors quantity has been developing exponentially. The ordinary centralized specialization can't accommodate such person needs due to extensive burden at the backhaul hyperlinks and lengthy latency. Therefore, new designs, that convey community capabilities and contents to the community aspect, are projected, i.e., cellular aspect computing and caching. Mobile factor networks offer cloud computing and caching abilities at the brink of cellular networks. During this survey, we will be inclined to create Associate in nursing entire overview at the innovative evaluation efforts on cellular aspect networks. We will be inclined to 1st offer a precis of cellular aspect networks, in addition to definition, architecture, and benefits. Next, a complete survey of issues on computing, caching, and verbal exchange strategies on the community aspect is given. The programs and use instances of cellular aspect networks are mentioned. Later on, the important thing enablers of cellular aspect networks, like cloud technology, SDN/NFV, and properly gadgets are mentioned. Finally, open evaluation demanding situations and destiny instructions are given additionally.


Fog computing extends the Cloud Computing paradigm to the edge of the network, for this reason allowing a modern-day breed of packages and services. Defining traits of the Fog are: a) Low latency and location awareness; b) Wide-unfold geographical distribution; c) Mobility; d) Very extensive quantity of nodes, e) Predominant function of wi-fi access, f) Strong presence of streaming and actual time programs, g) Heterogeneity. In this paper we argue that the above traits make the Fog the proper platform for type of essential
Internet of Things (IoT) offerings and programs, namely, Connected Vehicle, Smart Grid, Smart Cities, and, generally, Wireless Sensors and Actuators Networks (WSANs).


Recently, the theory of Internet of Things (IoT) is attracting a whole lot of interest due to the huge capacity. IoT makes use of the internet as a key infrastructure to interconnect various geographically heterogeneous IoT nodes that normally have scare resources, and so cloud is used as a key back-stop assisting infrastructure. Within the literature, the collection of the IoT nodes and additionally the cloud is prepare called an IoT cloud. Sadly, the IoT cloud suffers from various drawbacks like good sized community latency due to the fact the extent of data this is being processed a number of the gadget will boom. To alleviate this issue, the theory of fog computing is introduced, during that fog like intermediate computing buffers rectangular degree set among the IoT nodes and so the cloud infrastructure to locally technique a massive amount of local expertise. Compared to the number one IoT cloud, the conversation latency conjointly on account of the overhead on the backend cloud infrastructure can be extensively decreased with inside the fog computing supported IoT cloud that we're going to refer as IoT fog. Consequently, many treasured offerings, that have been hard to be introduced with the aid of using the traditional IoT cloud, rectangular degree normally correctly provided with the aid of using the IoT fog. During this paper, however, we generally tend to argue that the adoption of IoT fog introduces many distinct protection threats. we generally tend to 1st speak the theory of the IoT fog conjointly because of the triumphing protection measures, that cloud be useful to stable IoT fog. Then, we generally tend to discover capacity threats to IoT fog.


Fog Computing is likewise a paradigm that extends Cloud computing and offerings to the edge of the community. Similar to Fog, Cloud offers expertise, compute, garage, and alertness offerings to stop-users. During this article, we generally tend to complicated the incentive and advantages of Fog computing, and examine its packages in an extremely collection of actual eventualities, like exact Grid, exact visitors lighting in shipping networks and code mentioned networks. We generally tend to talk about the modern of Fog computing and comparable paintings below a comparable umbrella. Security and privateness issues rectangular degree greater disclosed in line with cutting-edge Fog computing paradigm. As companion instance, we generally tend to look at a standard assault, man-in-the-center assault, for the dialogue of protection in Fog computing. We generally tend to research the sneaky alternatives of this assault with the aid of using inspecting its digital device and reminiscence intake on Fog device.


Face identity and backbone era is important to shape positive the identification consistency of human beings in bodily residence and cyber residence. Within the cutting-edge internet of Things (IoT) and big expertise nation of affairs, the boom of packages supported face identity and backbone increases the pressure of computation, conversation, and garage capabilities. Therefore, we’ve deliberate the fog computing-primarily based totally face identity and backbone framework to enhance method functionality and store the data degree. However, there are a unit a few protection and privateness issues delivered with the aim of using the homes of fog computing-primarily based totally framework. During this paper, we have a propensity to endorse a protection and privateness upkeep subject matter to get to the bottom of the better than issues. We have a propensity to offer a precis of the fog computing-primarily based totally face identity and backbone framework, and summarize the safety and privateness issues. Then the authentication and consultation key settlement subject matter, coding subject matter, and expertise integrity checking subject matter location unit deliberate to get to the bottom of the troubles of confidentiality, integrity, and accessibility with inside the strategies of face identity and face resolution. Finally, we have a propensity to put into effect an instance gadget to degree the have an impact on of protection subject matter on gadget performance. Meanwhile, we have a propensity to moreover valuate and examine the safety homes of deliberate subject matter from the motive of study of logical formal evidence and
hence the confidentiality, integrity, and accessibility (CIA) homes of expertise protection. The effects suggest that the deliberate subject matter will correctly meet the desires for protection and privateness upkeep.

