Contemporary Applications of Fog Computing along with Security Problems and Solutions

Komuravelly Sudheer Kumar[1], K Ravi Chythanya[2], Bhavana Jamalpur [3], K Santhosh Kumar [4,] A Harshavardhan [5]
[1235]*Assistant Professor, Department of CSE, S R Engineering College, India*
[4]*Assistant Professor, Department of CSE, Jayamukhi Institute of Technological Sciences, India*

Abstract: Fog computing could be a new paradigm that extends the Cloud platform model by providing computing resources on the sides of a network. It is represented as a cloud-like platform having similar information, computation, storage and application services, however is basically completely different in this i.e., it's decentralized. Additionally, Fog systems are capable of processing massive amounts of knowledge regionally, operate on-premise, are absolutely transportable, and may be put in on heterogeneous hardware. These options build the Fog platform extremely appropriate for time and location-sensitive applications. For instance, Internet of Things (IoT) devices are needed to quickly process an oversized quantity of knowledge. This wide range of practicality driven applications intensifies several security problems relating to information, virtualization, segregation, network, malware and watching. This paper surveys existing literature on Fog computing applications to spot common security gaps. Similar technologies like Edge computing, Cloudlets and Micro-data centers have additionally been enclosed to supply a holistic review method. The bulk of Fog applications are actuated by the need for practicality and end-user needs, whereas the protection aspects are typically unnoticed or thought-about as associate degree afterthought. This paper additionally determines the impact of these security problems and potential solutions, providing future security-relevant directions to those chargeable for planning, developing, and maintaining Fog systems.

Keywords: Fog computing, Security threats, Internet of things, Performance, Wireless security, Malware protection

Introduction

Fog computing could be a localized computing design whereby knowledge is processed and keep between the supply of origin and a cloud infrastructure. This ends up in the minimization of knowledge transmission overheads, and after, improves the performance of computing in Cloud platforms by reducing the necessity to method and store massive volumes of superfluous knowledge. The Fog computing paradigm is for the most part motivated by an eternal increase in internet of Things (IoT) devices, wherever an ever increasing amount of knowledge (with reference to volume, variety, and velocity [1]) is generated from an ever-expanding array of devices.

IoT devices offer rich practicality, like connectivity, and the development of latest practicality is usually data intended. These devices would like computing resources to process the non inheritable data; but, quick call processes are also needed to keep up a high-level of practicality. This can gift measurability and irresponsibleness problems when utilizing a regular client-server design, where data is perceived by the consumer and processed by the server. If a server was to become over laden in exceedingly ancient client server architecture, then several devices might be rendered unusable. The Fog paradigm aims to supply a ascendable decentralized resolution for this issue. This is often achieved by creating a brand new hierarchically distributed and native platform between the Cloud system and end-user devices [2], as shown in Fig. 1. This platform is capable of filtering, aggregating, processing, analyzing and transmittal data, and can lead to saving time and communication resources. This new paradigm is called Fog computing, initially and formally introduced by Cisco [3].

Cloud computing provides several advantages to people and organizations through providing extremely accessible and efficient computing resources with a reasonable value [4].Many cloud services are accessible in current industrial solutions, however they're not appropriate for latency, movability and location-sensitive applications, like IoT, Wearable computing, smart Grids, Connected Vehicles [5] and Software-Defined-Networks [6]. Latency depends on the speed of internet connection, resource competition among guest virtual machines (VM) and has been shown to increase with distance [7]. Moreover, such applications generate massive volumes of information in an exceedingly high rate, and by the time information reaches a cloud system for analysis, the chance to inform the IoT device to require reactive action may be gone. For instance, think about IoT devices within the medical domain wherever the latency of performing on the perceived data may be life-critical.

Cisco pioneered the delivery of the Fog computing model that extends and brings the Cloud platform closer to end-user's device to resolve same issues. In line with [8], a Fog system has the subsequent characteristics:

- It’ll be placed at the sting of network with wealthy and heterogeneous end-user support;
- Provides support to a broad vary of commercial applications because of instant response capability;
- It’s its own computing, storage, and networking services;
- It’ll operate domestically (single hop from device to Fog node);
- It’s extremely a virtualized platform; and
- Offers cheap, versatile and transportable preparation in terms of each hardware and code.

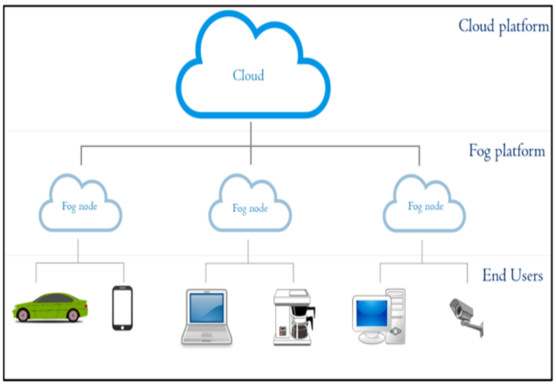

Fig. 1 Fog computing by Cisco.
This figure shows how diverse set of devices can communicate with the Cloud using Fog computing

Besides having these characteristics, a Fog system is completely different from Cloud computing in varied aspects and poses its own blessings and downsides. a number of the a lot of prominent are elaborated within the below list [9–11]:
A Fog system can have comparatively tiny computing resources (memory, process and storage) once compared to a Cloud system, however the resources will be exaggerated on-demand;

- They're ready to method information generated from a diverse set of devices;
- They will be each dense and sparsely distributed based on geographical location;
- They support Machine-to-Machine communication and wireless connectivity;
- It’s doable for a Fog system to be put in on low specification devices like switches and science cameras; and
- One amongst their main uses is presently for mobile and portable devices.

LikeCloud systems, a Fog system consists of Infrastructure,Platform, and Software-as-a-Service (IaaS, PaaS,and SaaS, respectively), at the side of the addition of information services [12, 13]. The technical design of a Fog platform [14] is shown in Fig. 2.

The Fog IaaS platform is created exploitation Cisco IOx API, which incorporates a UNIX and CISCO IOS networking software package. Any device, like switches, routers, servers and even cameras will become a Fog node that has computing, storage, and network property. Fog nodes collaborate among themselves with either a Peer-to-Peer network, Master-Slave design or by forming a Cluster. The Cisco IOx arthropod genus change Fog applications to speak with IoT devices and Cloud systems by any user-defined protocol. For developing Fog applications in PaaS atmosphere, Cisco DSX is employed to form a bridge between SaaS (which truly offers Metal-as-a-Service) and plenty of types of IoT devices. It provides simplified management of applications automates policy social control and supports multiple development environments and programming languages. The info service decides the appropriate place (Cloud or Fog) for information analysis identifies that information needs action and will increase security by creating information anonymous.

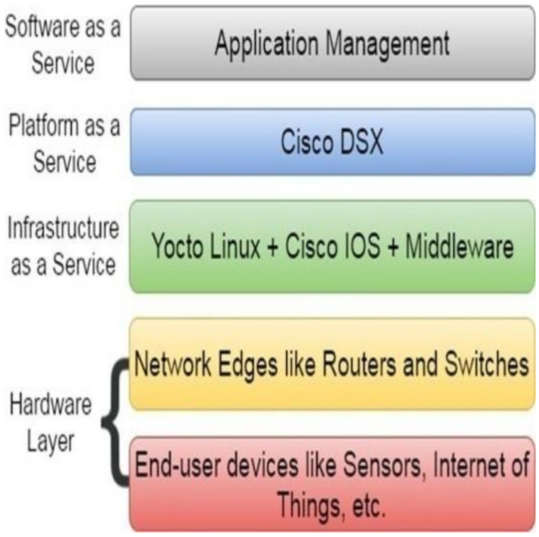
Software as a Service
Application Management
Platform as a Service
Cisco DSX
Infrastructure as a Service
Yocto Linux + Cisco IOS + Middleware
Hardware Layer
Network Edges like Routers and Switches
End-user devices like Sensors, Internet of Things, etc.

Fig. 2 Technical architecture of Cisco's Fog Computing Platform.
This figure shows all components from hardware to application layer

Many researchers and industrial infrastructure developers believe that Fog platforms are going to be developed and released within the future to produce associate degree enriched and a lot of reliable infrastructure to handle the ever increasing expansion of connected process devices. However, as with all distributed systems, the exposure to cyber threats is additionally current and sometimes heightened by the developer's want to produce practical systems initial, and then add-in security measures later on. Many researchers square measure adopting a security-centric or secure by design [15] philosophy for manufacturing such distributed systems. But this viewpoint continues to be in its infancy and lacks in comprehensive understanding of the safety threats and challenges facing a Fog infrastructure. This paper provides a systematic review of Fog platform applications, determines their doable security gaps, analyses existing security solutions so place forwards an inventory of comprehensive security solutions that may eliminate several potential security flaws of Fog systems. The literature used in this paper is gathered exploitation the Google Scholar search engine. The keywords wont to realize the literature square measure "Fog computing", "Fog computing applications", "Fog computing security", "Fog security issues" and "Fog security". The time frame of chosen papers is up to June, 2017. To best of our data, we tend to reviewed all papers that were displayed in the computer program at that point. Additionally to that, we tend to broadened the survey by together with many relevant research areas as Fog computing continues to be in its infancy stage. Alternative search terms were conjointly wont to search closely related developments subject areas. These embrace "edge computing", "cloudlet", "micro information centre" and "Internet of Things".

The paper is structured as follows: in the following section, a comprehensive review of literature is performed to identify established implementations of Fog and its similar systems. It conjointly discusses the potential security threats that haven't been acknowledged. Following this, an outline is provided to classify common shortcomings and to spotlight their significance. We have a tendency to additionally offer a discussion of potential mitigation mechanisms. Finally, we conclude by providing a discussion of the known shortcomings, motivating future analysis.

Related work - current fog applications

Review methodology

The Cisco Fog paradigm is viewed in a very broad and integrative manner as an enabler of the many advanced technologies. It will include, proliferate and impact many enhanced options like speedy analysis, ability among devices, enhanced time interval, centralized or machine-to-machine management, low bandwidth consumption, economical power consumption, device abstraction and lots of others. Similar approaches like Fog computing have currently been taken to extend the usability and potential of Cloud platform [16]. With the appearance of such wide relevance, the Fog and its similar platforms like Edge computing, Cloudlets and Micro-data centers are at risk of attacks which will compromise Confidentiality, Integrity, and accessibility (CIA) [17].Cloud Security Alliance [18] have known twelve vital security problems[154], as well as different researchers like [6, 19, 20]. These problems directly impact distributed, shared and on-demand nature of cloud computing. Being a virtualized environment like Cloud, Fog platform may also be affected by an equivalent threat (see Fig. 3). Our study considers following twelve security categories to formulate a systematic review:

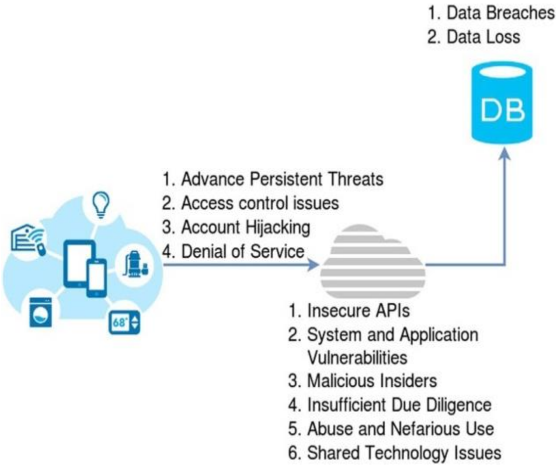
1. Data Breaches
2. Data Loss
DB
1. Advance Persistent Threats
2. Access control issues
3. Account Hijacking
4. Denial of Service
1. Insecure APIs
2. System and Application Vulnerabilities
3. Malicious Insiders
4. Insufficient Due Diligence
5. Abuse and Nefarious Use
6. Shared Technology Issues

Fig. 3 Potential security issues of Fog Platform inherited from Cloud Computing.
This figure shows how virtualization and other issues of Cloud platform can affect Fog platform as well

1. **Advance Persistent Threats (APT)** are cyber assaults wherein the purpose is to compromise a employer's infrastructure with the preference to thieve statistics and intellectual property.
2. **Access Control Issues (ACI)** can result in bad control and any unauthorized person being capable of gather information and permissions to put in software and change configurations.
3. **Account Hijacking (AH)** is wherein an attack aims to hijack the person accounts for malicious purpose. Phishing is a ability approach for account hijacking.
4. **Denial Of Service (Dos)** are where valid users are averted from the usage of a gadget (records and programs) by using overwhelming a machine's finite sources.
5. **Data Breaches (DB)** are while sensitive, covered or confidential information is released or stolen by an attacker.
6. **Data Loss (DL)** is wherein facts is by accident (or maliciously) deleted from the device. This doesn't should be resulting from a cyber assault and can stand up through herbal disaster.
7. **Insecure APIs (IA)** Many Cloud/Fog providers reveal application Programming Interfaces (APIs) for client use. The security of those APIs is pivotal to the safety of any applied applications.
8. **System and Application Vulnerabilities (SAV)** are exploitable bugs springing up from software ad configuration mistakes that an attacker can use to infiltrate and compromise a device.
9. **Malicious Insider (MI)** is a user who has permitted get entry to the network and system, however has deliberately decided to act maliciously.
10. **Inadequate Due Diligence (IDD)** frequently arises when a business enterprise rushed the adoption, layout, and implementation of any system.
11. **Abuse and Nefarious Use (ANU)** frequently arises when resources are made to be had free of charge and malicious users utilize stated resources to adopt malicious activity.
12. **Shared Technology Issues (STI)** arise because of sharing infrastructures, systems or applications. As an instance, underlying hardware additives won't have been designed to offer sturdy isolation homes.

