International Journal of LNCT, Vol 2(5)
ISSN (Online): 2456-9895

Current fog computing challenges for location privacy preservation in cloud networks

Diksha Singh Gour [1] and Vineet Richhariya[2]
M. Tech. Scholar, Department of Computer Science LNCT, Bhopal, India[1]
Professor, Department of Computer Science LNCT, Bhopal, India[2]

Abstract
In the current decade the mobility of communication devices faces a problem of location privacy preservation. Fog computing extends the edge network of cloud computing. Fog computing faces new security and privacy challenges besides those inherited from cloud computing. The edge network of cloud computing has multiple servers in form of mobility. The mobility of edge server is an open stack communication. The open stack communication invites security threats and malware software for the denial of services delivered by fog computing. This paper presents the review of location privacy preservation techniques in fog computing based on different location scenario and different cryptography techniques for location preservation of edge servers and edge device.

Keywords
Fog computing, Edge devices, LBS, Privacy, Cloud, Networks.

1.Introduction
Fog computing is a distributed computing paradigm that extends the services provided by the cloud to the edge of the network [1]. It enables seamless leveraging of cloud and edge resources along with its own infrastructure. It facilitates management and programming of computer, networking and storage services between data centres and end devices. Fog computing essentially involves components of an application running both in the cloud as well as in devices between endpoints and the cloud, i.e. smart gateways and routers [3]. Fog computing supports mobility, resource and interface heterogeneity, interplay with the cloud, and distributed data analytics to address the requirements of applications that need low latency with a wide and dense geographical distribution [7]. There are a number of benefits associated with Fog computing that assures its success. The first benefit is the reduction of network traffic. An uncontrolled increase in network traffic may lead to congestion and result in increased latency. Fog computing provides a platform for filtering and analysis of the data generated by sensors by utilizing resources of edge devices. This drastically reduces the traffic being sent to the cloud by allowing the placement of filtering operators close to the source of data [14]. Considerable reduction in propagation latency is the next important advantage of utilizing the Fog computing paradigm, especially for mission critical applications that require real-time data processing. The Fog-Network (FogNet) was initiated by Cisco to enable the fog computing technology at the edge of the network. The main characteristics of FogNet include ubiquity, decentralized management and cooperation. FogNets are composed of many devices connecting to Internet like IT devices, wearable devices and self-driving vehicles, etc. These devices form many ‘‘mini clouds’’ at the edge of the network and manage themselves in a distributed way [4, 9, 12].

The popularity of mobile devices in people’s daily life has motivated a series of applications, especially in energy-efficient mobile cloud computing. It is a common belief that when a person comes to an unfamiliar place, he/she wants to know if there is a supermarket or hotel nearby [8]. Location based services (LBS) are used to address this issue. Usually, mobile users continuously send queries to cloud LBS servers. If they order this information according to sequences of time and positions, users’ trajectory information can be obtained, which may pose a threat to these users if such data is leaked. For example, concerning check-in applications: many shops encourage users to check-in, and provide points to users for discounts [3]. The rest of paper is organized as section II which shall discuss the related work. Section III discusses edge communication models. Section IV discusses the analysis & survey, Section V future expectation and finally discusses conclusion in section VI.

2.Related work
Tian Wang, Jiandian Zeng, Md Zakirul Alam Bhuiyan, Hui Tian, Yiqiao Cai, Yonghong Chen and Bineng Zhong Et al. in [1] take the principles of similarity, intersection, practicability, and correlation into consideration and design a dummy rotation algorithm with several properties. Among the concerns about LBS privacy preservation, trajectory privacy preservation is a critical topic. Discussed to use a fog server to store partial important data that

can be physically controlled by users. A dummy rotation algorithm is designed considering the principles of similarity, intersection, practicability and correlation. Specifically, there are two types of insurances in the discussed fog structure. The simulation results show that the discussed method can achieve enhanced privacy preservation. Moreover, approximately 10% to 15% of the data can be stored on the local fog server to prevent restoration of the data by attackers.

Ivan Stojmenovic and Sheng Wen Et al. in [2] elaborated the motivation and advantages of Fog computing and analyses its applications in a series of realistic scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. Discuss the state-of-the-art of Fog computing and similar work under the same umbrella. Security and privacy issues are further disclosed according to current Fog computing paradigm. As an example, study a typical attack, man-in-the-middle attack, for the discussion of security in Fog computing. Investigate the stealthy features of this attack by examining its CPU and memory consumption on Fog device.

T.Rajesh Kanna, M. Nagaraju and Ch. Vijay Bhaskar Et al. in [3] discussed a different approach to securing data in the cloud using offensive decoy technology. Monitor data access in the cloud and detect abnormal data access patterns. When an unauthorized access is suspected and then verified using challenge questions, launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Discussed this paradigm in detail and review the work that has been done using this technology.

Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis Et al. in [4] present a novel approach to securing personal and business data in the Cloud. Discussed monitoring data access patterns by profiling user behaviour to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected and later verified, with challenge questions, for instance, inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology could provide unprecedented levels of security in the Cloud and in social networks.

Jiawen Kang, Rong Yu, Xumin Huang and Yan Zhang Et al. in [5] presented a privacy-preserved pseudonym scheme with a hierarchical architecture to achieve pseudonym management at the network edge. Geo-distribution authorities for pseudonym management are deployed in pseudonym fogs. Pseudonyms are generated and distributed to vehicles in time. For secure and efficient pseudonym management, secure communication protocols for privacy-preservation are designed in F-IoV. Finally, present a context-ware pseudonym changing game for vehicles to change pseudonym with context awareness. The security analysis shows that discussed scheme provides secure communication and privacy preservation for vehicles. Numerical results indicate that the scheme outperforms the existing pseudonym management schemes in terms of improving the vehicles' location privacy and reducing communication overheads.

Thanh Dat Dang and Doan Hoang Et al. in [6] presented a data protection model for fog computing to protect data and handle mobility. The model features a Region-Based Trust-Aware (RBTA) model for trust translation among fog nodes of regions, a Fog-based Privacy-aware Role Based Access Control (FPRBAC) for access control at fog nodes, a mobility management service to handle location requests at a region. In order to deploy their framework in practice, providing high availability of fog services and resources and up-to-date location services needs to be taken into account to address the sensitive-response requirement. The experimental outcomes demonstrated the feasibility and efficiency of the model.

M. Yannuzzi, R. Milito, R. Serral-Graci`a, D. Montero and M. Nemirovsky Et al. in [7] examines some of the most promising and challenging scenarios in IoT and shows why current compute and storage models confined to data centres will not be able to meet the requirements of many of the applications foreseen for those scenarios. Their analysis is particularly centred on three interrelated requirements: 1) mobility; 2) reliable control and actuation; and 3) scalability, especially, in Internet of Things (IoT) scenarios that span large geographical areas and require real-time decisions based on data analytics. Based on their analysis, expose the reasons why Fog Computing is the natural platform for IoT and discuss the unavoidable interplay of the Fog and

the Cloud in the coming years. In the process, review some of the technologies that will require considerable advances in order to support the applications that the IoT market will demand.

Shanhe Yi, Cheng Li and Qun Li Et al. in [8] survey discusses definitions of fog computing with similar concepts, gives representative applications which will promote fog computing, and mentions various aspects of issues, may encounter when design and implement fog computing systems. Besides, new opportunities and challenges in fog computing for related techniques are discussed and issues related to QoS, interfacing, resource management, security and privacy are highlighted. Fog computing will evolve with the rapid development in underlying IoT, edge devices, radio access techniques, SDN, NFV, VM and Mobile cloud. Think fog computing is promising, but currently need joint efforts from underlying techniques to converge at fog computing.

Mohammad Aazam and Eui-Nam Huh Et al. in [9] Fog computing plays an important role. Fog resides between underlying IoT and the cloud. Its purpose is to manage resources, perform data filtration, pre-processing, and security measures. For this purpose, Fog requires an effective and efficient resource management framework for IoTs, which provide in this paper. Their model covers the issues of resource production, customer type-based resource estimation and reservation, advance reservation, and pricing for new and existing IoT customers, on the basis of their characteristics. The implementation was done using Java, while the model was evaluated using CloudSim toolkit. The results and discussion show the validity and performance of their system.

Shanhe Yi, Zhengrui Qin and Qun Li Et al. in [10] the paper discusses several security and privacy issues in the context of fog computing, which is a new computing paradigm to provide elastic resources at the edge of network to nearby end users. Discuss security issues such as secure data storage, secure computer and network security. Also highlight privacy issues in data privacy, usage privacy, and location privacy, which may need new thinking to adapt new challenges and changes.

Jianbing Ni, Aiqing Zhang, Xiaodong Lin and Xuemin (Sherman) Shen Et al. in [11] the architecture, applications, and especially security, privacy, and fairness of fog-based vehicular crowd sensing. Specifically, first introduce the overall infrastructure and some promising applications, including parking navigation, road surface monitoring, and traffic collision reconstruction. Then study the security, privacy, and fairness requirements in fog-based vehicular crowd sensing, and describe the possible solutions to achieve security assurance, privacy preservation, and incentive fairness.

Ting He, Ertugrul N. Ciftcioglu, Shiqiang Wang and Kevin S. Chan Et al. in [12] studied the problem of protecting the location privacy of a mobile user in MECs using chaff services. Assuming that a cyber eavesdropper tracks the user by performing ML detection among observed service trajectories, examined a range of chaff control strategies, from a baseline strategy to an optimal strategy. Proved that the optimal strategy can reduce the eavesdropper's tracking accuracy to zero when the user's mobility is sufficiently random, while simpler strategies cannot. Their evaluations highlighted the dependency of the tracking accuracy of the user's mobility model, and verified the efficacy of their solutions in protecting the location privacy, even for users with highly predictable mobility.

