Fog Computing Security and Privacy Issues: A Survey

ISSN (e) 2520-7393
ISSN (p) 2521-5027
Received on 18st Dec, 2019
Revised on 27th Dec, 2019
www.estirj.com

Mudassar Hafeez[1], Irshad Ahmed Sumra[2]

Department of Computer Science Bahria University Lahore Campus.

Email address: mudassarwisky@gmail.com[1] , isomro28@gmail.com[2]

Abstract: Fog computing is referring to spreading cloud computing to the edge of an originality's network. It is basically a devolved research paradigm where knowledge, storage and software are spread in the absolute most defined, effective position between the information supply and the cloud. Besides the Similarities to cloud computing, it has some distinctiveness which makes the fog computing to experience new security and privacy challenges. This paper describes the definition of fog computing and similar perception, commences about application scenarios, and identifies security and privacy challenges in fog based computing systems.

Keywords: *Fog computing, Cloud computing, Mobile edge computing, Cloudlet*

1. Introduction

The visualization of fog computing has been delivered by Cisco whose main purpose is to facilitate applications on trillions of linked devices to perform directly within the network edge that happen to be previously connected while in the Internet of Things (IoT). Fog computing is considered a growth with the cloud computing model from the biggest market of network in your border together with the network during the considered Cisco. Cisco puts outdoors source and network operating-system together inside a networked device. Many developers got encouraged with this open application environment and carry her / his developed applications and connectivity interfaces while in the network edging. In spite of the outcomes of Cisco's practices, we will need to realize as to what the fog computing is as well the differences between cloud and fog. The infrastructure of fog distributed computing permits services to be served at end devices such as access point and let the applications to run as near as feasible. Cloud computing refers to paradigm that do centralized the data and application. It has provided many opportunities for enterprises by giving huge range of computing services to the customers. outcomes of Cisco's practices, we will need to realize as to what the fog computing is as well the differences between cloud and fog. The infrastructure of fog distributed computing permits services to be served at end devices such as access point and let the applications to run as near as feasible. Cloud computing refers to paradigm that do centralized the data and application. It has provided many opportunities for enterprises by giving huge range of computing services to the customers[1][2].

But, Cloud processing is not really a "one-size-fit-all" infrastructure. Issues however occur unsolved because Net of points purposes frequently wants freedom maintain, geographical circulation, consciousness about place and reduced latency. Haze processing is really a new design of spread processing that stretches the cloud processing and broaden it to the system side to help the efficient knowledge accessibility, computation, marketing, and storage. Haze processing show strong association with cloud processing in the shape of characterization. For instance, variable sources like computation, storage and networking are the building blocks of both of them which demonstrate that various technologies implemented in cloud computing can be straightly useful to fog computing. Though, numerous identical properties lie in fog computing that makes it distinguishable from other underlying computing infrastructure. Distance closure to end user is most significant[4].

As an example, flexible resources like computation, networking and storage are the building blocks of both of them which demonstrate that various technologies implemented in cloud computing can be straightly useful to fog computing. Following figure demonstrate a logical architecture of fog/cloud infrastructure. Haze support IoT programs and function various protection function through the healthy mixture of computational energy, connection, and course of control.

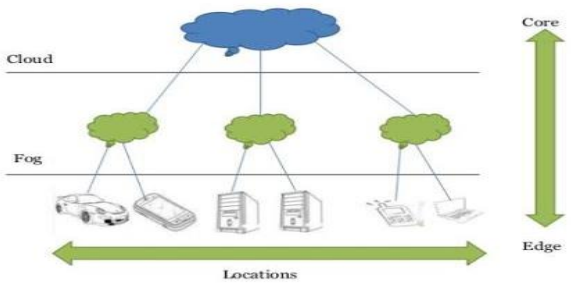

Figure 1. Cloud Architecture [14]

Corresponding author email address: mudassarwisky@gmail.com

Many protection and solitude problems in the perception of cloud research may be estimate to inescapably affect fog research, as fog is contemplating as a non-trivial cloud expansion. Small perform should need to be performed on protection and solitude problems as haze research is considered to stay baby stage. In the perception of Net of Points (IoT), the haze research is predicted and instigated from cloud research and yet in an effect cloud research solitude and protection issues are used in haze computing. While different shown alternatives in the perception of cloud research may handle several protection and solitude problems in haze research, haze because unique traits such as for example freedom help can generate new protection and solitude challenges. On different area, in the perception of IOT a great system could possibly be given by haze research to handle several protection and solitude issues.