The following section critiques an extensive-variety of Fog applications, paying unique interest to their potential security implications. Because the Fog computing remains in its infancy stage, comparable technologies have additionally been mentioned to make the survey extra holistic and beneficial. The Fog systems reviewed by way of analyzing publicly available literature have been grouped into the beneath subsections. At some point of this section, the 12 categories illustrated in Fig 3 are taken into consideration and a condensed summary is furnished in Table 2.

Fog Computing and Similar Technologies

Even though the term Fog computing built-in first coined by Cisco, comparable ideas have been researched and developed by numerous other parties.
The following list details three such technologies including some of their key differences with Fog systems. A more detailed comparison is available at [21] and [22] for edge computing.

1. **Edge Computing** performs localized processing on the device the usage of Programmable Automation Controllers (PAC) [23], which may handle information processing, garage and communication [22]. It poses a gain over Fog computing because it reduces the factors of failure and makes every device greater unbiased. But,

the same feature makes it tough to control and accumulate statistics in big scale networks which include IoT [24].

2. **Cloudlet** is a center part of three-tier hierarchy “mobile device - cloudlet - cloud”. There are four major attributes of Cloudlet: completely self-managing, possesses sufficient compute energy, low end-to-end latency and builds on general Cloud generation [25]. Cloudlet differs from Fog computing as software virtualization is not suitable for the environment, consumes greater sources and can't work in offline mode as indicated by [26, 27].
3. **Micro -data centre** [28] is a small and fully practical built-in integrated centre containing more than one server and is capable of provisioning many virtual machines. Many technologies, consisting Fog computing, can benefit from Micro data centers as it reduces latency, complements reliability, built-in protection protocols, saves bandwidth built-in by means of compression and may accommodate many new services.

Software Defined and Virtualized Radio Access Networks

Fog computing can enable customers to take complete manipulate and management of the network with the aid of providing Network Level Virtualization (NLV) and real-time information services. OpenPipe [29] utilizes Fog computing to implement NLV via a hybrid version, which consists of Virtual Software Defined Network (SDN) controller (placed in Cloud), [152]

Virtual local controllers (placed in Fog), virtual radio sources (for wi-fi conversation) and virtual cloud server. The SDN controller is a international and sensible module, which manages the whole community. Neighborhood controllers ahead data to an SDN controller, which fulfils the call for of actual-time and latency-touchy packages with the aid of finding out whether or not to method facts on neighborhood or SDN controller, based on person guidelines. The prolonged Open- flow (exOF) protocol is used to attach SDN and neighborhood controllers. The benefits of proposed device consist of load balancing, handover occasion without compromising Quality of service (QoS), low power intake, and reduced latency and coffee network overhead. in addition, Fog nodes can compress and reorganize the net objects for surest pace. In addition, various compelling research [30–32] had been supplied for improving the overall performance of SDN and virtual machines by using utilizing cloudlets, which are able to perform dynamic VM synthesis, single-hop low-latency wi-fi access and creates the VM overlays to simplest load the distinction of favored custom VM and its base VM. These capabilities were carried out with the aid of CarnegieMellon College in a undertaking referred to as Elijah and is available on Github repository [33].

Using surprisingly virtualized environment effects in a large variety of shared generation safety issues. For example, an insecure hypervisor can be exploited to convey down the whole Fog platform as it's miles a unmarried factor of failure and manages all of the digital Machines [34]. The virtualization problems include vulnerable tenant segregation permitting one malicious user or attacker to compromise different users’ account and statistics, facet-channel assaults [35], focused APTs and illegal privilege escalation to gain unauthorized records or resource get admission to. The dangers related to share generation are important as it takes a minor vulnerability or misconfiguration to harm all Fog offerings, consumer operations and allows attackers to benefit access to exploit Fog resources. Some of the encouraged solutions to cast off virtualization-primarily based assaults are multi element or mutual authentication, Host and community Intrusion Detection system, consumer-based totally permissions version, private networks and manner/facts isolation [36].

Web Optimization

Researchers from Cisco are using Fog computing to increase the overall performance of websites [37]. instead of creating a round ride for each HTTP request for content, style sheets, redirections, scripts and images, Fog nodes can assist in fetching, combining and executing them at once. Further, fog nodes can distinguish customers based on MAC addresses or cookies, track consumer requests, cache files, decide nearby network situation. It is also feasible to embed feedback scripts inner web page to degree the person browser’s rendering speed. The feedback script reports directly to the Fog nodes and informs approximately the user’s graphical resolution, modern area reception (if wireless) and network congestion. In any other similar paper, Fog computing appreciably reduced the response time of a Cloud-based temperature prediction device [38]. Due to Fog structures, the prediction latency changed into decreased from 5 to at least one. Five s, web-page display latency from 8 to 3 s and internet site visitors throughput from 75 to 10 Kbps. another related use of Fog computing is discussed in [39], in which the internet of everything (IoE),IP addresses may be changed with names, the usage of information Centric Networking (ICN) framework by more suitable cache mechanisms. Fog nodes are capable of manipulate cache (e.g. the use of Steiner Tree based highest quality aid Caching Scheme for Fog computing [40]), with the delivered gain of helping heterogeneous devices and computing, processing and storing on the edges of the network. any other simple approach [41] would be to apply part computing for generating consumer-unique pages by using replicating the software code at a couple of edge servers. The edge servers are capable of retaining numerous copies of statistics, perform content-conscious statistics caching and content material-blind information caching.

Using Fog platform for optimizing web-services will also introduce web safety problems. as an example, if person input isn't always properly confirmed, the utility will become susceptible to the code injection assaults, together with SQL injection, in which SQL code provided by way of the consumer is automatically carried out resulting within the ability for unauthorized information get entry to and modification. This can result in the compromise of complete Fog gadget's database or the forwarding of changed facts to a central server [42]. Similarly, because of insecure internet APIs, assaults like consultation and cookie hijacking (posing as a legitimate consumer), insecure direct item references for unlawful records access, malicious redirections and force-by means of attacks [43] should pressure a Fog platform to show it and the connected users. Internet's assaults can additionally be used for concentrated on different packages within the same Fog platform by way of embedding malicious scripts (go-web page scripting) and doubtlessly harm touchy facts. A capability mitigation mechanism is to cozy the software code, patch vulnerabilities, behavior periodic auditing, harden the firewall by defining ingress and egress traffic policies and upload anti-malware safety.

Provisioning 5G Cellular Networks

Mobile applications have turn out to be an integral a part of modern life and their extensive use has caused an exponential increase inside the consumption of cellular information, and consequently the requirement for 5G cellular networks. Fog computing can now not only provide a 5G community with better carrier quality, but they also can assist in predicting the future need of cellular customers [44]. Inherently, Fog nodes are disbursed within the proximity of customers; a characteristic that reduces latency and establishes adjoining localized connections. Broadly speaking, the diverse and multiple topological and mesh community connections amongst cellular community, Fog nodes, and Cloud platform make Fog system beneficial for 5G generation, NLV and SDN [45]. Fog computing is also able to handled load balancing problems of a 5G network [46].While many customers are simultaneously soliciting for computation in a large-scale community, developing small cells of Fog nodes primarily based on the scale of requested challenge and device parameters can enhance load balancing. This joint optimization of a couple of customers can enhance the high-quality of experience (QoE) and network performance by way of 90% of up to 4 users consistent with small cell. Aspect computing is likewise getting used for reducing community latency, making sure relatively efficient provider shipping and providing an progressed consumer experience with the aid of utilizing programmable nature of NLV and SDN [47].

Without well securing the virtualized infrastructure of Fog nodes in a 5G network, providers risks now not being able to acquire the desired performance. A single compromised Fog node in the 5G cell network can generate the capability access factor for a man-in-the- middle (MITM) assault and interrupt all connected users, leak records, abuse the carrier via exceeding the restrict of records plan and harm sibling Fog nodes. A MITMattack can be launched via a malicious internal consumer and can take advantage of the Fog platform through sniffing, hijacking, injecting and filtering statistics incoming from the end-person [48]. This can therefore affect the records conversation of the underlying network (E.g. the 5G network). The maximum commonplace manner of removing such troubles is to encrypt verbal exchange with symmetric and uneven algorithms, mutual authentication, the usage of the OAuth2 protocol, and ensuring the isolation of compromised nodes and certificates pinning as mentioned through [49].

Enhancing Throughput for Smart Meters

With the aid of deploying smart Grids, massive quantities of information is collected, processed and transmitted from smart meters the use of Data Aggregation Units (DAU). Meter Data Management System (MDMS) use the generated records to forecast future power needs. In line with [50], the information aggregation procedure takes a long time due to the low bandwidth potential of hardware, but can be improved with the assist of Fog computing. First, a Fog-based router is attached with smart meters that collect the information reading of all sub-meters inside a pre-defined time. Secondly, all values are transmitted to a second Fog platform, which plays information reduction techniques. This Fog-based approach was tested on a general purpose Cisco routers and IOx, which are capable of prominent among Fog and non-Fog network packets. This technique creates advanced Metering Infrastructure (AMI) which could reduce the quantity of conversation information and overheads inside the community, ensuing in a development in response time. A comparable structure is created in [51] for AMI, in which Fog computing helped in decreasing latency, delay jitter and distance while enhancing location consciousness and mobility help.

Despite the fact that sophisticated database software program and high garage potential hardware are used for aggregation and processing, information can without difficulty be replicated, shared, modified and deleted with the aid of any malicious intermediate or fake outside node the usage of a Sybil (forging identities) assault, which can undermine the CIA of statistics [52]. Similarly, it is hard for a Fog platform to centrally outline, set and maintain access manage attributes of consumer ownership in a big quantity of shifting data. Fog nodes are continuously processing, analyzing and amassing statistics to produce facts and it turns into hard to retain information integrity and prevent information loss. The tolerance at which a failure happens is likewise very low as the exact point of blunders is hard to pick out in a machine. To cast off these problems, safety policies and techniques must be included into Fog systems to tune energy intake facts along with contingency plans and catastrophe restoration modules [53, 54].

Improving Healthcare Systems and Their Overall Performance

Fog computing is likewise implemented in healthcare and elderly care systems, in which self-powered wireless sensors transmit records to Fog nodes, as a pose to sending them directly the Cloud. Using a massive range of sensors, it is feasible to create a smart healthcare infrastructure, in which semantic tagging and classification of information is performed within the Fog layer, offering the subtle information to a Cloud system for in addition processing [55]. Some other gadget makes use of a comparable method and integrates a Fog-computing-knowledgeable paradigm within a Cloud for scientific devices, imparting a good quality of service (QoS) and governance [56]. Each architecture is in the context of the OpSIT healthcare venture in Germany. With the help of Fog computing, healthcare structures offer services from nearby vicinity, keep heterogeneous facts, consists of smart low strength devices[151], and are capable of transfer amongst various communication protocols in addition to facilitating disbursed computing [57]. Some other utility of Fog computing in healthcare consists of Electrocardiogram (ECG) feature extraction to diagnose cardiac illnesses [58]. This entails medical sensors transmitting information to a Fog layer that stores information in distributed databases, extract ECG features, and supplying a graphical interface to display effects in real-time. The proposed device is rather portable and results indicate a 90% growth in bandwidth efficiency over contemporary solutions.

The detection of a person having a stroke is of key importance as the velocity of medical intervention is life critical. Two fall detection systems have been carried out using Fog platform, named U-FALL [59] and fast [60]. Each system distribute computational duties between Fog and Cloud platforms to offer a green and scalable answer, that's essential as it allows for a fast detection and notification of a patient fall.