Jianbing Ni, Kuan Zhang, Xiaodong Lin and Xuemin (Sherman) Shen Et al. in [13] examine fog-assisted IoT applications based on different roles of fog nodes. Then, present security and privacy threats towards IoT applications and discuss the security and privacy requirements in fog computing. Further, demonstrate potential challenges to secure fog computing and review the state-of-the-art solutions used to address security and privacy issues in fog computing for IoT applications. Finally, by defining several open research issues; it is expected to draw more attention and efforts into this new architecture.

Mithun Mukherjee, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury and Vikas Kumar Et al. in [14] the existing security and privacy measurements for cloud computing cannot be directly applied to the fog computing due to its features, such as mobility, heterogeneity, and large-scale GEO-distribution. This paper provides an overview of existing security and privacy concerns, particularly for the fog computing. Afterward, this survey highlights ongoing research effort, open challenges, and research trends in privacy and security issues for fog computing.

Hung Caoa, Monica Wachowicza, Chiara Rensob and Emanuele Carlini Et al. in [15] the paper discuss the characteristics of the analytical tasks at each layer. Notice that the amount of data being transported on the network decreases going from the

edge, to the fog and finally to the cloud, while the complexity of the computation increases. Such design allows to support different kind of analytical needs, from real-time to historical according to the type of resource being utilized. Implemented the discussed architecture as a proof-of-concept using the transit data feeds from the area of Greater Moncton, Canada.

3.Fog communication model

It envisions a dynamic IoT platform, which allows us to dynamically and efficiently change the programs/algorithms inside in the IoT devices. It proposes to adopt the concept of fog computing to implement it. The fog computing concept is discussed for IoT and generalized by Vaquero Et al. Fog computing leverages fog devices in data centres, edge networks, and end devices simultaneously, as illustrated in figure [11]. The fog devices are managed by a centralized server, which receives requests from users and decides how to serve the requests on the fog devices. The heterogeneous fog devices help us to pre-process the data in the resource-limited devices, including the edge networks and end devices. Moreover, the fog computing platform extends cloud to end devices, which are closer to end users, and result in lower latency. Shen et al. implements a simple fog computing platform to demonstrate the benefits of latency compared to the cloud [5-6].

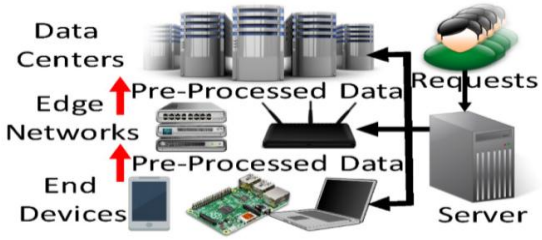

Figure 1 Considered fog computing platform

Implementing the fog computing platform that supports heterogeneous devices, in which the actual configurations of the devices and inter-connected networks need to be carefully optimized, resulting in several challenges. Firstly, because of the limited resources of the devices, they must split requests from users into smaller modules running on the devices. These modules collaborate among one another to fulfill the requests [3, 10]. Making decisions on de-compositions of requests is hard, because the large secured space and dynamic nature of the platform. Secondly, they must connect the modules, which are deployed on different devices. Building the flow among modules is a difficult task, as the networks are heterogeneous and dynamic [8].

4.Analysis & survey

The integration of network enriched the services of edge-based devices. The edge-based devices work as extension of cloud computing is called fog computing. The process of fog computing supports the concept of mobile servers for the facilitation of cloud-based services in local as well as global level.

Table 1Approach limitation

S. No.	Authors	Approach	Limitation	Challenges
1.	Tian Wang, Jiandian Zeng, Md Zakirul Alam Bhuiyan, Hui Tian, Yiqiao Cai, Yonghong Chen And Bineng Zhong	Dummy rotation algorithm	Trajectory privacy preservation is a critical issue when using location-based services	Users have no physical control of the TTP
2.	Ivan Stojmenovic and Sheng Wen	Game-Theoretic Energy Schedule (GTES) method	Environment Settings of Stealth Test	Compute and storage may be inspired in to handle data intensive services based on the interplay between Fog and Cloud
3.	T.Rajesh Kanna, M. Nagaraju and Ch. Vijay Bhaskar	Security mechanism makes use of two concepts known as user behaviour profiling and decoys.	Protects against the misuse of the user's real data	They did not generate the decoys on demand at the time of detection
4.	Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis	Monitoring data access patterns by profiling user behaviour to determine if and when a malicious	Decrease the value of that stolen information to the attacker	Real data also serve as sensors to detect illegitimate access

