TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

A Competent Model for Security and Privacy in IoT using Fog Computing

[1]N. Musrat Sultana , [2]K. Shirisha, [3]S. Vijaya Lakshmi
[1] Asst. Prof, CSE Dept-MGIT, [2] Asst. Prof, CSE Dept-MGIT, [3] Asst. Prof, CSE Dept-MGIT

Article Info
Volume 82
Page Number: 8264 - 8271
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 07 February 2020*

Abstract:
The Internet of things (IoT) characterizes the goal of everyday physical devices that are associated with the internet and having the option to recognize themselves to different devices. Today, Internet of Things is a place where changes occur as devices become more sophisticated, computation becomes smarter, and interaction becomes insightful. The standard integrated cloud computing model faces a number of challenges due to high demand for IoT applications, such as network instability, limited means, high delay and deprived security. Fog computing brings the cloud closer to IoT devices to address these challenges. Fog computing is a prototype that allows cloud computing to reach the edge of networks. Instead of sending them to the cloud, fog provides local data processing and storage on IoT devices. Unlike the cloud, the fog provides faster response and improved security services. This paper represents the fog computing technique and its compatibility with IoT by illustrating the advantages and challenges of implementation. We also concentrate on the fog and architecture and new IoT technologies that will be improved through the use of the fog template.

Keywords:*Fog Computing, Internet of Things, IoT Devices, Cloud Computing.*

I. INTRODUCTION

The market for creation of web applications is significant today. IoT is therefore a core technology that enables us to develop numerous useful web applications. Actually data is exchanged through routers and network devices with the help of physical objects that are connected to internet. With the help of existing network infrastructure IoT enables remote control of artifacts. IoT is an excellent and brilliant approach that lowers individual efforts along with smooth ingress of physical devices. In addition, any device is possible to be accessed without the absence of an individual with the help of this method.

Fog computing is a service started by networking giant, CISCO [1]. It would be very difficult to imagine fog computing without first defining cloud computing, because fog computing is essentially a cloud extension.

In order to work with Fog computing we should learn the process of running ICT tasks and services and storing computer resources over the Internet using Cloud Computing. This makes it possible for people and businesses to make use of third-party hardware and software located online. Cloud computing makes it really easy to access information and computer resources from anywhere as far as internet connection is available. With the wide-ranging availability of shared/pooled computing resources, cloud computing offers advantages over traditional on-site hosted services in terms of speed, security, privacy and efficiency.

Fog computing, at the same time, is the extension of cloud computing capabilities to the bottom/edge of the network in order to provide faster ICT (communication, storage, software, etc.) services to the lower end users. What separates fog computing

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

from cloud computing is therefore its familiarity with small end users, its broader consumer scope and greater flexibility.

Due to the advancement of computing, smart metering, smart home/city, connected vehicles and large-scale wireless sensor organize are making everything associated and more intelligent, named the Internet of Things (IoT). IDC (International Data Corporation) has anticipated that in the time of 2015, the IoT will keep on quickly extend the conventional IT industry up 14% from 2014 [2]. We realize that shrewd gadgets ordinarily face difficulties dependent on figuring force, battery and capacity which consequently impede the nature of administrations (QoS) and client experience. To mollify the trouble of restricted assets on savvy gadgets, haze processing is considered as a promising figuring worldview, which can convey administrations to end clients as far as framework, security, protection and supply applications with assets requiring little to no effort.Fog computing in the IoT was intended to enhance efficiency, reliability and mitigate in order to transfer data to the cloud for storage, filtering and storing. The data gathered by sensors is transmitted to network edge devices accordingly, for processing and temporary storage rather sent to the cloud, increasing network traffic and latency [3].