<table>
<thead>
<tr>
<th>Title of the paper</th>
<th>Authors</th>
<th>Name of the publication</th>
<th>Methodology</th>
<th>Issues/ Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fog Computing and its Role within the Internet of Things</td>
<td>Bonomi, Flavio &amp; Milito, Rodolfo</td>
<td>Proceedings of the MCC workshop on Mobile Cloud Computing, 2014</td>
<td>Fog the acceptable platform for variety of essential Internet of Things (IoT) services and applications.</td>
<td>They are theoretically studied</td>
</tr>
<tr>
<td>On security and privacy problems with fog computing supported Internet of Things environment</td>
<td>K. Lee, D. Kim, D. Ha, U. Rajput and H. Oh</td>
<td>International Conference on the Network of the Future (NOF), 2015</td>
<td>Fog like intermediate computing buffers are situated between the IoT nodes and the cloud infrastructure to locally process a major quantity of regional data.</td>
<td>There is no security for the system is considered.</td>
</tr>
<tr>
<td>The Fog computing paradigm: Scenarios and security issues</td>
<td>I. Stojmenovic and S. Wen</td>
<td>Federated Conference on Computer Science and Information Systems, Warsaw, Poland, 2014</td>
<td>Fog for Smart Grid, smart traffic lights in vehicular networks and software defined networks are analyzed</td>
<td>Theoretically analyzed and no practical work carried out</td>
</tr>
</tbody>
</table>

Many research have been proposed on popularity machine, the ones present popularity control structures didn’t don’t forget the manner to manipulate private records get admission to supported popularity over the cloud.

**III. PROBLEM STATEMENT AND METHODOLOGY**

Some compromised fog nodes may tamper with or thieve records while getting or shifting records. Therefore, while records is processed and transferred among fog gadgets, authentication, records safety, identification accept as true with and distinctive protection issues want to be followed. Among this layout of fog computing, as fog nodes and fog servers are less difficult to be attacked, the queried records from fog community won’t be sure. So, we have a propensity to pay attention on constructing an inexpensive interplay among cloud provider and fog community to resolve the verification disadvantage of queried records from fog community. Once a few programs should be forced to want term approach with excessive protection, cloud provider may pattern a few records from fog community to test the very last phrase consequences. For example, a person may short
accumulate the specified records from the fog community and pre-use information, while the person waits for the checked records from the cloud provider.

OBJECTIVES OF STUDY
The study's aim is to don't forget cloud gadgets which are public and trusted, however fog networks which are insecure and untrustworthy. When a few programs want real-time processing with excessive protection, cloud offerings can pattern records from the fog community to decide the very last consequences. For example, at the same time as looking ahead to the validated records from the cloud provider, a person can fast acquire the asked records from the fog community and pre-use the details. Finally, the patron will evaluate them to peer if the calculated solution continues to be appropriate.

IV. EXISTING SYSTEM
- As fog computing is carried out into IoT, a few protection demanding situations to IoT arise, like man-in-the-center attack, intrusion detection and malicious node detection. They additionally proposed a few ability protection technology in opposition to the threats. However, they didn’t cope with an appropriate answers for the prevailing issues.

- Some fog computing programs is to put in force a few positive features to meet the desires of a few fields, for that reason many protection issues are frequently ignored. They proposed a few not unusual place protection weaknesses in fog computing, and cautioned that encoding, records backup and different associated technology are frequently need to remedy the troubles.

- Some approaches, like authentication, consultation key protocol, encoding and records integrity checking, are frequently need to remedy the troubles of confidentiality, integrity and availability.

- Energy intake and high-satisfactory of provider (QoS) are frequently taken into consideration critical fog computing performance indicators. They cautioned a solution supported evolutionary algorithms to resolve the tradeoff problem.

- An green key alternate protocol supported cipher text-coverage characteristic primarily based totally encryption (CP-ABE), which permits actual and personal communications amongst a bunch of fog nodes.

- A fog-primarily based totally privacy-conscious function get admission to manipulate (FPRBAC) machine among fog nodes became carried out, in addition to a region-primarily based totally accept as true with (RBTA) version for accept as true with translation amongst fog nodes.

