Study on fog computing: security & privacy challenges in terms of IoT

Jayant Kumar Singh¹, Dr. Amit Kumar Goel²
¹,²Galgotias University, Computer Science, Plot No. 2, Yamuna Expy Sector 17A, Greater Noida, Uttar Pradesh
e-mail: ¹Jayanticfai87@gmail.com,²amit.goel@galgotiasuniversity.edu.in

Abstract. As of late, the idea of (IoT) Internet of Things is pulling in strong consideration because of the gigantic potential. IoT is the systems administration of physical devices that are both associated and smart. Threats and Security issues are a constant problem faced in cloud computing these days, but in total assurance it’s not yet completely researched. Cisco made the term ‘Fog Computing’ which is nothing but an extension of Cloud Computing to the system edge. Along with the enormous advancements in IoT, current Cloud frameworks face different disadvantages, for example, absence of versatility support, area mindfulness, geo-dissemination, high latency, just as digital dangers. Fog computing extends cloud computing, cloud computing give data, figure, stockpiling, and application administrations to end-user, additionally the fog computing likewise offer the types of assistance like process, data, application and capacity to end user. In this manner, fog computing might be viewed as decision for empowering the IoT to offer proficient and safe types of assistance for some IoT users. This paper dissects the difficulties and issues that are looked by Fog calculation regarding privacy and security in detail

Keywords: Cloud Computing, Fog Computing, Privacy & security Issues, IoT, etc.

1. Introduction
The internet’s innovation is one of humankind’s most esteemed achievements. The internet has changed the PCs, communication technology & communication like nothing has ever previously. Handling the data system worldwide is possible today because of Fog Computing on the cloud-to-endpoint continuum, as accordingly it allows us to make high level competent designs overcoming the IoT restrictions. As the IoT is described by restricted calculations as far as preparing capacity & power, it experiences numerous issues, For instance, security, dependability, execution, & privacy. In spite of all the advancements in the system computing of Fog still faces some of the Security & privacy issues including secure authentication, authorization, classification of data and communication [11]. Issues privacy & Security will slack advancement of fog computing if not very much tended to. Since fog computing is proposed with regards to IoT, and started from cloud computing, cloud privacy & security issues are acquired in fog computing. As fog computing is still in its newborn child stage, there is little work on issues of privacy & security. Figure 1 depicts the connection among IoT and Fog Computing.
2. Fog Computing

Fog computing is commonly considered as a non-inconsequential augmentation of cloud computing through centre system to the edge arrange. Fog computing was initially planned as an expansion of cloud computing with extra figure, communication & storage assets found near the end users. Edge & Fog computing being extended type of cloud computing offers answers for the difficulties looked by cloud computing that is appealing for Industrial-IoT ongoing applications [3]. The terms Edge & Fog computing are frequently utilized by industry conversely. Both these computing advancements leads to computing & preparing abilities close to the region where data begins. Fog computing is generally helped out cloud computing. Thus, end users, cloud and fog together structure a three layer administration conveyance model, as appeared in Figure 2.

For the most part, Fog computing dwells nearer to the devices or sensors of IoT and extends the cloud based computing, stockpiling and systems administration offices. Difficulties in Fogs going about as a moderate layer between device of IoT & cloud datacenters & audit present advancements in this field. The principle reason for this innovation was to help the particular needs of latency-basic applications, for example, enlarged reality, and IoT applications which produce monstrous volumes of data that are unfeasible to send to faraway cloud data communities for investigation [5].

At long last, in the period of big data, fog computing can bolster edge examination and stream mining, which can process and decrease data volume at a beginning period, in this manner spare bandwidth and chop down postponement.
3. Fog Computing and IOT Challenges

Recent concentrated cloud computing design is confronting extreme applications difficulties in Internet of Things. For example, it needs awareness in area as it is a unified model. Fog computing can indicate these difficulties. Furthermore, it can't bolster IoT time-touchy applications, for example, gaming, expanded reality and streaming of video.

The incorporation of Internet of Things & fog computing will carry numerous benefits to diverse applications of IoT. To build the effectiveness of applications of IoT, the greater part of the data produced by these objects/devices of IoT must be prepared and investigated continuously [7]. Fog computing goes about as a scaffold between large-scale cloud computing & devices of IoT and capacity administrations. The fog bolsters constant IoT devices communications to decrease latency, particularly for time-touchy applications of IoT. The accompanying Figure 3 shows the favorable circumstances that are given by Fog Computing to IoT.