Patient health information include sensitive statistics and there are a couple of factors in any Fog platform where they may be compromised, such as by exploiting any system and alertness vulnerability, unauthorized statistics get admission to at the same time as in garage or for the duration of transmission, malicious insiders threat and at the same time as sharing statistics with different structures [61]. Medical sensors are constantly transmitting information to Fog systems, via both wired and wireless connection. It is pretty possible to compromise affected person privacy, information integrity and system availability via exploiting sensors and their underlying communication network. Wireless sensors typically work in open, unattended and hostile environments. This ease-of-access has the capacity to increase the possibilities of assaults like DoS, record disruption, and selective forwarding assaults [62]. Further, if the Fog node manages sensitive information and lacks get admission to control mechanisms, it might leak the statistics because of account hijacking, unintended access, and different vulnerable points of access. To keep away from such problems, strict guidelines should be enforced to keep a high-level of manipulate the use of multifactor or mutual authentication, private networks and partial (selective) encryption.

Surveillance Video Stream Processing

Fog computing can play an important role, wherein the efficient processing and on the spot decision-making is required. Take an example of monitoring multiple targets in a drone video stream as stated in [63]. Rather than sending live video feeds to a Cloud-based utility, it is directed in the direction of the nearest Fog node. Any cellular device such as tablets, smart-phones and laptop can emerge as Fog node, run tracking algorithms and process raw video stream frames, subsequently casting off the latency of transmitting information from the surveillance location to the Cloud. Consequences show that the addition of a Fog platform reduced an average of 13% of overall processing time. The surveillance video processing can also be performed by using edge computing and its ability in finding missing children [64]. Pushing video feeds of each camera sensor immediately to the Cloud is not viable, however with the help of distributed edge servers and their processing strength, every video can be processed personally and the Cloud device can gather the final outcomes to yield a miles quicker output. Proximal algorithm [65] can also be implemented within the Fog nodes of a large-scale video streaming carrier, and might solve joint resource allocation problem.

A video information stream generated via a digital camera sensor is sent to the respective Fog nodes, where it is stored and processed. The privacy of the stream need to be maintained as it contains audio and visual records, which are transmitted to heterogeneous clients. Here, now not only is the safety of Fog node is important, but the community and all end-user devices worried in the transmission ought to additionally be taken into consideration, particularly in opposition to APTs. If a Fog platform or network contains any bugs due to lack of diligence, the critical video stream might be viewed, altered or even destroyed. It is essential that Fog node ensures a secure connection among all communicating gadgets and defend multi-media content through obfuscation strategies, fine grained access control, producing a new link for video stream, selective encryption and restricting the wide variety of connections [66].

Vehicular Networks and Road Safety

A new Vehicular Adhoc Networks (VANET) architecture has been proposed using Fog computing referred to as Fog-based software program defined network (FSDN) VANET [67]. The components of FSDN are SDN Controller (SDNC), SDN Wireless Nodes (vehicles), SDN road-facet-Unit (Fog tool), SDN road-side-Unit Controller (RSUC) and mobile Base Station (BS). SDNC controls complete network along with Fog Orchestration and aid control for the Fog. RSUC is a set of Fog devices that performs facts forwarding operations. BS also delivers Fog offerings and operates underneath the manipulate of SDNC. Fog nodes and different gadgets communicate in the form of policy guidelines and content. SDNC gets automobile information from BSs and transportation information from RSUs. Fog enabled BSs and RSUs making it viable to provide quicker offerings without contacting SDNC. Other comparable implementations have been proposed in [6, 68], where both Fog gadgets are connected centrally with SDNC and Cloud or interconnected with each different in a Machine to- system way. To increase road safety, a Fog-based intelligent decision support driving rule violation monitoring system [69] has also been advanced. The proposed machine has 3 layers: lower, center and upper. The lower layer is able to discover hand-held gadgets in the course of using and car variety the use of digital camera sensors, and send the records to nearest Fog server. In the center layer, Fog server confirms if motive force is deliberately violating the regulations and communicates the vehicle identifier information to Cloud server. Finally, in higher the layer, Cloud server issues a visitors violation decision and alert the applicable government.

The safety problems of Fog structures in vehicular and avenue networks are just like the ones associated with 5G cellular networks in phrases of troubles as a consequence of shared generation. Moreover, vehicular networks do no longer have fixed infrastructure, and due to the quantity of connections, there are a couple of routes among the same nodes. Such networks are exposed to ability DoS and information leak attacks because of a loss of centralized authority [70]. DoS assaults on a Fog platform, both from cease-customers or outside structures, can prevent valid service use because the community becomes saturated. Further, all conversation is wireless and subsequently prone to impersonation, message replay, and message distortion troubles [71]. Protection from those assaults is sizeable as human lifestyle is concerned. The most commonplace way of doing away with such issues is by way of implementing robust authentication, encrypted communication, key control carrier, perform regular auditing, and implement personal network and at ease routing.

Smart Food Traceability

Fog computing is also getting used as an answer for food traceability management, where the purpose is to eliminate terrible quality products from the supply chain using value-based processing [72]. A food object may be bodily traced using diverse attributes, including location, processing and transportation devices. The quality of a food item is determined through distributed food traceability via Cyber physical gadget (CPS), which makes choices based on Fuzzy guidelines. Both food traceability and fine information is sent to the Fog community, where the complete food supply chain is traceable. At this factor, the Fog network holds entire data about all tracked food objects and finally transmits food high-quality information to the Cloud machine which can be viewed with the aid of stakeholders using the internet.

The attackers may want to hinder supply chain operations through exploiting location and transportation approaches of this machine. If a Fog node is compromised by way of approach together with account hijacking or exploiting machine and application vulnerabilities, the statistics can be falsified, which could in the end result in the sale of substandard and low-quality food products. A network containing a huge number of wireless sensors, and machine-to-machine (M2M) communications instigates a large variety of safety concerns. One such example is resonance assault, in which sensors are pressured to function at one-of-a-kind frequencies and transmit incorrect information to a Fog node. This attack affects the real-time availability of community and facts, along with tolerance degree [73]. Such structures need to be protected by integrity checks, detecting deception attacks, redundancy to prevent single-factor of failure.

Collection and Pre-Processing Of Speech Data

A new Fog computing interface (fit) [74] is created for Android smart-watches connected with a smart tablet that collects, information and processes speech information from patients with Parkinson’s disorder. Rather than transmitting the whole audio records, fit extracts features like volume, short-time energy, zero-crossing rate and spectral centroid from speech and sends to the Cloud for lengthy-time period analysis. The application changed into examined on six sufferers and Fog computing made it viable to remotely system large amount of audio data in a discounted length. Another work extends the capabilities of mobile edge Computing (MEC) into a unique programming model and framework [75] allowing cellular utility developers to layout bendy and scalable aspect-based totally mobile applications. The developer can enjoy the presented work because the framework is capable of processing information before its transmission and considers geo-distribution facts for latency-touchy packages.

Smart phones and drugs host massive amount programs and might bring about many complexities in terms of excellent and safety. Each packages has to legitimate get entry to user's non-public information (frequently granted with the aid of the user at some stage in set up), which has been recognized because the using force in many cyber attacks [76]. Fog systems which are configured and executing on a cell operating system need to be blanketed, especially in case of open-supply structures, as one malicious utility can compromise Fog operations and the linked community along with consumer's non-public records [77]. Malware-based attacks can probably corrupt and damage the CIA of statistics and communication. A latest survey diagnosed that there are many capacity security answers, such as anti-virus, firewall, Intrusion Prevention gadget, consistent records backups, software patching, and often creating gadget repair points and performing behavior evaluation strategies thru dynamic monitoring [78].

Augmented Brain Computer Interaction

A real-time brain state detection system has been carried out using a multi-tier Fog computing infrastructure [79]. The Fog platform is the information hub and signal processor that gets and tactics information streams generated by electroencephalogram (EEG) headset and motion sensors. The Fog server extracts time-frequency traits from indicators and dispatches them to the brain nation classifiers. The advantages of the proposed device are validated through playing a multi-participant on-line sport known as EEG Tractor Beam. Some other comparable device is developed in [80], where a multi-tiered Fog and Cloud machine, linked facts, and category fashions have been used for EEG-primarily based brain-computer interfaces (BCI). The Fog servers are used for real-time records processing, caching, computation off-loading, coping with heterogeneity and forwarding statistics from cell gadgets and sensors to the Cloud device. Fog computing additionally has many potential programs in tele health structures [81], that can perform short mining and carry out evaluation on an uncooked statistics movement accumulated from specific wearable sensors. Fog nodes compress information and are bodily placed nearby, aiding to lessen bandwidth and electricity intake.

The CIA of each statistics stream should be ensured regardless of whether it is generated from a digital camera or EEG sensor. Basically, each Fog device have to don't forget suitable user access controls, facts encryption and transport layer security (TLS) protocol [82] to cozy statistics access, privateness, and transmission. If any sensor tool, Fog node, community or even all are compromised by way of attacker because of a few vulnerability or loss of diligence, the unique information will continue to be disclosed. Currently, mind alerts received with the aid of an EEG sensor are used to play games, which do not require excessive safety. But, for future touchy applications, it is vital to enforce encryption algorithms inclusive of Elliptic curve cryptography to protect against advance persistent Threats (APTs) and records loss threats.

Handling Resources in Micro Information-Centers

Aside from enabling superior technology, Fog computing can perform many system-stage tasks along with computation resource control, prediction, estimation and reservation. it can additionally perform statistics filtration based totally on policy, pre-processing and enhance security measures. A similar framework has been supplied via [83] for IoT devices [150] useful resource management in micro facts-centers. It consists of six layers:

- physical, digital 'things' and wireless sensors;
- interest, strength, reaction and provider monitoring;
- Pre-processing data by way of evaluation, filtering, reconstruction and trimming;
- Storing, distributing, replicating and de-duplicating facts;
- imparting security by means of encryption/decryption and integrity tests; and
- Transporting pre-processed information to the cloud.

The framework additionally carries a resource estimation and pricing model for brand spanking new IoT clients. Another article [84] shows that Fog computing can permit dynamic real-time analysis, included safety, reliability and fault tolerance. The Fog platform is incredibly bendy and scalable as processing nodes (mobile devices) can regularly be a part of and leave a network. This property additionally lets in the help for extra programming fashions and various device architectures to quick manage sizable facts.

Fog structures which might be used for the coping with computation assets of different structures are exceedingly inclined to shared era problems (discussed in “software program defined and virtualized radio get right of entry to networks” section). Some other essential danger is that of the malicious insider, who can violate get admission to control on user-to-consumer, consumer-to administrator, administrator-to-consumer and administrator to-administrator levels. As virtualized surroundings are loaded into reminiscence, it could also be exploited via aid abuse (privilege escalation and escaping attacks), account hijacking (exploiting authentication protocols or social engineering) and

DoS assaults because of big range of customers requesting resources use on the identical time. Such assaults may want to result from inefficient and inadequate aid policies as well as a lack of consumer activity tracking. On this case, identity-primarily based encryption algorithms [85] and role- primarily based get admission to manipulate version, as cautioned by way of NIST [86], can be carried out to growth safety.

Saving Energy in Cloud Computing

As Cloud operations require huge quantity of non-stop power, unique forms of applications are investigated in [87] the usage of Raspberry Pi based servers, which can be installed and configured as a Fog platform to lessen energy consumption. According to the results applications that continuously produce static facts inside end-user premises and have low connection rate (e.g. video surveillance), can save considerable energy using Fog computing. The authors also claim that the intake of energy normally depends on the amount of idle time, wide variety of downloads, updates and information pre-loading, whereas real content and number of network hops among users do no longer have critical impact. Another study [88] provides a systematic framework for developing a whole infrastructure such as a Cloud platform, wide area community (WAN), Fog structures and local area network (LAN) in a most beneficial manner. They also designed a numerical model to show that Fog computing substantially improves the overall performance of cloud computing by using buying and selling power consumption-put off with workload allocation. Similarly, to lessen the strength consumption in cell-telephones, researchers used name graph to dump computation to area servers through optimally managing and allocating communication resources [89].

This specific software encourages the usage of Fog structures in storing and processing particular (user-described) sorts of the (non-public) information domestically within the Fog nodes, reducing the verbal exchange cost and postpone. However, the presence of such personal statistics puts the Fog platform in a touchy position. As formerly stated there are many threats, which might be able to compromising CIA of information consisting of malicious insiders can examine, alter and delete data. These issues can be resolved through using encryption, authentication (uniquely validating and verifying every consumer), data classification primarily based on sensitivity, monitoring and data masking [90].