We shall speak about many protection and solitude problems in haze research in that report, by studying obtainable perform of fog computing and related work in underlying domain, to recognize privacy and security problems.

The section 2 described the characteristics and related work done on Fog Computing. Section 3 summaries the methods of application of Fog Computing like smart home, smart grid, smart vehicle, health data manager etc. In Section 4, we describe the privacy and security issues of Fog Computing like trust and authentication, network security, secure data storage and privacy related issued etc. and the conclusion of the research describe in Section 5.

2. Overview on Fog Computing

This section provides a brief overview on fog computing by giving its definition followed by some of the characteristics of fog computing.

2.1 Fog Computing

Fog computing is generally known as a visualize extension of cloud computing from the center network to the border network. Fog computing can be defined more comprehensively in a manner having increased exposure of a few significant properties, for example frequency associated with instant gain access to, heterogeneity along with physical syndication, sand-boxed environment along with flexible interoperability, along with large associated with nodes, which will occur out of issues along with systems that should account a fog.

There are a few terms such as mobile cloud computing, mobile edge computing, etc similar to fog computing. Each is explained briefly below.

1) Local Cloud: CLOUD created inside a neighborhood system describes since neighborhood cloud. Them relies upon neighborhood computers on what cloud-enabling computer software are usually working along with primarily support connection using far off cloud. Community fog up is effective correspondingly in order to far off fog up by means of working committed solutions in your area so they can improve this manage of internet data privacy.

2) Cloudlet: Cloudlet describes as “a knowledge middle in a box”, still another processing infrastructure to check out cloud processing product in an even more powerful fashion. It utilizes high-volume hosts which emphasis more on offering solutions to program who sits delay-sensitive, bandwidth limits in locality.

3) Mobile Edge Computing Cellular side processing reveals likeness to Cloudlet. Relatively it's originally located in programs that derive from mobile

4) Mobile Cloud Computing: A compounding of cellular computing, foreign computing and also WIFI computing is well known Mobile cloud computing (MCC). The item brings together prosperous computational options for you to multilevel staff, cellular end users together with computing providers. The main objective is usually to build a strong facility in which the two facts storage space and also facts control carried out over and above smart phones, with the use of computations and also facts storage space out of cell phones for you to cloud.

2.2 Characteristics

Edge location is one of the basic characteristic of fog computing, and that’s why is capable to support low latency requirements applications. Features like wealthy system situation data, such as for example regional system condition, traffic data and data about customer position could be given by side spot that may be used by haze paradigm to supply context-aware optimization. Yet another amazing quality could be the recognition regarding location. Geo-distributed haze node not merely gathers a unique spot but yet another thing it can perform to aid freedom is that the haze node may monitor conclusion consumer product, that might effect a casino game adjusting component for location-based programs and paradigms’. Service delivery and deployment models As being similar to cloud research, we will anticipate that haze research support supply infrastructures might well be categorized in to three organizations: application as solutions (SaaS), software as solutions (PaaS), and infrastructure as solutions (IaaS). We may also foresee the outlined arrangement designs: neighborhood haze, community haze, individual haze and cross haze [1] [3].

There are a few existing works on the idea of fog computing currently. In this paper, we will see some of the related work done. Hong et al have developed a model based on high-level programming for fog computing infrastructure. Mobile Fog contains some occasion handlers and features which can be named by an application. Cellular Haze design is patterned for specific software perhaps not developed as universal design, while escaping out features that agreement with specialized difficulties of

worried picture handling primitives. Haze processing paradigm decreases latency and system traffic.