The convergence of fog computing and IoT creates a new market for many companies, known as Fog as a Service (FaaS), in which a service provider frames a group of fog nodes across its surroundings and acts as a landlord to many residents from many steep markets. Each fog node hosts local computation, networking and storage capabilities [4]. FaaS will allow the delivery of new products and services to clients. Apart from clouds, which are usually operated by large communities who can afford to build and operate huge data centers, FaaS will enable big and small communities to arrange and serve private or public computing, Services for processing and monitoring to address the needs of such a wide range of customers [10]. Let us focus on the properties of fog computing, the architecture of fog, and some for security and privacy issues related to data shared in the environment. We now focus on how fog computing provides low latency, storage and authenticity at each layer of fog architecture.

II. Fog Computing Overview

A. Definition

Fog computing is still not a common term across the world as a completely new computing method. In fact, fog computing is indeed an enhancement to the edge of the network of cloud computing, which is really a fully potential resource pool system that offers storage, software and data services to near-end users.

B. Characteristics of Fog Computing

With the help of fog computing the end users get benefitted by enjoying the services such as storage, processing and other networking solutions with end devices. A fog works as a medium across the cloud and the devices. These devices are known as nodes of fog. With a network connection, they can be deployed anywhere. Every device having processing, storage and access to the network can be a fog node, for example switches, home appliances, smartphones, routers, and video surveillance devices respectively [5, 6].

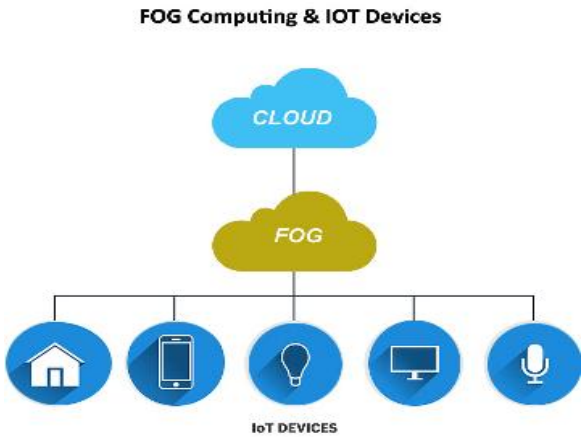

Fig. 1

The location-awareness is another interesting feature; not only does the geo-distributed fog node derive its own location, nevertheless the fog node will control end-user devices to enable versatility, that can be a pioneering factor to location-based

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

services but also applications. In addition, the transaction between fog and fog, cloud and fog is becoming essential as fog can certainly obtain a local impression whereas global broadcasting merely can be attained at the upper layer.

C. Fog Node

Increase in emergence of smart devices as well as the fast technological development and cloud technology is creating numerous applications of fog nodes possible. Fog nodes are classified under two groups, varying well into the location of edge devices, (a) Fog nodes as mini-clouds with "dumb" edge devices that serve as data makers / buyers. Usually, dumb nodes are high-end servers by means of dominant CPU, massive memory, and processing. (b) Fog nodes as mini-clouds loaded with IT capabilities with "smart" edge tools. Such nodes are suitable because of their operational abilities and their accessibility to the edge of the network [7]. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) can be classified under three groups. The following distribution models may also be needed, such as private fog, social fog, and public fog including hybrid fog.

III. Fog Computing Architecture

The administrations gave with the aid of Fog Computing engineering are performed as follows. Right off the bat, the records is shared into lumps. These pieces are allocated to contending hubs and they are arranged before transmission. Contingent on the line, the channels remain circulated that reasons rarely any pieces to enslave the inert channels in the number one stage and staying of them anticipate resulting free channels. The organized pieces are masterminded inner their finishing up time because the appropriated handling is completed. Further those lumps are returned to have making use of channel designation. Toward the cease, these pieces are accumulated on the host [8].

Server farm's assignments are added to the edge of the machine with the aid of Fog Computing. In a disseminated way the Fog offers restrained figuring, setting away and organizing administrations among cease devices and the normal dispensed computing server farms. Giving stable and low idleness to time-sensitive IoT applications is the number one objective of mist processing.