Disaster Response and Hostile Environments

Fog computing can aid human search and rescue operations carried out over massive geographical region in the occurrence of natural disaster [91]. Heterogeneous Commodity-Off-The-Shelf (COTS) Fog devices with low energy intake with wi-fi help are utilized in the implementation of the device. Specific quality of service (QoS) metrics which includes strength consumption, mobility, localization, most appropriate route calculation, statistics distribution amongst Fog gadgets and performance are measured in the simulated submit-catastrophe version to evaluate the machine. Similar paintings suggests that VM-primarily based Cloudlets [92] and tactical Cloudlets [93] can provide huge blessings in adversarial surroundings (e.g. army operations) as they're deployed in close proximity and can be placed inside cars for portability, ensuring non-stop carrier, carry out information filtering, reduces facts leakage and assist heterogeneous gadgets.

Disaster healing is a touchy region wherein Fog structures and related gadgets are speculated to paintings in extreme occasions. In this case, the integrity and availability of the system are greater vital than confidentiality. Wireless Safety protocols can perform checksum (stumble on facts errors), encrypt packets with minimal sources [94] and provision excellent-grained access manipulates to strictly validate users (terminating undesirable connections). Furthermore, in case of emergency and key control to save you dropping decryption keys, these mechanisms ought to be taken into consideration to retain availability and integrity without compromising the overall performance of machine.

Summary of Security Issues

Table 1 provides the connection of the surveyed Fog application regions and the kinds of security problems. A description of each category can be located in “review methodology” segment. Even though the table has been populated primarily based upon interpreting published literature, it must be mentioned that in some cases it's far possible that the authors may not have communicated specifics of their application which mitigate a potential security risk category. The table identifies that none of the surveyed utility areas have taken the necessary precautions to minimize the potential effect and threat of each category of protection threat.

Table 2 provides a summary of protection controls in appreciate to every application area. This table highlighting the potential effect on Fog structures with respect of CIA version. The development of safety features in Fog structures is hastily progressing, and some of the contemporary publications do no longer contain enough detail to provide an intensive assessment. This effect in number of the information gaps being speculative and futuristic and based at the state-of-the-art research activity. It is vital to note that due to continuous boom in attack vectors, it isn't an exhaustive listing and a few security problems may have been neglected. With the advancement in Fog infrastructure development, new security troubles will want to be identified and recounted.

Table 1 Knowledge gaps for application area based analyzing current Fog implementations against the twelve categories of security issues

Application Area	APT	ACI	AH	DoS	DB	DL	IA	SAV	MI	IDD	ANU	STI
Software Defined And Virtualized Radio Access Networks	✓	✓	✓	□	✓	□	□	✓	✓	□	✓	✓
Web Optimization	□	□	✓	□	□	✓	✓	□	□	□	□	□
Provisioning 5G Cellular Networks	□	□	□	□	✓	✓	□	□	✓	□	✓	✓
Enhancing throughput for Smart Meters	□	✓	□	□	□	✓	□	□	✓	□	□	□
Improving Healthcare Systems And Their Overall Performance	□	✓	✓	✓	✓	□	✓	✓	✓	□	□	□
Surveillance Video Stream Processing	✓	□	□	□	✓	□	□	□	□	✓	□	□
Vehicular Networks And Road Safety	□	□	□	✓	✓	□	□	□	□	□	□	✓
Smart Food Traceability	□	□	✓	□	□	✓	□	✓	□	□	□	□
Collection And Pre-Processing Of Speech Data	□	□	□	□	□	✓	□	□	✓	□	□	□
Augmented Brain Computer Interaction	✓	✓	□	□	✓	□	□	□	□	✓	□	□
Handling Resources In Micro Information-Centers	□	✓	✓	✓	□	□	□	□	✓	✓	✓	✓
Saving Energy In Cloud Computing	□	□	□	□	✓	✓	□	□	□	□	□	□
Disaster Response And Hostile Environments	□	✓	□	✓	□	□	□	□	□	✓	□	□

Existing Safety Solutions for Fog Computing

As discussed in the above sections, the advent of Fog platform functionality among end-users and the Cloud structures creates a brand new factor for vulnerabilities, which could potentially be exploited for malicious activities. In contrast to for Cloud structures, there are no general security certifications and measures defined for the Fog computing. In addition, it can also be said that a Fog platform:

- Has distinctly smaller computing resources due to their very nature and for this reason it would be tough to execute a full suite of security solutions which might be in a position to locate and prevent sophisticated, focused and distributed attacks;
- Is an appealing goal for cyber-criminals because of high volumes of information throughput and the chance of being capable of accumulate sensitive information from both Cloud and IoT gadgets; and
- Is more available in contrast with Cloud structures, relying at the network configuration and physical location, which will increase the possibility of an attack happening.

The real-world applications of Fog computing and similar technologies, which can be surveyed in “related work - current fog applications” section, are on the whole influenced via functionality. But, it has also been recognized that in maximum instances potential safety features in opposition to that can be implemented to mitigate threats are unnoticed. A potential reason for that is that the security troubles going through Fog structures is an infant research area, and only few of answers are to be had to locate and prevent malicious attacks on a Fog platform. The below section gives an outline of such systems.

Privateness Maintaining In Fog Computing

Research into maintaining privateness in sensor-fog networks [95] consists of the following summarized steps to secure sensor information among end-user device and Fog community:

- They collect sensor information and extract capabilities;
- Fuzzing of information by placing Gaussian noise in information at a certain degree of variance to lower the threat of eavesdropping and sniffing assaults;
- Segregation by splitting information into blocks and shuffling them to keep away from man-in-the-middle (MITM) attacks;
- enforcing Public Key Infrastructure for encrypting every information block; and
- Transmit segregated facts to Fog node, in which information packets are decrypted and re-ordered.

The device additionally consists of characteristic reduction ability for minimizing information communication with Fog nodes to assist minimizes threat. This work is of importance because it focused on keeping personal and crucial information during transmission. The proposed technique may be improved by choosing an encryption and key management algorithm, focusing on people who play an crucial role in retaining the privacy of records. Similarly, there's little discussion on the specified computational overheads for performing huge data manipulation (fuzzing, segregation, encryption, decryption and ordering, reordering) before and after the communication. This can be of importance when designing and producing a Fog device as the required computation overheads might now not be available. Any other crucial factor to notice here is that sensors transmit facts constantly, in all likelihood over longer durations of time, and the proposed privacy framework would possibly overload or even crash the underlying Fog machine.

Mitigating Insider Data Theft

One study [96] provides a solution for protecting information from malicious insiders the use of components of Fog and Cloud computing. It combines behavior profiling and decoy processes to mitigate protection threats. If any profile famous peculiar behavior, which includes the growth of getting access to unique files at unusual instances, the system will tag the get right of entry to as suspicious and block the respective person. Decoy is a disinformation assault that includes fake files, honeyfiles, honeypots and other kinds of baiting records that can be used to stumble on, confuse and capture the malicious insider. This studies area is vast because it demonstrates ability altering and mitigation strategies to shield towards information theft. Extra in particular, they reveal that the proposed method can successfully perceive ordinary behavior with a mean accuracy more than 90%. However, the experiment is executed with a restrained quantity of information. More particularly, eighteen students from a unmarried university over the period of 4 days. Subsequently, the consequences in terms of accuracy they declare may not reproducible or universal. Their method can be improved by means of growing the population size and going for walks the test over longer timespan [97]. Furthermore, the computational requirements of such an approach aren't noted. The paper presents no information on the amount of statistics that is stored, as well as the CPU time and memory required at some point of evaluation. Such behavior profiling techniques are regularly completed in a conventional patron-server structure in which computation resources are freely to be had. It isn't always clean how this approach is able to be executed on a Fog node without having destructive influences on middle capability. The technique can be further advanced through critically analyzing and choosing possible machines getting to know techniques and schooling facts required for behavior profiling. This contains greater significance because of the presence of a huge quantity of person and documents. Comparable behavior profiling and decoy strategies are used in different works [98, 99] to come across and prevent malicious insider threat. The behavior profiling, tracking and consumer matching manner might now not exert any burden on Cloud assets and save you actual information theft without exposing any sensitive data. As an introduced benefit, all of these operations will happen on-premise and execute relatively faster due to low bandwidth latency.

Policy-Driven Secure Management Of Sources

One piece of work introduces a preliminary policy control framework for the sources of Fog computing to enhance secure interaction, sharing and interoperability amongst consumer-requested resources [100]. The device is divided into 5 most important modules:

- Policy Decision Engine (PDE) for taking movement based on pre-described policy policies;
- Application Administrator (AA) to manage Fog multi-tenancy;
- Policy Resolver (PR) for attribute-based totally authentication;
- Policy Repository (PRep) keeping regulations and guidelines; and
- Policy Enforcer (PE) to hit upon any discrepancies in policy implementation.

AA is accountable for defining regulations and guidelines (stored in PRep) even as considering a couple of tenants, packages, facts sharing and communication offerings. When a sure carrier request is made from a consumer, it is sent to a PR that identifies the consumer based on specific set of attributes and get right of entry to privileges against a requested aid. The person attributes and their respective permissions are saved in a database. PDE takes consumer statistics from the PR, extracts rules from the PRep, analyze them and put into effect via the PE. The eXtensible access control Markup
Language (XACML) is used to create rules and the
OpenAZ framework for constructing PDE. Regardless of being in an preliminary segment, this coverage framework has capability to turn out to be an quintessential part of actual-time distributed structures
in future, wherein there may be a robust need for access, identity and resource management skills. but, this framework is restrained to only those systems, that are capable of allocate dedicated sources within Fog platforms for the majority of computations required by various modules to execute the framework. Fog systems need to be capable of handling incredibly time-touchy applications; however the proposed validation manner might take longer to make choices. Some other flaw of their technique is that the answer itself is inherently prone to DoS attacks because of the complex authentication process in PR and PDE. If an attacker establishes a huge quantity of connections, simultaneously, repeats the ’validation technique’ inside the equal connection continuously or responds to the authentication protocol in a low and slow manner [101], the Fog resources turns into exhausted and rendered unavailable for the meant customers. However, these safety worries can be decreased via constructing a overall performance version that is accumulating values of reminiscence, CPU and disk utilization and periodically evaluating with expected values [102]. In case the gadget identifies an anomaly, the user would be redirected to the Shark Tank cluster, which is essentially a proxy to carefully monitor the consumer however can grant complete application talents.

Authentication in Fog platform

Insecure authentication protocols among Fog systems and end-consumer gadgets were recognized as a major protection difficulty of Fog computing with the aid of [19]. The writer’s claim that the IoT devices, especially in smart grids, are at risk of information tampering and spoofing attacks and can be prevented with the help of a Public Key Infrastructure (PKI), Diffie-Hellman key exchange, Intrusion detection strategies and monitoring for changed enter values. Moreover, the authors show the excessive significance and effect of MITM assault on Fog computing by means of launching a Stealth assault on video name between 3G and the WLAN users within a Fog community. Consequences display that the attack did
not cause any visible alternate in memory and CPU intake of Fog node, hence it's far quite hard to come across and mitigate. The authors suggest that the threat of such assaults can be averted by means of securing communication channels among the Fog platform and the person via enforcing authentication schemes. Primarily based on the modern state of authentication in Fog platform, Fog structures are lacking rigorous authentication and secure communication protocols as in keeping with their specification and requirements. In a Fog platform both protection and performance factors are taken into consideration in conjunction, and mechanisms inclusive of the encryption methodologies called absolutely homomorphic [103] and Fan-Vercauteren truly homomorphic [104] may be used to relaxed the information. Those schemes consist of a hybrid of symmetric and public-key encryption algorithms, in addition to different editions of attribute-primarily based encryption. As homomorphic encryption allows normal operations without decrypting the facts, the discount in key distribution will maintain the privacy of information. Other studies offer a similar framework to at ease clever grids, regardless of Fog computing, referred to as the Efficient and Privacy Preserving Aggregation (EPPA) scheme [105]. The device plays information aggregation primarily based at the homomorphic Paillier cryptosystem. As the homomorphic ability of encryption makes it viable for nearby community gateways to carry out an operation on cipher-textual content without decryption, it reduces the authentication price (in terms of processing energy) at the same time as retaining the secrecy of facts.