### Table 1: Comparison: Fog and Cloud Computing

| Particulars          | Fog Computing                  | Cloud Computing              |
|----------------------|--------------------------------|------------------------------|
| **Hardware**         | Computing Power and Storage is limited | Computing Power and Storage is Scalable |
| **Latency**          | Low                            | High                         |
| **Server and Client Distance** | One hop                       | Multiple hops                |
| **Server Nodes Location** | On the Local Network edge      | Within Internet              |
| **Measures of Security** | Not Defined Easily            | Can easily be defined        |
| **Environment of Working** | Indoor or Outdoor             | Air conditioning systems with building of the size of Warehouses |
| **Awareness of Location** | Yes                           | No                           |
| **Deployment**       | Distributed                    | Centralized                  |
| **Data Attack**      | Probability is High           | Probability is Less          |

![Figure 3: Customer Services Efficiency Improvement through Fog Computing in IoT](image)

### 3.1 Privacy & security in IoT

#### End User Privacy

Saving the privacy of end user's is a huge fog computing issue faces as fog hubs are nearer to end users, which permits them to gather progressively delicate data including money related records, personality, utilization of utilities, area and others. Besides, as fog hubs are disseminated in large regions, keeping up concentrated control is troublesome. Unbound fog hubs can be the passage point for an assailant who can get into the system and take user data that are traded among fog objects. More research is required in Ensuring fog privacy hubs is difficult.

#### Security
There are very much read cloud computing issues of security for that assimilate critical measures of security to ensure in cloud. Nonetheless, measures are not appropriate for fog computing because of its diverse quite portability, attributes, large-scale geo-dispersion and heterogeneity. Furthermore, the fog is an engaging objective for digital aggressors since large volumes are contained in the fog of delicate data from both the IoT and cloud devices. In this manner, more research is required to improve security in fog.

4. Privacy & Security Challenges in Fog Computing

Following are the Security & Privacy Challenges that faced in Fog Computing are stated below:

- **Security of Network:** Nodes of Fog are conveyed at the Internet edge, which certainly carry system’s substantial weight to the executives, envisioning the expense of keeping up huge scope servers of cloud which are disseminated everywhere throughout the system edge without simple access for upkeep. Because of remote in fog networking prevalence, remote system security is big worry to fog networking. Those attacks can be tended to in the exploration area of remote system, which isn’t in the extent of this overview. Model attacks are sniffer, sticking, attacks, and so forth.

- **Trust:** Trust accept a vital part in empowering relations considering past relationship among fog nodes and edge contraptions. A fog node is viewed as the most critical part as it is answerable for ensuring security and anonymity for end customers. Furthermore, this part ought to be trusted for completing its assignment, as they ought to be ensured that the fog node performs the overall coverless process on their released data and releases just non-compromising activities. This requires a specific level of trust among all nodes that work inside the system of fog [7].

- **Authentication:** Authentication of organized devices bought in to services of fog is one of the chief prerequisite in fog arrange. To get to the services of a fog arrange, a device needs to initially turn out to be a piece of the system by confirming itself to the fog organize. This is fundamental to forestall the passage of unapproved nodes. It turns into a considerable difficulties as the devices associated with the system are obliged in different manners including force, handling and capacity.

- **Forgery:** Malicious attackers may fashion their personalities and profiles, yet in addition create counterfeit data to misdirect different substances. What’s more, the system assets, for example, bandwidth, stockpiling and energy, would be too much devoured dependent on the faked data.

- **Insecure APIs:** Many Fog/Cloud suppliers uncover APIs (Application Programming Interfaces) for client use. The APIs security is essential to the actualized applications security.

- **Privacy of Identity:** The user identity incorporates location, name, visa number, phone number, public-key endorsement to keep secure this data of user it’s very challengeable.

- **Problem of Malicious Fog Node:** In request to manage the cost of user service, fog nodes process data got from the IoT devices. On the off chance that outstanding task at hand is overwhelming it is partitioned and handled by a few fog nodes. On the off chance that some fog nodes are agitated by malicious user it is hard to guarantee the completeness of data. Along these lines, before calculation starts, fog nodes must trust each other for which authentication convention is required [10].

- **Fog Computing Environments-Malicous Detection Technique:** When some nodes of fog are undermined, cross breed detection procedure is helpful to recognize node’s malicious code of fog. It is joined with detection that is signature-based strategy & conduct based detection method. Be that as it may, IoT devices have low computing power. The conduct based detection method costs largely overhead. While signature-based detection method is more effective than it. Nonetheless, it is hard to identify different types of the malicious code in fog nodes. So as to supplement this issue, some calculation of conduct based detection procedures that is running on the cloud is dispersed into fog nodes. Suspected malware documents on a fog node are sent to cloud. On the off chance that the record is new malware, a consequence of examination is put away in the signature database. The outcome is transmitted to the fog node and refreshed signature data.