V. PROPOSED SYSTEM
- A data query platform for cloud and fog computing that is stable.

- When the fog community sends the queried records to the customers, we use the cloud server to peer the queried records from the fog community.

- The cloud server can pre-designate a few records aggregation timber to the fog community, and then it'll pattern a few records from the fog community to determine the very last consequences added to the customers.

- Two records verification strategies have been furnished for records aggregation of fog community and records sampling of cloud server, respectively.

- Furthermore, the network authentication and for this reason the (t, n) threshold key sharing scheme are used to validate the authenticity of records sampling for the cloud provider.

Advantages
- The protection and feasibility of our proposed structure had been evaluated primarily based totally at the safety requirements of fog computing.
The proposed structure now no longer handiest guarantees the reliability of vital records however additionally successfully defends records from malicious person man-in-the-center attacks, unmarried node attacks, and collusion attacks.

Experiments exhibit that our proposed machine is powerful and green compared to comparable works.

VI. SYSTEM ARCHITECTURE

The above figure shows the system architecture of proposed system, this represents all implemented modules node deployment, Fog node architecture and data gathering to cloud server is shown. the modules included in our implementation are as follows

TERMINAL NODE

The sensor nodes are divided into disjoint clusters, and each cluster capabilities a cluster head which acts as an aggregator. Data are periodically accrued and aggregated via way of means of the aggregator.

FOG NODE AND REPUTATION MODEL

Because fog nodes are the nearest acquirers to the terminal gadgets, the safety and privateness of processed records in fog computing ought to be considered. In fog community, the processed records can also be tampered with or illegally captured via way of means of a few malicious nodes at the same time as the information are transferred or aggregated. Additionally, the interplay of cloud-fog computing additionally offers an possibility for the attackers. The protection of the interplay of cloud-fog computing to clear up the verification of queried records from fog community. Thus, recommend a protection requirement frame. In the interplay of cloud-fog computing, there exist numerous forms of attack.

DATA ACCUMULATING AND DATA AGGREGATION

The fog nodes immediately cope with huge unique records acquired from terminal gadgets at community edge. Thus, if a few fog nodes are compromised via way of means of malicious users, then the corrupted fog nodes may match collectively with outside attackers to eavesdrop personal records or tamper with personal records acquired via way of means of themselves. Every Terminal node specially area will ship a studying to its Fog node. It is believed that studying a records of numerical price in variety of 19.00 to 19.ninety nine and the studying are dispatched to fog node for aggregation.
It is believed that the Fog node itself isn't compromised and focus on algorithms which make aggregation steady whilst the man or woman terminal nodes is probably compromised and is probably sending fake records to the Fog node. Each records fog node has sufficient computational electricity to run an aggregation set of rules for records forwarding to cloud server.

**FIND COLLUSION ATTACK**

Through the compromised Terminal nodes the adversary can ship fake records to the fog node with a cause of distorting the combination values. Compromised nodes are often in test of one adversary or a colluding enterprise of adversaries, allowing them to launch a sublime attack. The records from attacker node is recognized via way of means of cluster head and it's miles dropped from aggregation. Only valid readings are aggregated and dispatched to Cloud Server.

The following screen shows the application page of cloud server

![Cloud Server Application Page](image1)

The following screen shows the application page of Fog node, which acts as aggregator

![Fog Node Application Page](image2)

Activate node in particular region
The terminal node design is shown in the below screen.

Terminal node established data and sending to Aggregator.
VII. CONCLUSION

In fog computing, fog nodes are the nearest acquirers to the terminal devices, the processed information can be tampered with or illegally captured with the aid of using a few malicious nodes. The proposed paintings is a stable information question framework for cloud and fog computing. We use cloud carrier to test queried information from fog community whilst fog community affords queried information to users. In our framework, a person can also additionally rapid reap the desired information from the fog community, after which the cloud carrier should pattern a few information from the fog community to test the very last consequences and affords them to the person. Based on the safety necessities of fog computing, our proposed framework now no longer most effective ensures the reliability of information however additionally correctly protects information towards man-in-the-center assault, unmarried node assault and collusion assault of malicious users. Also, the experiments display our framework is powerful and efficient.

VIII. FUTURE ENHANCEMENT

As destiny paintings, we plan to analyze the opportunity alternatives method in addition. We additionally plan to in addition lessen the computational price with the aid of using exploiting partial relationships amongst get admission to manipulate policies (ACPs).

Access manipulation determined to be a sizable mechanism for defensive confidentiality and privateness in cloud computing, coming with appropriate version that would lessen computation complexities at content material proprietor in addition to solve the facts leakage on the cloud server and outsiders, which want non-stop interest and in addition enhancement makes the researches on this subject to get increasingly intensive.
REFERENCES