Using Advance Encryption Standard (AES)

This paper [106] concludes that AES is an appropriate encryption algorithm for a Fog platform. A couple of metrics were taken into consideration for the performance evaluation: consumer load against CPU time and file length against encryption/decryption time and memory usage. according to the outcomes, encryption time turned into almost the same for each smart phone and laptop using small quantity of information, consisting of 500 Kb, 5 Mb, and 10 Mb.

although, AES encryption is universally popular [107] and is possible for Fog computing, because of low hardware specifications and smaller computations, the test does no longer compare AES with another to be had encryption algorithm. In addition, the size of the encryption key performs a crucial position in strengthening the encryption. Moreover, the experiment should also have as compared the performance and performance vector of different key sizes; 128, 192 or 256-bits. Their work lacks proof and justification as simplest three sample files are used in entire experiment. Using small sample size won't offer the deep perception to whether AES is a suitable algorithm for Fog networks and storage or not. Furthermore, best textual statistics is used for encryption/decryption procedures and it is uncertain if the equal results may be replicated with images or any other information format. Furthermore, the Fog platform consists of heterogeneous devices with distinct specifications and unmarried set of rules might not be capable of cover all viable scenarios. Encryption is already an extra challenge for the Fog platform and additionally consumes huge amounts of sources. The choice of encryption algorithm (whether symmetric, asymmetric or hybrid) ought to be accomplished in accordance with provider and infrastructure necessities.

Conclusion

It is obvious in the above sections that the recommended security solutions are personally not sufficient to defend the CIA of Fog platform. Consequently, the modern-day security state of Fog networks does not satisfy the modern day protection requirements. Broadly speaking, the literature in brief presents the answers to information integrity, insider threat, dealing with aid access policy, consumer authentication and encryption. But, there may be a urgent need to clear up important problems stemming from shared technology, lack of access control, user account management, service downtime, data loss/breach, insufficient vulnerability patching and poor device tracking. Any of those stated threats can permit attackers to threat the CIA of Fog network and related gadgets. One potential solution to these issues may be to reuse well-established and proven security protocols of other similar technologies. The Fog platform components and their operations are not completely new because they mimic Cloud (as stated in “creation” phase). The main challenge here is to link and modify the security features and practice them in accordance with the requirements of Fog platform. The prevailing security features have gone via rigorous testing, and the use of them has the ability to ensure that any Fog system satisfies vital industrial security standards.

Recommended Security Measures and Future Challenges

Inside the light of above literature review, this section gives the security knowledge gaps that should be covered to build a reliable, applicable and truthful Fog platform. Regardless of having huge ability and number of packages, there's a lack of security solutions to be had for Fog gadget developers and architects. But, as Cloud computing and many comparable technologies (albeit centralized systems) resemble the working mechanism of Fog computing, they can offer a deeper perception into the safety threats and solutions. Despite the fact that each Fog deployment has a distinctive set of safety necessities, applications and sensitivity, the subsequent subsections provide a comprehensive, efficient and applicable protection solutions, that are gathered and examined on diverse structures. They also can be used as popular great practice guidelines even as growing the Fog software program, in order that the security is enabled from within the platform. Table 2 presents a summary of the relationship between the following proposed security solutions and the twelve categories (“Review methodology” section) of security threats used throughout this paper.

Table 2 Security solutions that can resolve twelve potential security issues in Fog implementations

Security Solution	APT	ACI	AH	DoS	DB	DL	IA	SAV	MI	IDD	ANU	STI
Data Encryption					✓	✓			✓	✓		
Preventing Cache Attacks					✓		✓	✓				
Network Monitoring	✓	✓		✓	✓				✓	✓	✓	✓
Malware Protection			✓			✓	✓	✓				✓
Wireless Security	✓	✓			✓						✓	
Secured Vehicular Networks	✓	✓	✓	✓								✓
Secured Multi-Tenacy		✓	✓		✓		✓		✓		✓	✓
Backup and recovery						✓				✓		

Data Encryption

Advice 1: *The information needs to be secured earlier than (at rest in source location), in the course of (in movement via network) and after (at rest in destination location) communication among IoT devices, the Fog community and Cloud platform.*

Future Challenge 1*: added information security [153] measures normally cause extensive reduction in computational sources available for regular Fog-based operations [108]. Further, the cipher-text can consumes extra disk space than original text and in addition impacts the operating mechanism of application and database layers.*

Information encryption is a extensively used mechanism to guard information confidentiality. To overcome the higher resource allocation issues of encryption, best sensitive and critical information need to be encrypted, which include consumer’s identification in vehicular networks, patient information in healthcare systems, cached information and so on? For information at rest, the AES algorithm with 256-bit key size or obfuscation can be used to make sure privateness, at the same time as the secure Socket Layer (SSL) protocol can be used for establishing comfortable communication among a server and a client [109, 110]. In addition, efficient information integrity tests [111] need to be finished before and after communication to validate the received data and its sender. The important element right here is to actually distinguish among archival information and sensitive data. Encrypting archival information like public video streaming will reduce the performance of Fog system and effect upon the performance of sibling applications. It's far, therefore, critical for the designer of a Fog gadget to adequately determine the importance of the data and enforce –safety measures in which vital.

Preventing Cache Attacks

Advice 2*: Fog platforms maintained for Cache control gadget are vulnerable to software cache based side channel attacks such as exposing cryptographic keys, which might also lead closer to leaking sensitive information*.

Future Challenge 2*: Prevention of cache-based totally assaults is either too costly for sensible implementation or the solution only protects in opposition to a selected type of assault. Research suggests that cache interferences is the most common sort of attack, whose removal calls for each hardware and software adjustments [112].*

Fog structures which can be used for enhancing the overall performance and power efficiency of different systems the use of advanced memory caching strategies may be probed through Cache side Channel attacks [113], resulting within the exposure of sensitive information inside connected systems. The cache holds information that is frequently used and could incorporate private user information. Fog structures used in this manner need to encompass security solutions like Newcahe [114] and STEALTHMEM [115]. Those answers are alternative low-level implementations of a security-centric memory cache system that can better protect residing information. For new cache designs, answers like Partition Locked cache and Random Permutation cache [116] can relieve Fog community from cache interferences attacks. Similarly, the mechanism to prevent changes in smart meter information in the advanced metering infrastructure might be to retain collected information in Fog node for particular duration of time earlier than release. Despite the fact that these security solutions are costly and difficult to enforce, Fog platform developers have to remember them as it's far crucial not to depend on preferred default implementations which could result in widespread weaknesses.

Network Monitoring

Advice 3*: Fog structures which are constantly coping with personal information (e.g generated by IoT device) from end-user to Cloud platform and vice versa, need to monitor and detect anomalous activity in* network via automated enforcement of communication security policies and guidelines.

Future Challenge 3: *A Fog network is commonly linked to massive number of small devices. The information generated by way of a single device can be small, but when the streams of a couple of gadgets are combined, the amount of overall information will become significantly hard to handle [117]. Hence, filtering each network packet might instigate the necessity to increasing processing and memory ability.*

Every Fog platform must enforce aid efficient network monitoring mechanisms. They must be taken into consideration as a critical part of each Fog machine, so that malicious activity may be diagnosed and terminated before any real damage happens. The essential underlying process comprises of scanning dynamic and huge networks to mark suspicious and malicious network packets based on pre-defined policies and regulations. A Fog platform can set up efficient tools like CLOUDWATCHER [118] for partial network monitoring by means of choosing specific devices and PayLess [119] for scanning SDN communication with minimal computing sources. The network scanning method can be labeled as static, dynamic or an aggregate of both. Scanning is generally achieved by using assorting Firewalls, Anti-viruses and Intrusion Detection and Prevention structures [120–122]. For similarly development, the network tracking applications can begin working in distributed and intelligent way. They are able to use artificial Neural Networks (ANNs) and rule matching [123] for

Threat detection as a large quantity of heterogeneous (IoT) gadgets is transmitting and processing heterogeneous data on a couple of stages (hypervisor, working machine, and programs). Moreover, because of the localized nature of Fog devices, the implementation of Virtual Private Networks (VPNs) also can assist in keeping apart the network from outside assaults.

(Zero Day) Malware Protection

***Advice 4**: Fog systems need to protect themselves towards both new and existing malware-based attacks, that could arise in the form of virus, trojan,rootkit, spyware and worms to avoid undesirable contamination and serious harm.*

***Future Challenge 4**: The ever increasing complexity of malware assaults, lack of modern day threats detection, possibility of more zero day vulnerabilities, and the and sparse nature of connected (cellular) gadgets provides massive safety challenges. The Fog system additionally requires a lightweight, cross-storage host agent and a network-based detection service to completely protect towards those threats [124].*

Most Fog structures are missing suitable malware safety schemes as they requires dedicated and non-stop allocation of network and computation assets, which may not be available in each Fog platform. With the presence of a massive number of end-users and zero day threats, any user's device or malicious tenant could (unknowingly) inject and spread malware, which as a result could compromise the whole community. As many Fog structures are also deployed on smart-phones and drugs consisting of in BCI programs, they are able to emerge as a source of malware contamination [125]. One appropriate answer could be a physical malware detection device [126] as it would use minimum Fog resources. By increasing the Fog platform specifications, equipment like BareCloud [127] can be deployed, that may routinely locate evasive malware. Moreover, machine learning strategies [128–130] may be applied to identify zero day attacks with better accuracy. These techniques basically train algorithms like support vector machines with a benign software model and after that, any unusual behavior can trigger the detection event. apart from stealing information or modifying core device functionality, the presence of malware can decrease gadget overall performance. As a result, it is vital to continuously experiment for compromised nodes and install counter-measures to prevent the inclusion of malicious nodes and end-user devices. those designing and growing Fog structures might need to take into account the capacity of underlying running system [131] to turn out to be compromised and considering how their system, and its physical implications can be covered to minimize damage. For example, inside the health-care domain, it would be important that if a Fog system became compromised, that critical information and functionality would still be protected by having strong integrity tests and ensure that the machine is quarantined as quickly as malicious activity appears within the host operating system.

Wireless Security

***Advice 5:** The internal and external wireless communications of Fog platform with end-user gadgets want to minimize packet sniffing, rouge access points and similar challenges by imposing both encryption and authentication processes.*

***Future Challenge 5**: Fog structures are mainly composed of wireless sensors and IoT devices [132].Due to the volume and visibility of every wireless capable device, it's far difficult to make certain the security of the Fog network. If no longer hidden and secured, the wireless network offers exceptional freedom to attackers to intercept sensitive information in transmission.*

Many wireless devices, which includes health tracking, camera sensors, RFIDs and mobile phones are connected with Fog platforms and are constantly transmitting personal information from nearby places. It's far vital that their communication is encrypted using Wi-Fi safety algorithms like WiFi protected access (WPA),WPA2 [133] etc. Wireless access points are commonly visible to all gadgets without any connection. If they're no longer well secured, attacker can emerge as part of network (Sybil assault), use bandwidth illegally (Flood assault) and intercept network visitors using MiTM attack to alter or even terminate information communication [134]. In case of medical applications, insecure wireless connection might also put human life at threat. It is therefore of crucial importance to enforce wireless protocols like 802.11 or its amendments: 802.11a and 802.11g. in addition, exceptional intrusion detection strategies can be used for protective the communication of heterogeneous 5G cellular networks as discussed in a latest survey paper [135].

Secured Vehicular Networks

***Advice 6**: in an effort to boom road safety and real-time application of vehicular networks, they ought to guard themselves from internal and external protection threats.*

***Future Challenge 6:** A vehicular Fog community is unstable because the connection with end-user is set up for handiest a shorter time frame, which makes it difficult to verify identities .The quantity of connections, heterogeneous facts and elements of multi-hop connection can boom to a big scale, so one can render even a robust protection device useless. [136].*

While the usage of a Fog platform to aid vehicular community, the safety protocols must no longer be limited to BSs, SDNCs and RSUCs but need to also embody Fog devices that are simply processing, storing and forwarding vehicular information. A Fog device should secure itself by using authenticating user identity, take a look at for information consistency and integrity, provider availability, capability to revoke any connection and nameless key control as well as beautify the protection of connected systems by means of tracking and placing actual-time constraints [137]. If Fog nodes are able to performing user authentication and message integrity tests, it'll put off message suppression, fabrication, replay and alteration assaults [138]. The method need to be nameless and stateless like STAMP [139], in order that the consumer's area and identity is kept personal, even from the Fog community. The implementation of such safety features among vehicles and Fog nodes will prevent primitive assaults before they reach and make the most cloud system too, and could help in improving the common road safety.