The Fog Computing Architecture is grouped into six training viz., bodily and virtualization, observing, pre-handling, impermanent stockpiling, safety and shipping layer as seemed in Fig 2 dependent on Mukherjee et al. [10], Aazam and Huh [9,5] and Muntjir et al. [11].

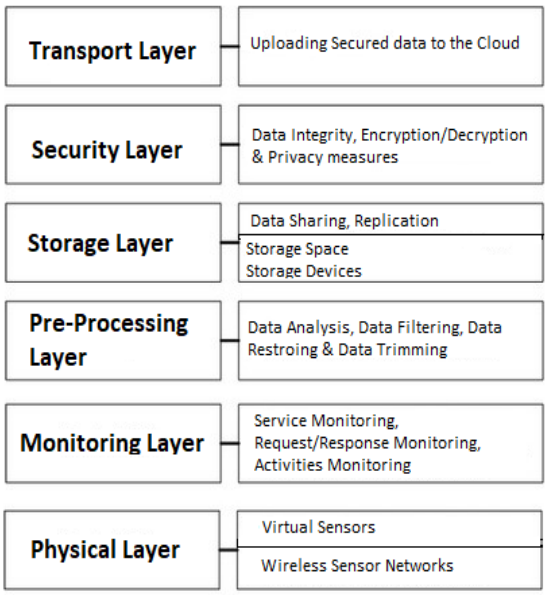

Fig 2.

The physical nodes, virtual sensor networks and virtual nodes are taken care by the physical layer. Based on the types and service needs these nodes are supervised and maintained. With the help of numerous groups of sensors the environs are covered and the data will be sent and received will be uploaded to the superior layers via gateways in relation to advance processing and filtering [12]. The availability of fog nodes, sensors and network elements are supervised at the monitoring layer. This layer supervises all tasks performed by nodes and are supervised; supervising which node is performing which job, when, and what will be done further. Hence the execution and level of work done from all the applications and services which are

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

setup on the infrastructure are supervised [10]. Moreover, the fog computing utilizes several devices with distinct standards of power usage, the energy conservation efforts should be monitored promptly and effectively [10, 9].

Data management functions are handled by the Pre-Processing layer. In order to retrieve meaningful information the gathered data is analyzed, trimmed and then filtered. The temporary storage layer stores the pre-processed data. At the end the cloud receives the filtered data and it need not to be stored locally, further the temporary storage media removes the locally stored data [9, 11].

The process of encryption and decryption is done at the security layer. In order to protect the data from tampering integrity efforts are implemented. The cloud extracts the pre-processed data and provides useful services from the uploaded data in the transport layer [9, 11]. Only a lot of received data is uploaded to the cloud for efficient power conservation. A method called smart gateway [13] is applied to the cloud in order to processes the data prior transmitting to the cloud. These smart gateways transfer the data to the cloud received from the sensor networks and various IoT devices. Further the received data is stored in the cloud and then used to establish provisions to the users [9]. Depending upon the implementation of fog a proper communication protocol must be adhered because of restricted resources in fog [14]. The communication protocol must be efficient, adaptable and light weighted. Only then a good communication can be maintained between the cloud and the IoT devices.

A. Fog Computing with IoT

In IoT implementations, the cloud computing architecture does not solve some problems. For example, it cannot uphold live IoT applications like gaming, video streaming, etc. Being a centralized model it lacks the location awareness of devices. Whereas fog computing overcomes these problems. The following table I shows the differences between the traditional cloud and fog computing.

Table – I

Objectives	Cloud Computing	Fog Computing
Security	Specific	Hard to define
Attacks	Less Probability	High Probability
Location awareness	No	Yes
Latency	High	Low
Deployment	Centralized	Distributed

Fog computing serves as a bridge between cloud Computing, IoT devices and storage services. Fog computing is a segment of the cloud computing model which carries the internet nearer to the edge of the network, according to Cisco [6]. Fog offers a huge feasible paradigm of computation, storage and networking resources among classical cloud servers and end devices [15].