- **Attacks of Replay:** the enemy can be transmitted data to the goal node by utilizing malicious node or device with legitimate data of recognizable proof which has been accomplished by the objective node, in a mission to make the malicious node or device to pick up the trust of Fog organize. Replay attacks are regularly presented during the time spent authentication to demolish the distinguishing proof legitimacy. In Fog arrange, more plans (secure time stamp plans, and so on.) ought to be planned and created to alleviate the replay attack.

- **Assault:** Gadgets and Devices with nodes of fog are conveyed a wide range of spots including those where assurance is frail or missing. Subsequently they may confront malicious assaults. Likewise, a poisonous customer can either record off-base or bogus readings, parody IP locations and addresses or change its own smart meter.

- **Fortification of Network:** In perspective on the enormity of remote networking in fog computing, remote structure or remote system security is gigantic worry to fog computing. Attacks or strikes like sticking, sniffing can be tended to in the assessment scope of remote networks.
Privacy of Location Data: Currently, huge applications on cell phones gather location of the users' data. It appears that privacy of the location is a sort of privacy which is needed to forfeit so as to appreciate online services, for example, route and location-based services. In any case, location privacy safeguarding is basic without a doubt.

Attacks of Sybil: Fog networks are large scope shared networks, which has capacity to bargain the malicious user. The malicious user is known as Sybil node has guaranteed numerous recognizes to bargain the entire system. Sybil device has numerous legitimate personalities; bogus data that was transmitted by the Sybil device can without much of a stretch be gotten by their prompt neighboring devices. Curiously, just a solitary way is resolved and all the data that has been transmitted requires experiencing the Sybil device, wherein sticking and DoS can be utilized. Secure distinguishing proof and authentication components should have been produced for Fog frameworks to defend against Sybil attacks.

Fog computing engineering can conquer the security difficulties of the IoT cloud design somewhat. The enhancements in fog computing will assist us with implementing the IoT. The essential thought of this technology is making all the physical devices interface with internet and make them smart to construct the smart world. It is speculative circumstance to demonstrate the security of fog. Fog computing has numerous difficulties to survive and give the general security to the users [9]. Sooner rather than later IoT-Fog-cloud design will be generally utilized as increasingly more IoT devices are created and the expanding demand for quick calculation.

5. Research Method
3.1 Introduction
In this Study an improved adaptation of Bloom Filter was utilized to safeguard the Location of Fog Server Privacy. The value of query created changes area of same query and send to server for the handling. Here changed the vector counter of the area the value of M-counter put away in the vector with the index value of an approaching query and server continues information. Transform area is essentially an approval purpose of region of interest & position of interest. The size of LBP vector is deducted by the size of M*k grid. It is a most extreme cutoff for accepting query. In the wake of getting the value of change counter check the greatest successive change value of transform. In this time term process the greatest change frequent value of the M-counter and produce the close to area as per the query.
3.2 Model Flow Diagram

Algorithm Process
Where:
H(x) = Query Index
e = M-counter Frequent Value Change
SA = Result Query
I = Frequent Counter Value Time Duration Hop
Transform Query Value Generation:

\[ SA = \sum_{i=0}^{F(e)} (hf(e) \times ti) \]

At the point when a counter estimation of filter (M) is turn on and turn off the recurrence of checking e is coming it is need to embed e into LBP information structure. At the point when the estimation of e creates question rub then the estimation of e is expelled from the LBP information structure. Algorithm: - embedding frequency of counter e.
Input LBP, e, T
Outputs update LBP and SA
i < -0;
while (i < T(e))
    temp < −LBP(e)
    if (temp < Ti) then
        LBPi. add(e)
        Return LBP, T
    End if;
    LBPi. remove (e,temp)
    T. increase(e);
    i + +
end while
LBP. add(e);
T. add(e, i);
Return LBP, T
Now the result query is captured and transforms result of frequent element e value from LBP vector
6. Analysis and Results
4.1 Analysis
To assess the performance of distributed computing strategies in distributed computing condition for the augmentation of server, here we are utilizing different quantities of fog based figuring topology for the reason a simulation with a proposed strategy. To collaborate with different administrations in the Fog computing and to keep up the privacy of server area in cloud condition. For the further correlation and execution for execution assessment we utilized java programming dialects with Net Beans IDE 8.0.1 apparatuses for complete outcomes/usage process. Visit component e esteem from LBP vector.

Fig. 1. Proxy Server with Fog Server Process Block Diagram

Fig. 2. Implementation Work: Post-Physical Topology Importation in Browsed Topology
This Topology Consists of Proxy Fog Server and Intermediate Server for Location Preservation with Data Actuator.
Table 2: BM Method Evaluation of Performance

| Value of Node | 2     | 1     | 5     | 4     | 3     |
|---------------|-------|-------|-------|-------|-------|
| Maximum Capacity | 0.28  | 0.35  | 0.08  | 0.15  | 0.2  |
| Random        | 0.28  | 0.35  | 0.08  | 0.15  | 0.2  |
| Lowest Latency | 0.2   | 0.3   | 0.02  | 0.05  | 0.12 |

Diverse Latency Value Shows the Fog Node Behaviors Server Connected.