Stojmenovic, Ivan, and Sheng Wen [2] gives a study on about the motivation and advantages of fog computing and explanation of its applications of actual problems is a series like smart Grid. he also exposed some security problems. he also discusses some attack. This attack would be examined through the impact of strong features on its memory consumption and CPU.

Yi, Shanhe, Zhengrui Qin, and Qun Li [3] explain that the previous study elaborates few security and privacy problems about fog computing, to give flexible resources to nearby consumers at the edge of network. He discusses some privacy problems such as location privacy, data privacy and usage privacies are highlighted for the adoption of new challenges. He also discusses a concise and compact definition the fog occupying technologies as diverse as peer to peer network, sensor network and configuration technologies

J. Zhu, et [4] have offered web applications with dynamic customizable optimization which is founded on mix off client devices and native network conditions composed by fog nodes. With network edge specific knowledge, more dynamic alteration on the user's conditions can certainly be achieved. As a result, a user's Web page providing performance is enhanced ahead of that accomplished by simply applies those methods at the Web server.B. Otten wilder et al. [5] developed a placement and immigration technique for Cloud and Fog resources suppliers. By making plan on the migration further on time it minimizes the network consumption and guarantees end-to-end application-defined latency constraints. They also provide application knowledge of how the complex system of event processing might be used to diminish the necessitate bandwidth of virtual machines between their movement. Operators that are intensive to network are put on distributed Fog devices whereas Operators that are intensive to computationally are in the Cloud. By picking migration goals that guarantee low predicted network utilization for an adequately long time, migration costs are estimated. That function doesn't both enhance how big is flexibility expense or get a grip on data, or doesn't show system get a grip on techniques for obtaining most useful routes for different applications. Additionally, it doesn't use workload flexibility since Haze products will also be ready to transport responsibilities which can be computationally intensive.

Bonomi, F., Miliot, R., Zhu, J[6] gives a study on fog computing and its role in IoT .he said that fog computing is very important for IoT due to some properties like low latency location awareness wide spread of nodes and geographical area and strong use in real time application.

Cao et al. [11] have discovered the usage of fog computing in health examining such as real-time fall recognition. An experimental study has conducted by Mohammed et al. by utilizing fog computing in perspective of storage expansion and computation offloading to support mobile application.

Much more work has done about how rich information is gathered by fog computing infrastructure and also can optimize procedures or immigration for data processing in fog computing.

Ha, et al. [13] have explored and implemented a real-time wearable cognitive support on Google Glass supported by Cloudlet

3. Applications of Fog Computing

As per Nielsen and Mollich, this section is elaborating different usability evaluation methods below which were discovered through evaluation to assessment the mapping for systems.

3.1 Smart Home

Internet has evolved so many things and with the fastest development smart devices and sensors are connected to home. It has been seen that products of different suppliers hardly work together. Few tasks need huge amount of computation and storage capacity just like real time video analytics but that is infeasible because of limited competency of hardware. Fog computing is used to mix everything in one program and to inspire intelligent house software with variable reference components. If house protection software is taken for example it'll include protected receptors of intelligent locks, video/audio reorder, sensors. If goods are of various same vendors, then it's difficult to integrate. Haze research give house protection software at bigger scale.

- Good Program is for adding all separate units
- Variable assets generally help computation and storage
- Real-time running & low-latency result

As soon as haze software is established with every safe and sound warning can be linked with consumer sensor. Remote computer use might be hooked up to separate VMs. Superior handling judgement might be put in place upon VMs which method information contributed by simply usually safe and sound keep an eye on applications. For example, motions warning discovers any improbable motions in an income area next cleanup robotic with digicam provides the sequence connected with looking at actual location. Real-time online video analytics will probably estimate all those videos and make sure possibly it is just a fake alarm or not. Notification and evaluation report will be sent to the home owner and system will call police.