Numerous IoT applications get benefited with the association of fog computing along with IoT. In order to reduce latency fog maintains real time connections between IoT devices particularly for temporary applications. Iot devices tend to enumerate in millions, so fog computing uses an important aspect to assist large scale sensor networks. Addressing IoT devices will be a big problem in the future days. Lists are some the benefits provided to IoT applications, as shown in Fig 3.

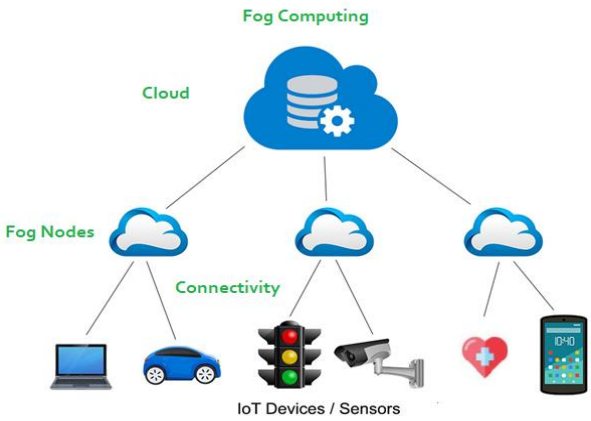

Fig 3.

Cloud computing architectures depend only on cloud and end-user devices which are connected with IoT devices. Cloud computing has many limitations which are effectively addressed by fog

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

computing.

IV. Security and Privacy Issues

In every layer of the fog computing system, security and privacy shall be aimed. The nature of fog itself is fragile compared to cloud computing, the fog nodes are to be secured using follow the same security controls, cybersecurity services and physical security mechanisms [6]. Because of fog's heterogeneity, mobility and its large scale geo distribution the existing privacy and security policies might not be applied precisely [16]. Cryptography and authentication have been used to enhance network security to guard over cyberattacks in fog computing, based on a research study [17].

A. Trust

Security itself doesn't mean in IoT environment, Trust is over and above to integrity, reliability and solidity in order to provide a service. The future behavior of each node can be predicted by implementing trust management in architecture of fog computing. It can be applied to resource-limited devices, fog clients and even to fog nodes. When it is possible to predict future behavior, fog clients will pick a proximity fog node that will deliver the greatest provision.

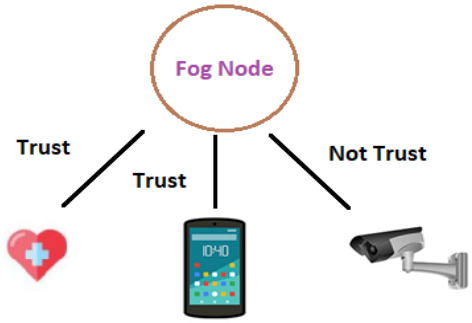

Fig 4.

In e-commerce, peer-to-peer (P2P), user reviews and online social networks, Reputation-based trust model [18] is so popular. Damiani et al. [18] established a robust reputation selection system in P2P networks using a decentralized polling algorithm to test a resource's quality prior to downloading. A few issues are to be addressed while designing a reputation based system for fog computing, for instance 1) in what way consistent, novel and lucid identity can be obtained, 2) How to cope with unintentional and intentional fault, 3) How to administer credibility retribution and reputation. Further in fog computing applications, unique trust based models are available namely Trusted Platform Module (TPM), Trusted Execution Environment (TEE) and Secure Element (SE) which offers trusted services.

A rogue fog node may typically be a fog device or fog occurrence pretending to be legitimate and enticing end users to connect to it. For instance, a fog administrator may be allowed to handle instances of fog in an intruder attack, but may reflect a case of rogue fog rather than a legitimate one.