Secured Multi-Tenancy

Advice 7*: Fog computing should enable exceptionally confined access control on each information and network, along with truthful resource allocation mechanisms to defend confidentiality and integrity within a multi-user environment.*

Future Challenge 7: *when a huge number of end-users start to share Fog packages and resources, the overall performance, scalability, information security, person identification management, monitoring and the capability arising from insiders' threats will become difficult to manipulate in a Fog network [140].*

As stated above, Fog systems are a relatively virtualized environment, supporting multi-tenancy and are able to provisioning resource management centers to Cloud systems. Many safety issues are pushed by multi-tenancy implementations, such as co-resident information, malicious tenants, eavesdropping, memory escaping and hopping and misconfiguration [141, 142]. Fog systems need to enforce multi-aspect authentication mechanisms based on either the function or identification of end users, logically segregate information and sources and aggressively analyze the activities of each administrator and tenants. Another system referred to as secure and Resilient Networking (SeReNe) service can provide a Fog platform with programmable environment to alter its topology, bandwidth allocation, and traffic policies [143]. Furthermore, as many devices are connected, Fog system have to be able to pretty allocate compute sources among users in the meantime preventing virtualization-based (hypervisor and VM) assaults (as shown in table 2) to maintain the infrastructure to be had.

Backup and Restoration

Advice 8: *Depending upon the form of application,*
Fog systems have information backup and restoration modules. Such systems must replicate copies of information on-site, off-site or each on a regular basis. It will benefit both customers and company to keep the operations running from using previous backups, minimizing service disruptions.

Future Challenge 8*: The Fog platform has a high frequency of information throughput and relatively low quantity of stored information; however this does rely upon the necessities and application. The assignment is that statistics backup and recovery is a expensive technique [144] and requires acute awareness on information selecting, mapping, testing and figuring out accessibility roles in case of recovery procedure.*

In case of natural catastrophe, system failure or cyber attack, Fog platforms can lose all information and consequently there may be a need for primary and secondary backups. The selection of information that goes in to backup depends upon the sensitivity, demand and its role in day to day operations. According to [145], it is important to not duplicate the information earlier than backup. It will decrease costs and extensively lessen the intake of sources throughout backup process and recovery. There also are many techniques every day to improve the method in terms of consistency, co-ordination and performance, such as Fibre Channel, High Security Distribution and Rake Technology (HS-DRT), Parity Cloud Service technique (PCS), Efficient Routing Grounded on Taxonomy (ERGOT), Cold and Hot Backup Service Replacement strategy (CBSRS) and Shared Backup Router Resources (SBRR) [146]. Further enhancements for the Fog platform are backup and healing approaches for SSD assisted database structures [147] and VM images [148] as an entire. For mobile and wireless Fog structures, the scenario may get challenging as the system could require portable and on-site backup storage or will need a massive quantity of network bandwidth day transmit information day the off-site region.

Protection with Performance

Advice 9*: A balanced exchange-off among the degree of functionality and integrated security is crucial for Fog community performance. It's going to permit absolutely featured applications meanwhile protecting the CIA of information and networks against internal and external threats.*

Future Challenge 9*: A poor safety device implementation could have huge overall performance issues. Subsequently, it's far crucial to cautiously select, in-accordance with the necessities, what safety functions to integrate, the degree and extent of usage, required components and defining performance benchmarks.*

It is not continually the case that improving the security posture of a gadget does no longer always suggest to compromise on performance. It's matter of trade-off among features and removal of unneeded security measures to make effective use of available sources. A Fog community is capable of sharing information loads, and their computing assets also can be expanded on-demand, even though it may not be the case for each single Fog platform. This is probably a cause why many safety solutions mentioned in section existing security solutions for Fog computing do not consider the lack of Fog resources as a problem, as the computing power can be extended. The safety solutions must emerge as an integral a part of each Fog platform because if they are insecure, their performance might decrease ultimately due to assaults like malware infection, resource abuse, and so forth. A large range of IoT devices sending information toward Cloud systems creates a subtle role for intermediate processing on a Fog platform. If security solutions are constructed within Fog software program and no longer as a bolt-on addition, it would help to reduce the resource utilization as well. Despite the fact that the principle reason of a Fog platform is to offload obligations for higher overall performance, the security measures must be taken under consideration as an essential component of the Fog device for keeping CIA of all kinds of information. Consequently, the primary task for Fog platform developer is to construct a system that may successfully provision security without making eminent sacrifices in overall performance.

Table 3 Summary of potential security issues found in Fog applications

Attack category	**Possible threats**	**Possible solutions**	**Impact**
Virtualization issues	Hypervisor attacks	Multi-factor Authentication	As all services and VMs are executing in a virtualized environment, its compromise will have adverse effect on all Fog services, data and users
	VM-based attacks	Intrusion Detection System	
	Weak or no Logical Segregation	User data isolation	
	Side channel attacks	Attribute/identity based encryption	
	Privilege Escalation	Role-Based Access Control model	
	Service abuse	User-based permissions model	
	Privilege escalation attacks	Process isolation	
	Inefficient resource policies		
Web security issues	SQL injection	Secure code	Exposure of sensitive information, attacker can become legitimate part of network, and enable malicious applications to install
	Cross-site scripting	Find and patch vulnerabilities	
	Cross-site request forgery	Regular software updates	
	Session/Account hijacking	Periodic auditing	
	Insecure direct object references	Firewall	
	Malicious redirections	Anti-virus protection	
	Drive-by attacks	Intrusion Prevention System	
Internal/external communication issues	Man-in-the-Middle attack	Encrypted communication	Attacker can acquire sensitive information by eavesdropping and get access to unauthorized Fog resources
	Inefficient rules/policies	Mutual/Multi-factor authentication	
	Poor access control	Partial encryption	
	Session/Account hijacking	Isolating compromised nodes	
	Insecure APIs and services	Certificate pinning	
	Application vulnerabilities	Limiting number of connections	
	Single-point of failure	Transport layer security (TLS)	
Data security related issues	Data replication and sharing	Policy enforcement	High probability of illegal file and database access, where attacker
	Data altering and erasing attacks	Security inside design architecture	

	Illegal data access	Encryption	can compromise both user and Fog system's data
	Data ownership issues	Secure key management	
	Low attack tolerance	Obfuscation	
	Malicious Insiders	Data Masking	
	Multi-tenancy issues	Data classification	
	Denial of Service attacks	Network monitoring	
Wireless security issues	Active impersonation	Authentication	Vulnerable wireless access points can compromise communication privacy, consistency, accuracy, availability and trustworthiness
	Message replay attacks	Encrypted communication	
	Message distortion issues	Key management service	
	Data loss	Secure routing	
	Data breach	Private network	
	Sniffing attacks	Wireless security protocols	
	Illegal resource consumption		
Malware protection	Virus	Anti-malware programs	Malware infected nodes will lower the performance of the entire Fog platform, allow back-doors to the system and corrupt/damage data permanently
	Trojans	Intrusion Detection System	
	Worms	Rigorous data backups	
	Ransomware	Patching vulnerabilities	
	Spyware	System restore points	
	Rootkits		
	Performance reduction		

Conclusion and future work

Table 4 Summary of recommended security solutions and impact on CIA

Solution category	Resolves	Benefits
Data Encryption	Malicious insiders	If data is breached either at rest, processing or motion, encryption will keep the original data hidden from unauthorized recipients
	Data Breach	
	Data Loss	
	Insufficient Due Diligence	
	Spyware/malicious processes	
Preventing cache attacks	Insecure API	If a Fog platform is acting as cache server, the frequently accessed (relevant and sensitive) data by users or other systems via Fog will remain private
	Service and application vulnerabilities	
	Sensitive data Leakage	
	Sniffing attacks	
Network monitoring	Advance Persistent Threats	Can immediately notify about the ongoing attack, log malicious events for analysis, block suspicious ingress/egress network traffic and determine/indicate overall health and performance of system
	Access control issues	
	Denial of Service attack	
	Malicious Insiders	
	Insufficient Due Diligence	
	Abuse and Nefarious use of resources	
	Data Breaches	
	Attack detection	
Malware protection	Account Hijacking	Provides real-time scanning and removal of known malicious applications (static analysis), protects against zero-day exploits by intelligent event/behaviour monitoring (dynamic analysis) and ensures consistent performance of the Fog platform
	Insecure API	
	Service and application vulnerabilities	
	Data corruption/damage risks	
	Shared Technology Issues	
	Performance degradation	

Wireless security	Advance Persistent Threats	Fog nodes can increase their mobility in secure manner, enables more IoT devices to connect from anywhere and allows the Fog platform to become more cost effective
	Access control issues	
	Data breach	
	Eavesdropping attacks	
	Illegal bandwidth consumption	
Securing vehicular networks	Advance Persistent Threats	Increases road safety by preserving data communication integrity while keeping the user identity and location data private
	Access control issues	
	Account/Session Hijacking	
	Denial of Service attacks	
	User identity protection	
Secured multi-tenancy	Access control issues	Secure data collaboration among approved users, prevention of memory escaping/ hopping attacks to protect each user's space and increase in efficient use and allocation of Fog resources
	Account Hijacking	
	Insecure APIs	
	Malicious Insiders	
	Abuse and Nefarious use of resources	
	Data Breaches	
	Segregation Issues	
Backup and recovery	Data Loss	In case of natural disaster, malware infection or DoS attack, the data will remain available to users and system along with its integrity
	Data unavailability issues	
	Insufficient Due Diligence	
	Malware infection	
	Data integrity issues	

The motive of this study changed into to review and examine real world Fog computing applications to become aware of their viable security flaws. To offer a holistic review, Fog associated technologies like edge computing and Cloudlets are also discussed. It was observed that most Fog application-s do now not bear in mind safety as part of gadget, but alternatively focus on functionality, which ends up in many Fog systems being inclined. Literature additionally information that Fog computing has a wide capacity and variety of packages that every one demand a excessive level of safety to guard the CIA of the customer facts. Fog systems are a exceptionally new paradigm, and this take a look at can assist readers and developers to foresee security measures and their challenges, even as envisaging the design of latest Fog systems. Table 4 summarizes the discussion of how advocated security answers (see section encouraged security measures and future challenges) is probably capable of prevents, hit upon and seasoned-actively protect against the threats stated in table 3. The aim of these security solutions is to shield the CIA of complete Fog system and its customers. Additionally, Fig. 4 illustrates the possible security answer categories with admire to numerous additives of Fog infrastructure, living between IoT devices and Cloud.

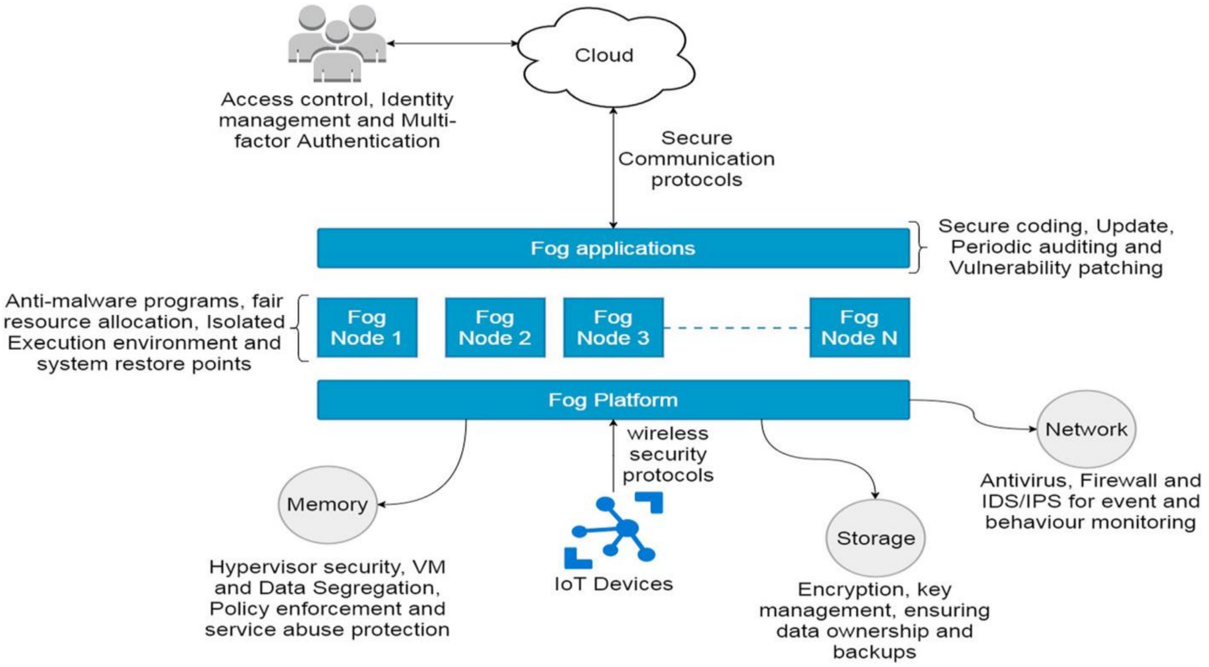
Cloud
Access control, Identity management and Multi-factor Authentication
Secure Communication protocols
Fog applications
Secure coding, Update, Periodic auditing and Vulnerability patching
Anti-malware programs, fair resource allocation, Isolated Execution environment and system restore points
Fog Node 1
Fog Node 2
Fog Node 3
Fog Node N
Fog Platform
wireless security protocols
Network
Antivirus, Firewall and IDS/IPS for event and behaviour monitoring
Memory
Hypervisor security, VM and Data Segregation, Policy enforcement and service abuse protection
IoT Devices
Storage
Encryption, key management, ensuring data ownership and backups