3.2 Smart Grid

Smart Grids are usually an electrical power submitting system having good feet's which is integrated at a number of area for calculating the particular real-time rank

information. Central remote computer which is known as SCADA procedure constantly accumulates in addition to examines the particular rank data to get mailing requires to grant an answer to get backing the energy grid. Haze computing can grant help to good lines greatly. Using errors computing, SCADA can grant your supplement to get decentralized type to get micro-grids which could not simply develop scalability, cost-efficiency, protection in addition to rapidly answer associated with electricity procedure but additionally incorporate the particular handed out electricity generation devices having the leading electricity grid. Haze computing good lines converts ordered procedure having discussion amongst fogs in addition to superior tiers. The top the particular rate, the particular bigger regional protection in addition to much larger the particular latency. Ultimate Worldwide Protection is actually offered by SCADA which in turn is liable for long-time repository in addition to monetary analytics.

3.3 Smart Vehicle

Fog computing is combined into vehicular based networks. It will depend on extra infrastructure which needed, vehicular fog is computing is categorized into further two sorts that's infrastructure-based and autonomous. YouTube relies upon fog nodes positioned along roadside fog nodes account of send/retrieve information to/from driving by vehicles. That makes use of automobile on-the-fly so that you can coming from errors and/or impair so that you can approve ad-hoc event. Just about every error can easily make contact with consumer of these fig premises. Regardless of the program with regard to road errors computing mainly because of several types. Well known program provided site visitors lighting organizing, traffic jam mitigation, preventative measure spreading, vehicle ability managing, site visitor's facts using spreading etc.

3.4 Health Data Manager

Health data management is a sensitive issue because it contains precious and private information. The main goal is to take the control of data health locally. Health data is memorized in fog computer including smartphone and smart vehicle. Whole process is outsourced for storage purpose because of patient want help from medical health. Data modification always occurs directly in patient-owned fog node.

4. Fog Privacy and Security Issues

We all agree to this fact on security and privacy must be addressed in each defined layer especially from designing fog computing system. Here we need to ask a question from us "What's new for fog computing about security & privacy? Fog computing

characteristics make that potent to tackle all the future problems.

4.1 Trust and authentication

In cloud processing arrangement, information stores are approved by cloud support providers. Haze support companies may have various events due to specific arrangement choices

- Online sites company who've get a handle on of house gateways and mobile programs that could construct haze with the present infrastructure.
- Cloud support companies need growth of these cloud companies for a benefit to network. It could construct the infrastructures.
- Customers possess regional individual cloud that are looking to mitigate the expenses of possession that are looking to show the individual cloud in to haze and different sacrifice methods around the neighborhood individual cloud.

1) Trust Model: Trust models based on e-commerce and peer to peer, social networks have been victorious as always. As per the strong repute system in resource selection of P2P networks by utilizing the distributed polling algorithm to determine the reliability of resource before downloading. Fog computing reputation system designing may be a time-consuming approach but need to solve the issues just like

Get to know about achievement of persistent, unique and distinct identity

- How to deal intentional & accidental misbehavior
- How to conduct punishment and redemption of reputation

Many relying types generally predicated on specific equipment as Protected Factor and Respected Delivery Atmosphere or Respected Software Component that will supply the electricity confidence for handling research

2) Rouge Fog Node: A rogue fog node always pretends to be legitimates the end users to connect. For instances, we instantiate a rogue fog instead of genuine one. All work has been demonstrated with the possibility of in-the middle attack for further fog computing either the gateway should be compromise or substitute with the pirated one. Once the fog node is connected then adverse things can be processed with outgoing and incoming request from all ends.

It is usually simply initiated the further attacks.

Currently fake fog node is a huge warning to user data security and privacy. These complaints are hard to find out in fog computing as a result of several reasons that may be:

- Complex Trust position demands numerous trust management schemes
- Dynamic creation, deletion of VM instance to really make it complex to conserve a blacklist of rogue nodes

It is usually simply initiated the further attacks.

Currently fake fog node is a huge warning to user data security and privacy. These complaints are hard to find out in fog computing as a result of several reasons that may be:

- Complex Trust position demands numerous trust management schemes
- Dynamic creation, deletion of VM instance to really make it complex to conserve a blacklist of rogue nodes
- Authentication: This is an important problem for the security of fog computing when services are offered to massive scale audience by using front fog node. It has been considered the main security issue of fog computing just like the authentication at numerous level. Traditional based authenticity is not that much efficient and scalability level is zero.