Chain based on trust is implemented in IoT devices in order to address this issue. To achieve authentication fog computing, certificates are issued and chain of trust is also practiced. Based on the levels trust is managed, for example a low grade node is trusted when a trusted higher grade node says one of its lower grade nodes can be trusted. The chain of trust follows a decentralized method. The high grade nodes must have a brief account of its next level nodes, yet it's not possible to store all the trust values in a single system. Because, the high grade nodes are trusted it it's the responsibility of high grade node to understand the low grade node. Likewise the trust works in a chain manner.

B. Authentication

In fog computing, trust can offer some solution but authentication remains a big problem. In fog architecture, the major security issue is authentication. Trust can possibly guarantee the reliability of authentication. A cheater node can enter the network and acquire accessibility to the private information without any authentication.

Authentication is the major security point in fog computing at various extents in fog nodes Stojmenovic et al. [19]. Authentication depending on traditional Public Key Infrastructure (PKI) is not efficient and lacks scalability. Also, in the case of cloudlet [20], Near Field Communication (NFC) can

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

be used to simplify the authentication procedure. Various authentication techniques available now a days like face authentication, fingerprint authentication, key stroke-based and touch-based authentication etc., Applying biometric authentication in fog computing will be more beneficial.

C. Network Security

Security of the wireless network is a major concern for fog networking. Some of the networking attacks are sniffer attacks, jamming attacks, etc. We generally have to trust any configurations locally developed by a network administrator throughout the network and isolate network management traffic against the standard data traffic [21]. Furthermore, fog nodes are secured at the edge of the Internet, which certainly puts a heavy burden on network management, estimating the cost to maintain large-scale cloud servers which are spread across the edge of the network without efficient maintenance access.

Using Software Defined Networking (SDN) in many areas of fog computing can promote adoption and management, and improve network interoperability and reduce costs. Free flow to redirect traffic for security monitoring applications can be used for the security layer Network Control and Intrusion Detection System (IDS). The separation and prioritization of traffic can be used to stop attacks from accessing the network or dominant available resources including CPU or disk input / output. Fog optimized routers can be accessible to guests in the home network if the network sharing is precisely developed for security risks. For instance, guest WiFi authentication is transmitted to the cloud in open WiFi routers as a means to create guest identity, guest access is set independently, and accounting is implemented to entrust guest accountability.

D. Secure Data Storage

Strategies like homomorphic cryptography and retrieval cryptography indeed coupled to ensure cloud storage system integrity confidentiality and validity to allow a client to validate their stored data on untrusted servers. Third Party Auditor (TPA) is a privacy preserving public auditing method for cloud storage data suggested by Want el al. [22]. To protect form TPA this method uses random mask and homomorphic authentication method. To prevent redundancy of data storage, previous storage systems use erasure codes and network coding to manage data corruption detection and data repair, this mechanism provides lower storage costs, faster data recovery, and equivalent communication costs. The new challenges in Fog Computing are developing secure storage systems for low latency, enabling dynamic operation and coping with deployment between fog and cloud fog computing.

E. Privacy

While using cloud computing, IoT, wireless networks leakage for example location, usage of data are drawing interest from the users. Also there are issues in fog computing to protect such privacy, as fog nodes are close to end-users and can collect much more sensitive information than those of remote clouds even in the main network. In many contexts, including cloud, wireless network, smart grid as well as other online social networks, privacy protection strategies have also been suggested. A few of the core areas of privacy include information privacy, protection of use and privacy of location.

V. ISSUES IN FOG COMPUTING

Although the paradigm of fog computing provides several advantages for various IoT applications, it poses other difficulties which stands in the way of its effective implementation. Such obstacles involve latency, interoperability, security, complexity, respectively as shown in Fig 5.