Fig. 4 Fog Computing Platform and the deployment of security solutions on various components of the Fog system. This figure shows how and where proposed security solutions can be placed and help in eliminating various security flaws

References

1. Sagiroglu S, Sinanc D (2013) Big data: A review. In: Collaboration Technologies and Systems (CTS), 2013 International Conference On.IEEE. pp 42–47
2. Cisco (2015) Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Online:https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-solutions.pdf. Accessed 13 Dec 2016
3. Tang B, Chen Z, Hefferman G, Wei T, He H, Yang Q (2015) A hierarchical distributed fog computing architecture for big data analysis in smart cities. In: Proceedings of the ASE BigData & SocialInformatics 2015. ACM. p 28
4. Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011) Cloud computing-the business perspective. Decis Support Syst 51(1):176–189
5. Parkinson S, Ward P, Wilson K, Miller J (2017) Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans Intell Transp Syst PP(99):1–18. doi:10.1109/TITS.2017.2665968
6. Stojmenovic I, Wen S (2014) The fog computing paradigm: Scenarios and security issues. In: Computer Science and Information Systems (FedCSIS), 2014 Federated Conference On. IEEE. pp 1–8
7. Kim JY, Schulzrinne H (2013) Cloud support for latency-sensitive telephony applications. In: Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference On, vol. 1. IEEE. pp 421–426
8. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. ACM. pp 13–16
9. Sareen P, Kumar P (2016) The fog computing paradigm. Int J Emerging Technol Eng Res 4:55–60
10. Vaquero LM, Rodero-Merino L (2014) Finding your way in the fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM Comput Commun Rev 44(5):27–32
11. Saharan K, Kumar A (2015) Fog in comparison to cloud: A survey. Int JComput Appl 122(3):10–12
12. Dastjerdi AV, Gupta H, Calheiros RN, Ghosh SK, Buyya R (2016) Fog computing: Principals, architectures, and applications. arXiv preprint arXiv:1601.02752
13. Mahmud R, Buyya R (2016) Fog computing: A taxonomy, survey and future directions. arXiv preprint arXiv:1611.05539
14. Cisco (2015) Cisco Fog Computing Solutions: Unleash the Power of the Internet of Things. Online: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-solutions.pdf. Accessed 13 Dec 2016
15. Schumacher M, Fernandez-Buglioni E, Hybertson D, Buschmann F,Sommerlad P (2013) Security Patterns: Integrating security and systems engineering. Wiley
16. Satyanarayanan M (2015) A brief history of cloud offload: A personal journey from odyssey through cyber foraging to cloudlets. GetMobile:Mob Comput Commun 18(4):19–23

17. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Futur Gener Comput Syst 28(3):583–592
18. Alliance CS (2016) The Treacherous 12 Cloud Computing Top Threats in 2016. Online: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats. pdf. Accessed 22 Dec 2016
19. Stojmenovic I, Wen S, Huang X, Luan H (2015) An overview of fog computing and its security issues. Concurrency and Computation: Practice and Experience
20. Yi S, Qin Z, Li Q (2015) Security and privacy issues of fog computing: A survey. In: International Conference on Wireless Algorithms, Systems, and Applications. Springer. pp 685–695
21. Klas GI (2015) Fog computing and mobile edge cloud gain momentum open fog consortium, etsi mec and cloudlets
22. Ahmed A, Ahmed E (2016) A survey on mobile edge computing. In: Intelligent Systems and Control (ISCO), 2016 10th International Conference On. IEEE. pp 1–8
23. Series Q, Safety MQ. Programmable automation controller
24. Pierson RM (2016) How Does Fog Computing Differ from Edge Computing? Online: https://readwrite.com/2016/08/05/fogcomputing- different-edge-computing-pl1/. Accessed 12 June 2017
25. Ha K, Satyanarayanan M (2015) Openstack++ for cloudlet deployment. School of Computer Science Carnegie Mellon University Pittsburgh
26. Li Y, Wang W (2013) The unheralded power of cloudlet computing in the vicinity of mobile devices. In: Globecom Workshops (GC Wkshps), 2013 IEEE. IEEE. pp 4994–4999
27. Jaiswal A, Thakare V, Sherekar S. Performance based analysis of cloudlet architectures in mobile cloud computing
28. Bahl V (2015) Emergence of Micro Datacenter (cloudlets/edges) for Mobile Computing. Online: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/11/Micro-Data-Centers-mDCs-for-Mobile-Computing-1.pdf. Accessed 12 June 2017
29. Liang K, Zhao L, Chu X, Chen H-H (2017) An integrated architecture for software defined and virtualized radio access networks with fog computing. IEEE Netw 31(1):80–87
30. Clinch S, Harkes J, Friday A, Davies N, Satyanarayanan M (2012) How close is close enough? Understanding the role of cloudlets in supporting display appropriation by mobile users. In: Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference On. IEEE. pp 122–127
31. Sindhu S, Mukherjee S (2011) Efficient task scheduling algorithms for cloud computing environment. In: High Performance Architecture and Grid Computing. Springer. pp 79–83
32. Satyanarayanan M, Bahl P, Caceres R, Davies N (2009) The case for vm-based cloudlets in mobile computing. IEEE Pervasive Comput 8(4):14–23
33. University CM (2017) Elijah: Cloudlet Infrastructure for Mobile Computing. GitHub
34. Almorsy M, Grundy J, Müller I (2016) An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107
35. Younis YA, Kifayat K, Shi Q, Askwith B (2015) A new prime and probe cache side-channel attack for cloud computing. In: Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference On. IEEE. pp 1718–1724
36. Shahid MA, Sharif M (2015) Cloud computing security models, architectures, issues and challenges: A survey. Smart Comput Rev 5:602–616
37. Zhu J, Chan DS, Prabhu MS, Natarajan P, Hu H, Bonomi F (2013) Improving web sites performance using edge servers in fog computing architecture. In: Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium On. IEEE. pp 320–323
38. Krishnan YN, Bhagwat CN, Utpat AP (2015) Fog computing-network based cloud computing. In: Electronics and Communication Systems (ICECS), 2015 2nd International Conference On. IEEE. pp 250–251
39. Abdullahi I, Arif S, Hassan S (2015) Ubiquitous shift with information centric network caching using fog computing. In: Computational Intelligence in Information Systems. Springer. pp 327–335
40. Su J, Lin F, Zhou X, Lu X (2015) Steiner tree based optimal resource caching scheme in fog computing. China Commun 12(8):161–168
41. Sivasubramanian S, Pierre G, Van Steen M, Alonso G (2007) Analysis of caching and replication strategies for web applications. IEEE Internet Comput 11(1):60-66
42. Halfond WG, Viegas J, Orso A (2006) A classification of sql-injection attacks and counter measures. In: Proceedings of the IEEE International Symposium on Secure Software Engineering, vol. 1. IEEE. pp 13–15
43. Egele M, Kirda E, Kruegel C (2009) Mitigating drive-by download attacks: Challenges and open problems. In:

iNetSec 2009–Open Research Problems in Network Security. Springer. pp 52–62
44. Gao L, Luan TH, Liu B, Zhou W, Yu S (2017) Fog computing and its applications in 5g. In: 5G Mobile Communications. Springer. pp 571–593
45. Luan TH, Gao L, Li Z, Xiang Y, Sun L (2015) Fog computing: Focusing on mobile users at the edge. arXiv preprint arXiv:1502.01815
46. Oueis J, Strinati EC, Barbarossa S (2015) The fog balancing: Load distribution for small cell cloud computing. In: 2015 IEEE 81st Vehicular Technology Conference (VTC Spring). IEEE. pp 1–6
47. Hu YC, Patel M, Sabella D, Sprecher N, Young V (2015) Mobile edge computing-a key technology towards 5g. ETSI White Paper 11:1–16
48. Desmedt Y (2011) Man-in-the-middle attack. In: Encyclopedia of Cryptography and Security. Springer. pp 759–759
49. Nayak GN, Samaddar SG (2010) Different flavours of man-in-the-middle attack, consequences and feasible solutions. In: Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference On, vol. 5. IEEE. pp 491–495
50. Nazmudeen MSH, Wan AT, Buhari SM (2016) Improved throughput for power line communication (plc) for smart meters using fog computing based data aggregation approach. In: Smart Cities Conference (ISC2),2016 IEEE International. IEEE. pp 1–4
51. Yan Y, Su W (2016) A fog computing solution for advanced metering infrastructure. In: Transmission and Distribution Conference and Exposition (T&D), 2016 IEEE/PES. IEEE. pp 1–4
52. Ozdemir S, Xiao Y (2009) Secure data aggregation in wireless sensor networks: A comprehensive overview. Comput Netw 53(12):2022–2037
53. Rajagopalan SR, Sankar L, Mohajer S, Poor HV (2011) Smart meter privacy: A utility-privacy framework. In: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference On. IEEE. pp 190–195
54. McDaniel P, McLaughlin S(2009)Security& privacy challenges in the smart grid.IEEE Secur Privacy 7(3):75–77
55. Prieto González L, Prieto González L, Jaedicke C, Jaedicke C, Schubert J, Schubert J, Stantchev V, Stantchev V (2016) Fog computing architectures for healthcare: Wireless performance and semantic opportunities. J Inf Commun Ethics Soc 14(4):334–349
56. Stantchev V, Barnawi A, Ghulam S, Schubert J, Tamm G (2015) Smart items, fog and cloud computing as enablers of servitization in healthcare. Sensors Transducers 185(2):121
57. Shi Y, Ding G, Wang H, Roman HE, Lu S (2015) The fog computing service for healthcare. In: Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015 2nd International Symposium On. IEEE. pp 1–5
58. Gia TN, Jiang M, Rahmani AM, Westerlund T, Liljeberg P, Tenhunen H (2015) Fog computing in healthcare internet of things: A case study on ecg feature extraction. In: Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference On. IEEE. pp 356–363
59. Cao Y, Hou P, Brown D, Wang J, Chen S (2015) Distributed analytics and edge intelligence: Pervasive health monitoring at the era of fog computing. In: Proceedings of the 2015 Workshop on Mobile Big Data.ACM. pp 43–48
60. Cao Y, Chen S, Hou P, Brown D (2015) Fast: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation. In:Networking, Architecture and Storage (NAS), 2015 IEEE International Conference On. IEEE. pp 2–11
61. Li M, Yu S, Ren K, Lou W (2010) Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In: International Conference on Security and Privacy in Communication Systems. Springer. pp 89–106
62. Ren K, Lou W, Zhang Y (2008) Leds: Providing location-aware end-to-end data security in wireless sensor networks. IEEE Trans Mobile Comput 7(5):585–598
63. Chen N, Chen Y, You Y, Ling H, Liang P, Zimmermann R (2016) Dynamic urban surveillance video stream processing using fog computing. In: Multimedia Big Data (BigMM), 2016 IEEE Second International Conference On. IEEE. pp 105–112
64. Shi W, Dustdar S (2016) The promise of edge computing. Computer 49(5):78–81
65. Do CT, Tran NH, Pham C, Alam MGR, Son JH, Hong CS (2015) A proximal algorithm for joint resource allocation and minimizing carbon footprint in geo-distributed fog computing. In: 2015 International Conference on Information Networking (ICOIN). IEEE. pp 324–329
66. Varalakshmi L, Sudha GF, Jaikishan G (2014) A selective encryption and energy efficient clustering scheme for video streaming in wireless sensor networks. Telecommun Syst 56(3):357–365
67. Truong NB, Lee GM, Ghamri-Doudane Y (2015) Software defined networking-based vehicular adhoc network