It has proposed a cheap and user-friendly solution to authenticity issue which is in local ad-hoc wireless system that is dependent upon bodily contact for pre-authentication in just a confined area channel. NFC can be applied to gauge the authorization process. With the increase of biometric credibility within portable processing and cloud processing the same as fingerprint and experience credibility possibly feel centered or keystroke centered authentication. It's very therapeutic for using biometric-based credibility particularly in haze computing.

4.2 Network Security

As a result of frequency with WIFI throughout errors network, WIFI multilevel stability is actually significant worry to be able to errors networking. Performing assaults in addition to sniffer assaults include the greatest issues. Commonly, throughout multilevel, we will have to idea an options that happen to be yourself made by way of multilevel supervisor in addition to segregate multilevel control site visitors out of standard info traffic. Nonetheless, errors nodes are generally sorted out near World-wide-web, that will certainly lower a major problem on the multilevel control, picturing the velocity with sustaining enormous degree impair web servers that happen to be allocated on multilevel borders devoid of basic entry to get maintenance. Just how do SDN aid a peace of mind in errors multilevel?

- Community Keeping track of in addition to Breach Detectors Process that will direction site visitors to get stability overseeing uses as well as IDS.
- Site visitor's prioritization in addition to solitude can often acquire deterrence an episode out of congesting a network.
- Community Source Obtain Management include consist of an entry handle structure over a SDN control centered across the Amenable circulation
- Community Expressing in case the multilevel expressing to be able to company is actually very carefully fashioned with stability problems.

4.3 Secure Data Storage

User results are deployed and user's authority over results are given up to fog node, that describes the protection threats same because it is in cloud computing. First, it is not easy to ensure data integrity, second, the uploaded data may be molested by unauthorized parties. for data protection, Auditable data storage utility continues to be profound for cloud computing for addressing these threats. Techniques like homomorphic encryption and searchable encryption are combined for integrity and confidentiality for cloud storage system to permit suer to examine its data saved on mistrustful servers. In fog computing, you will discover first-hand trials for designing secure storage system to realize low-latency, support dynamic operation and interaction between fog and cloud

4.4 Secure and Private Data Computation

To accomplished secure and privacy maintaining computation that is deployed to fog nodes. Let's have some discussion in following:

1) Verifiable Computing: Verifiable processing allows a processing system to clear of the find out of a purpose from untrusted machines, through the preservation of verifiable results. Another machines assess the big event and get back the end result with a appropriate computation. In haze processing, to give the computation offloaded to the haze node, the haze person should manage to examine the correctness of the computation. Listed here are some solutions to complete verifiable computing. The project may present insight and result solitude to the customer in a way that the machine does incapable of know any data about the insight and output. Par no and Gentry have constructed something that's named Pinocchio, by which customer may authenticate standard calculations that is performed with a machine while depending just on cryptographic suppositions. With Pinocchio, the customer creates a community evaluation crucial to determine her computation, and the machine then evaluates the computation and techniques the evaluation crucial is to make an evidence of accuracy.

2) Data Search: That is to protected knowledge solitude sensitized knowledge from customers that will need to be protected ahead of deploying to the haze node, It generates knowledge operation powerful is really a touch challenging. One of the very substantial companies is keyword search. It is completed in all the protected file. Experts have developed different searchable security practices that enable a person to easily research around protected knowledge applying keywords without decryption. They have proposed secrecy for encryption, query separating support of hidden query and controlled searching.

4.5 Privacy

The leak of personal information, including data, location or usage, this occurs when customers are applying services

like cloud computing, wireless network. There's also competitive situation for securing such privacy in fog computing. Privacy-preserving approaches are already planned in lots of scenarios contain cloud, smart grid, wireless network, and social online network.