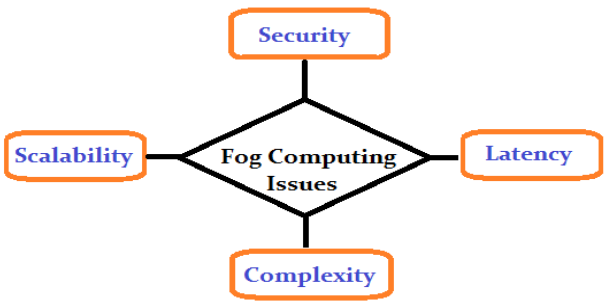

Fig 5.

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

A. Security

The fog model is susceptible and minimum secured in contrast with cloud computing. It is because the fog nodes are safeguarded with routine strategic controls and methods. With the help of cyber security solutions [6] and physical security fog nodes cannot be protected. Because of fog computing's large scale geo-distribution, heterogeneity and mobility the security and privacy metrics of current cloud computing cannot be applied directly. To achieve better network security over cyber-attacks in fog computing various studies concentrate on authentication, cryptography methods [17].

B. Latency

The major problem with cloud computing is its low latency specifically for time-sensitive utilizations. Although, there are several reasons offering a high latency of application or service performance on fog computing platforms. The users will be disappointed with the fog when it gives high latency [23].

C. Complexity

Selecting standard elements is getting difficult as lot of IoT devices and sensors are accessible from surroundings. Based on respective needs software and hardware selection is also becoming difficult. Sometimes, high-security applications need the proper functioning of specific hardware and protocols, which raises functional complexity [16].

D. Scalability

Large volume of data is produced by large number of Iot devices it requires lot of expedients like storage and processing etc. Therefore, Fog servers should assist these devices with sufficient expedients. A major challenge would be the ability to react to IoT devices as well as applications continued growth [16].

CONCLUSION

In our world, Fog Computing does have the ability to communicate with almost every device. In fact, IoT devices are quite efficient and have limited capabilities of storing data and processing. However, there are many problems with conventional centralized cloud, like high latency as well as network loss. To address these problems, fog computing is developed as a cloud extension, yet nearer to the IoT devices where all data processing is done at fog nodes, decreasing latency, especially for time-sensitive applications. Integration of fog computing with IoT can offer several advantages to various IoT applications. We addressed the art of fog computing in this paper, along with a review of fog characteristics and architecture. In the context of fog computing, security issues such as secure data storage including network security. We also explored some security and privacy issues. We also highlight various issues of privacy, such as data privacy, privacy of use and privacy of location which may require new thinking to address new challenges. Fog computing offers an intelligent framework in the future to handle the new IoT infrastructures distributed and in real time. Creating new networks at the edge by fog computing would offer network operators new business models and opportunities.

REFERENCES

1. https://www.cisco.com/c/en_in/index.html
2. Gil Press: Idc: Top 10 innovation forecasts for 2015. Http://goo.Gl/zFujnE
3. Wen, Z.; Yang, R.; Garraghan, P.; Lin, T.; Xu, J.; Rovatsos, M. Haze coordination for internet of factors administrations. IEEE Internet Comput. 2017, 21, 16–24. [CrossRef]
4. Yang, Y. FA2ST: Fog as a Service Technology. In Proceedings of the 2017 IEEE 41st IEEE Annual Computer Software and Applications Conference, Turin, Italy, four–eight July 2017; p. 708.
5. Verma, M.; Bhardwaj, N.; Yadav, A.K. Continuous Efficient Scheduling Algorithm for Load Balancing in Fog Computing Environment. Int. J. Inf. Technol. Comput. Sci. 2016, eight, 1–10. [CrossRef]
6. Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are.

January-February 2020
ISSN: 0193-4120 Page No. 8264 - 8271

White Paper. 2016. Accessible at the internet: http://www.Cisco.Com/c/dam/en_us/preparations /styles/iot/medical doctors/processing overview. Pdf (were given to on 8 April 2018).