S. No.	Authors	Approach	Limitation	Challenges
		insider illegitimately accesses someone's documents in a Cloud service		
5.	Jiawen Kang, Rong Yu, Xumin Huang and Yan Zhang	Provides secure communication and privacy preservation for vehicles	Aim to address location privacy issues in IoT	Discussed scheme is not very applicable to situations with sparse vehicles

5.Future expectation

In future research work can be done on the further issues which were identified during above analysis. The major challenges for edge device servers are preserving the location of the servers from the side of the attacker and illegal access of network. In current research trend various authors gives the process of geometrical solution for the location preservation. Mapping location of coordinates plays an important role for privacy preservation, the mapping of coordinates faced certain problem discuss here [3, 5, 6].

1. The coordinates of area of interest in MAP: An easy way to get coordinates for a "Point of Interest" (POI) is to use Google Maps, or even easier, Google Earth.
2. Point of interest in MAP: Point of interest (POI) or POI Mapping is referred to data set that is quick, easy and accurate way to populate the mapping project with important places of feature/buildings/ landmarks. POI data supports a range of application including digital mapping enhanced routing products and validation of databases. POI also known as feature of interest data supports a range of application including digital mapping.
3. Transformation value of POI
4. Number of user processing
5. Location based processing: A location-based service (LBS) is a software-level service that uses location data to control features. As such LBS is an information service and has a number of uses in social networking today as information, in entertainment or security, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device

6.Conclusion

The applicability of the Internet of Things is increasing in every field on a day to day basis. The success story of the internet of things depends on the performance of edge devices and wireless communication media. The major supporting technology of the internet of things is fog computing. The fog computing provides edge devices for the processing of data to IoTs based services. The major issue in fog computing is poor quality of services and low latency of data rate. The poor quality of service depends on the available resources in fog environments. The future of fog computing depends on the future of location privacy preservation of fog computing.

References

[1] Wang T, Zeng J, Bhuiyan MZ, Tian H, Cai Y, Chen Y, Zhong B. Trajectory privacy preservation based on a fog structure for Cloud location services. IEEE Access. 2017; 5:7692-701.

[2] Stojmenovic I, Wen S. The fog computing paradigm: Scenarios and security issues. In computer science and information systems (FedCSIS), Federated conference on 2014 (pp. 1-8). IEEE.

[3] Kanna TR, Nagaraju M, Bhaskar CV. Secure Fog Computing: Providing Data Security. IJRCCT. 2015; 4(1):053-5.

[4] Stolfo SJ, Salem MB, Keromytis AD. Fog computing: mitigating insider data theft attacks in the cloud. In Security and Privacy Workshops (SPW), 2012 IEEE Symposium on 2012 (pp. 125-8). IEEE.

[5] Kang J, Yu R, Huang X, Zhang Y. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Transactions on Intelligent Transportation Systems. 2017.

[6] Dang TD, Hoang D. A data protection model for fog computing. In fog and mobile edge computing (FMEC), Second international conference on 2017 (pp. 32-8). IEEE.

[7] Yannuzzi M, Milito R, Serral-Gracià R, Montero D, Nemirovsky M. Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing. In computer aided modeling and design of communication links and networks (CAMAD), IEEE 19th International Workshop on 2014 (pp. 325-9). IEEE.

[8] Yi S, Li C, Li Q. A survey of fog computing: concepts, applications and issues. In proceedings of the 2015 Workshop on Mobile Big Data 2015 (pp. 37-42). ACM.

[9] Aazam M, Huh EN. Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. In advanced information networking and

applications (AINA), 2015 IEEE 29th international conference on 2015 (pp. 687-94). IEEE.
[10] Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: a survey. In International Conference on Wireless Algorithms, Systems, and Applications 2015 (pp. 685-95). Springer, Cham.
[11] Ni J, Zhang A, Lin X, Shen XS. Security, privacy, and fairness in Fog-based vehicular crowdsensing. IEEE Communications Magazine. 2017; 55(6):146-52.
[12] He T, Ciftcioglu EN, Wang S, Chan KS. Location privacy in mobile edge clouds. In distributed computing systems (ICDCS), 2017 IEEE 37th international conference on 2017 (pp. 2264-9). IEEE.
[13] Ni J, Zhang K, Lin X, Shen X. Securing fog computing for internet of things applications: Challenges and solutions. IEEE Communications Surveys & Tutorials. 2017.
[14] Mukherjee M, Matam R, Shu L, Maglaras L, Ferrag MA,et al. Security and privacy in fog computing: Challenges. IEEE Access. 2017; 5:19293-304.
[15] Cao H, Wachowicz M, Renso C, Carlini E. An edge-fog-cloud platform for anticipatory learning process designed for Internet of Mobile Things. arXiv preprint arXiv:1711.09745. 2017.