1) Data Privacy: Privacy-preserving algorithms are in a row in between the fog along with fog up when people algorithms are often useful resource banned after devices. Errors node within the side generally collects very sensitive facts manufactured by alarms along with conclude devices. Differential comfort can be utilized to be certain non-disclosure associated with comfort of the randomly solo accessibility with your data collection in the event of math queries.

2) Usage Privacy: Yet another privacy make any difference will be the use style and design certainly where a fog customer utilizes the particular fog services. For example, throughout sensible power grip, the particular sensible mustimeter looking through will advise you a lot of details about children which no individual exists at your house, as well as moment where the particular TV is actually started up, which will totally smash customer's confidentiality. On the other hand, this particular remedy is going to go up the particular haze patient's imbursement as well as spend assets as well as energy. Something else could well be creating some sort of good way regarding splitting up the application form to ensure the particular offloaded origin uses will not show solitude data

4.6 Access Control

Accessibility get a grip on is just a real software to validate the protection of the machine and sustaining the solitude of user. In cloud centered research, the entry regulates generally cryptographically sent applications for used data. different community important centered answers are proposed attempting to attain entry get a grip on of fine-grained. In haze research, how to create entry get a grip on on both parties of client-fog-cloud, at the same time frame meet up with the planning objectives and reference limitations will soon be challenging.

4.7 Intrusion Detection

In fog computing, IDS may be arranged on haze node process part to spot unpleasant conduct by tracking and considering wood record, entry get a grip on guidelines and individual login information. They could also be implemented at the haze system part to identify horrible episodes such as for instance denial-of-service (DoS), slot checking, etc. Additionally, there are checks such as for instance utilizing intrusion recognition in geo-distributed, large-scale, high-mobility haze processing setting to generally meet the low-latency requirement.

5. Conclusion

We have briefly described the concept of fog computing and after evaluating similar concepts, a more comprehensive definition of fog computing is provided. A short note on the applications of fog computed is given here. This paper also provides discussion about various security and privacy matters in the perspective of fog computing, which a recent is research infrastructure to supply expanding assets at the side of system to regional conclusion users. That report describes safety problems such as for instance protected knowledge storage, protected computation and system security. Solitude problems in knowledge solitude, consumption solitude, and place solitude may also be outlined in that report, which might necessitate new want to acclimatize new problems and changes.

References

[1] Stojmenovic, Ivan, and Sheng Wen. "The fog computing paradigm: Scenarios and security issues." Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. IEEE, 2014.

[2] Yi, Shanhe, Zhengrui Qin, and Qun Li. "Security and privacy issues of fog computing: A survey." International conference on wireless algorithms, systems, and applications. Springer, Cham, 2015.

[3] . J. Zhu et al., “Improving web sites performance using edge servers in fog computing architecture,” in SOSE. IEEE, 2013.

[4] Otten wilder et al.[5], “Finding your way in the fog: Towards a comprehensive definition of fog computing,” ACMSIGCOMM CCR, 2014.

[5] Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: workshop on Mobile cloud computing. ACM (2012).

[6] Cloud Security Alliance, “Top Threat to Cloud Computing V1.0,” March 2010. M. Arrington, “In our inbox: Hundreds of confidential

[7] Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudlets authentication in NTC -based mobile computing. In: MobileCloud. IEEE (2014).

[8] Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: workshop on Mobile cloud computing. ACM (2012).

[9] Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudlets authentication in NTC -based mobile computing. In: MobileCloud. IEEE (2014).

[10] S Cao et al “A survey of fog computing: Concepts applications and issues,” in Proceedings of the 2015 Workshop on Mobile Big Data. ACM, 2015.

[11] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwalder, and B. Kold- ¨ ehofe, “Opportunistic spatio-temporal event processing for mobile situation awareness,” in Proceedings of the ACM international conference on Distributed event-based systems, 2013.

[12] Ha, et al. [13]. "Fog computing: Platform and applications." 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb). IEEE, 2015.

[13] Stojmenovic I, Wen S. The fog computing paradigm: Scenarios and security issues. InComputer Science and Information Systems (FedCSIS), 2014 Federated Conference on 2014 Sep 7. IEEE

[14] http://www.slideshare.net/saisharansai/fog-computing-46604121