7. Security and Privacy Issues of Fog Computing: A Survey. Shanhe Yi, Zhengrui Qin, and Qun Li. School of William and Mary. Syi, zhengrui, liqun@cs.Wm.Edu.
8. Yang liu , Jonathan e. Fieldsend, (component, IEEE), and Geyong min, (Member, IEEE) Department of Computer Science, University of Exeter, Exeter EX4 4QF, U.K. A Framework of Fog Computing: Architecture, Challenges, and Optimization Corresponding writer: Geyong Min (g.Min@exeter.Ac.United kingdom)
9. Aazam, M.; Huh, E.N. Haze processing and eager portal based totally correspondence for haze of factors. In Proceedings of the 2014 International Conference on Future Internet of Things Cloud, FiCloud 2014, Barcelona, Spain, 27–29 August 2014; pp. 464–470.
10. Mukherjee, M.; Shu, L.; Wang, D. Review of Fog Computing: Fundamental, Network Applications, and Research Challenges. IEEE Commun. Surv. Guide. 2018, PP. [CrossRef]
11. Muntjir, M.; Rahul, M.; Alhumyani, H.A. An Analysis of Internet of Things (IoT): Novel Architectures, Modern Applications, Security Aspects and Future Scope with Latest Case Studies. Int. J. Eng. Res. Technol. 2017, 6, 422–447
12. Liu, Y.; Fieldsend, J.E.; Min, G. A Framework of Fog Computing: Architecture, Challenges and Optimization. IEEE Access 2017, four, 1–10. [CrossRef]
13. Aazam, M.; Hung, P.P.; Huh, E. Keen Gateway Based Communication for Cloud of Things. In Proceedings of the 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Singapore, 21–24 April 2014; pp. 1–6.
14. Marques, B.; Machado, I.; Sena, A.; Castro, M.C. A Communication Protocol for Fog Computing Based on Network Coding Applied to Wireless Sensors. In Proceedings of the 2017 IEEE International Symposium on High Performance Computer Architecture, Vosendorf, Austria, 24–28 February 2017; pp. 109–114.
15. Agarwal, S.; Yadav, S.; Yadav, A.K. An Efficient Architecture and Algorithm for Resource Provisioning in Fog Computing. Int. J. Inf. Eng. Electron. Transport. 2016, 8, forty eight–61. [CrossRef]
16. Luan, T.H.; Gao, L.; Li, Z.; Xiang, Y.; Wei, G.; Sun, L. Haze Computing: Focusing on Mobile Users on the Edge. ArXiv 2015, arXiv:1502.01815.
17. Yi, S.; Hao, Z.; Qin, Z.; Li, Q. Haze registering: Platform and packages. In Proceedings of the 3rdWorkshop on Hot Topics in Web Systems and Technologies, HotWeb 2015, Washington, DC, USA, 24–25 October 2016; pp. Seventy three–seventy eight.
18. Damiani, E., et al.: A notoriety based methodology for selecting dependable property in shared systems. In: CCS. ACM (2002)
19. Stojmenovic, I., Wen, S.: The haze registering worldview: Scenarios and security problems. In: FedCSIS. IEEE (2014)
20. Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudlets verification in nfc-based totally versatile registering. In: MobileCloud. IEEE (2014)
21. Tsugawa, M., et al.: Cloud registering protection: What modifications with programming characterized organizing? In: Secure Cloud Computing. Springer (2014)
22. Wang, C., Wang, Q., Ren, K., Lou, W.: Privacy-saving open evaluating for records stockpiling security in allotted computing. In: INFOCOM. IEEE (2010)
23. Choi, N.; Kim, D.; Lee, S.; Yi, Y. Mist Operating System for User-Oriented IoT Services: Challenges and Research Directions. IEEE Commun. Mag. 2017, fifty five, 2–9. [CrossRef].
24. Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-safeguarding multi-watchword located seek over scrambled cloud facts. TPDS 25 (2014).
25. Rial, A., Danezis, G.: Privacy-safeguarding eager metering. In: Proceedings of the 10th every year ACM workshop on Privacy within the digital culture. ACM (2011).