Table 3: SA Method Evaluation of Performance

| Value of Node | 2     | 1     | 5     | 4     | 3     |
|---------------|-------|-------|-------|-------|-------|
| Maximum Capacity | 0.28  | 0.35  | 0.08  | 0.15  | 0.2  |
| Random        | 0.28  | 0.35  | 0.08  | 0.15  | 0.2  |
| Lowest Latency | 0.17  | 0.25  | 0.001 | 0.04  | 0.08 |

The Maximum Capacity of Fog Node Indicate The Performance Behaviors of Data Preservation During the Processing of Fog to Proxy Server.

Fig. 3. BM Method Evaluation of Performance: Graphical Representation
4.2 Result Discussion
Bloom filter is fundamentally information structure and guide the single piece data. We proposed area privacy protection algorithm utilizing improved bloom filter. The proposed algorithm jam area privacy at low computational and communication cost. In this examination altered the bloom filter for the preparing of privacy protection in area based administrations. The proposed algorithm approved the genuine area of privacy conservation. The proposed algorithm utilized the estimation of counter for the procedure of user area question agreeing. The proposed strategy is productive for the area and position privacy. The change estimation of inquiry creates the close to estimation of user area and jam the genuine area of user.

A key element of the framework is that we dispose of the completely confided in substances to give upgraded security.

5. Conclusion
The Research Study feature the difficulties looked by this developing field of security & privacy issues in fog computing & IoT. IoT is an ever-developing field. Fog and edge computing have begun substituting traditional cloud computing for the calculation of data from IoT devices. Devices of IoT have capabilities of processing and are dynamic in nature & restricted stockpiling. Be that as it may, with a bunch of data coming right away soon, we should find new calculation strategies remembering the privacy and security of the user data first before anything else. Thus, the present security province of Fog networks don't fulfill the advanced security prerequisites. The successful intermingling of Fog Computing & IoT has numerous advantages for Distinct Apps of Internet of Things, if the issues are investigated before long be managed. The current security measures have experienced thorough testing, and utilizing them can possibly guarantee that any Fog framework fulfills fundamental mechanical security standards. Later on, edge and fog computing ought to supplant traditional cloud computing however much as could reasonably be expected.

References
[1] Dastjerdi, A., H. Gupta, R. Calheiros, S. Ghosh, and R. Buyya. 2016. Chapter 4—fog computing: Principles, architectures, and applications. In Internet of Things: Principles and Paradigms, ed. R. Buyya, and A.V. Dastjerdi, 61–75. New York: Morgan Kaufmann.
[2] Sarkar, S., and S. Misra. 2016. Theoretical modelling of fog computing: A green computing paradigm to support iot applications. IET Networks 5(2): 23–29.
[3] Lu, R., et al. (2012): Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. TPDS 23
[4] Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B. (2017) An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), Porto, Portugal, 24–26 April 2017; pp. 254–260.
[5] Ai, Y.; Peng, M.; Zhang, K. (2017) Edge cloud computing technologies for internet of things: A
[6] Skarlat, O.; Schulte, S.; Borkowski, M.; Leitner, P. (2016) Resource provisioning for IoT services in the fog. In Proceedings of the 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications, SOCA 2016, Macau, China, 4–6 November; pp. 32–39.

[7] Liu, Y.; Fieldsend, J.E.; Min, G. (2017) A Framework of Fog Computing: Architecture, Challenges and Optimization. IEEE Access, 4, 1–10.

[8] Puliafito, C.; Mingozzi, E.; Anastasi, G. (2017) Fog Computing for the Internet of Mobile Things: Issues and Challenges. In Proceedings of the 2017 International Conference on Smart Computing (SMARTCOMP), Hong Kong, China, 29–31 May; pp. 1–6.

[9] 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 Commun. Surv. Tutor. 20, 416–464.

[10] Atlam, H.F.; Alenezi, A.; Hussein, R.K.; Wills, G.B. (2018) “Validation of an Adaptive Risk-Based Access Control Model for the Internet of Things. Int. J. Comput. Netw. Inf. Secur., 10, 26–35.

[11] Wen, Z.; Yang, R.; Garraghan, P.; Lin, T.; Xu, J.; Rovatsos, M. (2017) Fog orchestration for internet of things services. IEEE Internet Comput., 21, 16–24.

[12] Mukherjee, M.; Shu, L.; Wang, D. (2018) Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. IEEE Commun. Surv. Tutor, PP