with fog computing. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE. pp 1202–1207
68. Datta SK, Bonnet C, Haerri J (2015) Fog computing architecture to enable consumer centric internet of things services. In: 2015 International Symposium on Consumer Electronics (ISCE). IEEE. pp 1–2
69. Roy S, Bose R, Sarddar D (2015) A fog-based dss model for driving rule violation monitoring framework on the internet of things. Int J Adv Sci Technol 82:23–32
70. Joshi B, Singh NK (2016) Mitigating dynamic dos attacks in mobile ad hoc network. In: Colossal Data Analysis and Networking (CDAN), Symposium On. IEEE. pp 1–7
71. Defta LC, Iacob NM (2016) Aodv-authentication mechanism in manet.Calitatea 17(S3):59
72. Chen RY (2017) An intelligent value stream-based approach to collaboration of food traceability cyber physical system by fog computing. Food Control 71:124–136
73. Saqib A, Anwar RW, Hussain OK, Ahmad M, Ngadi MA, Mohamad MM, Malki Z, Noraini C, Jnr BA, Nor RNH, et al. (2015) Cyber security for cyber physcial systems: A trust-based approach. J Theor Appl Inf Technol 71(2):144–152
74. Monteiro A, Dubey H, Mahler L, Yang Q, Mankodiya K (2016) Fit a fog computing device for speech teletreatments. arXiv preprint arXiv:1605.06236
75. Orsini G, Bade D, Lamersdorf W (2015) Computing at the mobile edge: Designing elastic android applications for computation offloading. In:IFIP Wireless and Mobile Networking Conference (WMNC), 2015 8th.IEEE. pp 112–119
76. Heuser S, Negro M, Pendyala PK, Sadeghi AR (2016) Droidauditor : Forensic analysis of application-layer privilege escalation attacks on android. Technical report. Technical report, TU Darmstadt
77. Wei X, Gomez L, Neamtiu I, Faloutsos M (2012) Malicious android applications in the enterprise: What do they do and how do we fix it? In: Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference On. IEEE. pp 251–254
78. Singh P, Tiwari P, Singh S (2016) Analysis of malicious behavior of android apps. Procedia Comput Sci 79:215–220
79. Zao JK, Gan TT, You CK, Méndez SJR, Chung CE, Te Wang Y, Mullen T, Jung TP (2014) Augmented brain computer interaction based on fog computing and linked data. In: Intelligent Environments (IE), 2014 International Conference On. IEEE. pp 374–377
80. Zao JK, Gan TT, You CK, Chung CE, Wang YT, Méndez SJR, Mullen T, Yu C Kothe C, Hsiao CT, et al. (2014) Pervasive brain monitoring and data sharing based on multi-tier distributed computing and linked data technology. Front Hum Neurosci 8:370–386
81. Dubey H, Yang J, Constant N, Amiri AM, Yang Q, Makodiya K (2015) Fog data: enhancing telehealth big data through fog computing. In: Proceedings of the ASE BigData & SocialInformatics 2015. ACM. p 14
82. Ha DA, Nguyen KT, Zao JK (2016) Efficient authentication of resource-constrained iot devices based on ecqv implicit certificates and datagram transport layer security protocol. In: Proceedings of the Seventh Symposium on Information and Communication Technology. ACM. pp 173–179
83. Aazam M, Huh EN (2015) Fog computing micro datacenter based dynamic resource estimation and pricing model for iot. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications. IEEE. pp 687–694
84. Dastjerdi AV, Buyya R (2016) Fog computing: Helping the internet of things realize its potential. Computer 49(8):112–116
85. Mao Y, Li J, Chen MR, Liu J, Xie C, Zhan Y (2016) Fully secure fuzzy identity-based encryption for secure iot communications. Comput Standards Interfaces 44:117–121
86. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R (2001) Proposed nist standard for role-based access control. ACM Trans Inf Syst Security (TISSEC) 4(3):224–274
87. Jalali F, Hinton K, Ayre R, Alpcan T, Tucker RS (2016) Fog computing may help to save energy in cloud computing. IEEE J Selected Areas Commun 34(5):1728–1739
88. Deng R, Lu R, Lai C, Luan TH (2015) Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing. In: 2015 IEEE International Conference on Communications (ICC). IEEE. pp 3909–3914
89. Di Lorenzo P, Barbarossa S, Sardellitti S (2013) Joint optimization of radio resources and code partitioning in mobile edge computing. arXiv preprint arXiv:1307.3835
90. Chang V, Ramachandran M (2016) Towards achieving data security with the cloud computing adoption framework. IEEE Trans Serv Comput 9(1):138–151
91. Jayanth HC (2014) A fog computing architecture for disaster response networks. PhD thesis, Texas A&M University
92. Satyanarayanan M, Lewis G, Morris E, Simanta S, Boleng J, Ha K (2013) The role of cloudlets in hostile

environments. IEEE Pervasive Comput 12(4):40–49
93. Lewis G, Echeverría S, Simanta S, Bradshaw B, Root J (2014) Tactical cloudlets: Moving cloud computing to the edge. In: Military Communications Conference (MILCOM), 2014 IEEE. IEEE. pp 1440–1446
94. Ochang PA, Irving P (2016) Performance analysis of wireless network throughput and security protocol integration. Int J Future Generation Commun Netw 9(1):71–78
95. Kulkarni S, Saha S, Hockenbury R (2014) Preserving privacy in sensor-fog networks. In: Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference For. IEEE. pp 96–99
96. Stolfo SJ, Salem MB, Keromytis AD (2012) Fog computing: Mitigating insider data theft attacks in the cloud. In: Security and Privacy Workshops (SPW), 2012 IEEE Symposium On. IEEE. pp 125–128
97. Vaux DL, Fidler F, Cumming G (2012) Replicates and repeats-what is the difference and is it significant? EMBO Reports 13(4):291–296
98. Sudha I, Kannaki A, Jeevidha S (2014) Alleviating internal data theft attacks by decoy technology in cloud. IJCSMC, March
99. Dong MT, Zhou X (2016) Fog computing: Comprehensive approach for security data theft attack using elliptic curve cryptography and decoy technology. Open Access Library J 3(09):1
100. Dsouza C, Ahn GJ, Taguinod M (2014) Policy-driven security management for fog computing: Preliminary framework and a case study. In: Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference On. IEEE. pp 16–23
101. Mirkovic J, Reiher P (2004) A taxonomy of ddos attack and ddos defense mechanisms. ACM SIGCOMM Comput Commun Rev 34(2):39–53
102. Shtern M, Sandel R, Litoiu M, Bachalo C, Theodorou V (2014) Towards mitigation of low and slow application ddos attacks. In: Cloud Engineering (IC2E), 2014 IEEE International Conference On. IEEE. pp 604–609
103. Gentry C (2009) Fully homomorphic encryption using ideal lattices. In:STOC, vol. 9. ACM. pp 169–178
104. Bos JW, Castryck W, Iliashenko I, Vercauteren F (2017) Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling. In: International Conference on Cryptology in Africa. Springer. pp 184–201
105. Lu R, Liang X, Li X, Lin X, Shen X (2012) Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distributed Syst 23(9):1621–1631
106. Vishwanath A, Peruri R, He JS (2016) Security in fog computing through encryption. Int J Inf Technol Comput Sci (IJITCS) 8(5):28
107. Mahajan P, Sachdeva A (2013) A study of encryption algorithms aes, des and rsa for security. Global J Comput Sci Technol 13(15):15–22
108. Shmueli E, Vaisenberg R, Elovici Y, Glezer C (2010) Database encryption: an overview of contemporary challenges and design considerations. ACM SIGMOD Record 38(3):29–34
109. Varriale A, Prinetto P, Carelli A, Trotta P (2016) SEcube (TM): Data at rest and data in motion protection. In: Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), Athens. pp 138–144
110. Hussein NH, Khalid A, Khanfar K (2016) A survey of cryptography cloud storage techniques
111. Wang Q, Wang C, Li J, Ren K, Lou W (2009) Enabling public verifiability and data dynamics for storage security in cloud computing. In: European Symposium on Research in Computer Security. Springer. pp 355–370
112. Page D (2003) Defending against cache-based side-channel attacks. Inf Security Technical Rep 8(1):30–44
113. Acıiçmez O, Koç Ç,K (2006) Trace-driven cache attacks on aes (short paper). In: International Conference on Information and Communications Security. Springer. pp 112–121
114. Liu F, Lee RB (2013) Security testing of a secure cache design. In: Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy. ACM. p 3
115. Kim T, Peinado M, Mainar-Ruiz G (2012) STEALTHMEM: System-level protection against cache-based side channel attacks in the cloud. In: USENIX Security Symposium. Usenix. pp 189–204
116. Kong J, Aciicmez O, Seifert JP, Zhou H (2008) Deconstructing new cache designs for thwarting software cache-based side channel attacks. In: Proceedings of the 2nd ACM Workshop on Computer Security Architectures. ACM. pp 25–34
117. Hu F, Hao Q, Bao K (2014) A survey on software-defined network and openflow: From concept to implementation. IEEE Commun Surv Tutorials 16(4):2181–2206
118. Shin S, Gu G (2012) Cloudwatcher: Network security monitoring using openflow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?) In: Network Protocols (ICNP), 2012 20th IEEE International Conference On. IEEE. pp 1–6

119. Chowdhury SR, Bari MF, Ahmed R, Boutaba R (2014) Payless: A low cost network monitoring framework for software defined networks. In: Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE. pp 1–9
120. Aceto G, Botta A, De Donato W, Pescapè A (2013) Cloud monitoring: A survey. Comput Netw 57(9):2093–2115
121. Ab Rahman NH, Choo K-KR (2015) A survey of information security incident handling in the cloud. Comput Secur 49:45–69
122. Liu J, Liu F, Ansari N (2014) Monitoring and analyzing big traffic data of a large-scale cellular network with hadoop. IEEE Netw 28(4):32–39
123. Sawant MD, Phatak MM, Ranavde MA, Laxamanan NR (2015) Intelligent firewall using intrusion detection system based on neural networks. J Netw Inf Security 2(2):14–17
124. Hatem SS, El-Khouly MM, et al. (2014) Malware detection in cloud computing. Int J Adv Comput Sci Appl 5(4):187–192
125. Malhotra A, Bajaj K (2016) A survey on various malware detection techniques on mobile platform. Int J Comput Appl 139(5):15–20
126. Demme J, Maycock M, Schmitz J, Tang A, Waksman A, Sethumadhavan S, Stolfo S (2013) On the feasibility of online malware detection with performance counters. In: ACM SIGARCH Computer Architecture News vol. 41. ACM. pp 559–570
127. Kirat D, Vigna G, Kruegel C (2014) Barecloud: Bare-metal analysis-based evasive malware detection. In: USENIX Security. Usenix, University of California, Santa Barbara Vol. 2014. pp 287–301
128. Comar PM, Liu L, Saha S, Tan PN, Nucci A (2013) Combining supervised and unsupervised learning for zero-day malware detection. In: INFOCOM, 2013 Proceedings IEEE. IEEE. pp 2022–2030
129. Berlin K, Saxe J (2016) Improving zero-day malware testing methodology using statistically significant time-lagged test samples. arXiv preprint arXiv:1608.00669
130. Zolotukhin M, Hamalainen T (2014) Detection of zero-day malware based on the analysis of opcode sequences. In: Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th. IEEE. pp 386–391
131. Embleton S, Sparks S, Zou CC (2013) Smm rootkit: a new breed of os independent malware. Secur Commun Netw 6(12):1590–1605
132. Aazam M, Huh EN (2014) Fog computing and smart gateway based communication for cloud of things. In: Future Internet of Things and Cloud (FiCloud), 2014 International Conference On. IEEE. pp 464–470
133. Al Ameen M, Liu J, Kwak K (2012) Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 36(1):93–101
134. Pathan A-SK, Lee HW, Hong CS (2006) Security in wireless sensor networks: issues and challenges. In: Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, vol. 2. IEEE. p 6
135. Gai K, Qiu M, Tao L, Zhu Y (2015) Intrusion detection techniques for mobile cloud computing in heterogeneous 5g. Secur Commun Netw10:3049–3058
136. Mokhtar B, Azab M (2015) Survey on security issues in vehicular ad hoc networks. Alexandria Eng J 54(4):1115–1126
137. Razzaque M, Salehi A, Cheraghi SM (2013) Security and privacy in vehicular ad-hoc networks: survey and the road ahead. In: Wireless Networks and Security. Springer. pp 107–132
138. Rawat DB, Yan G, Bista BB, Weigle MC (2015) Trust on the security of wireless vehicular ad-hoc networking. Ad Hoc Sensor Wireless Netw 24(3-4):283–305
139. Boumerdassi S, Renault É, Muhlethaler P (2016) A stateless time-based authenticated-message protocol for wireless sensor networks (stamp). In: Wireless Communications and Networking Conference (WCNC), 2016 IEEE. IEEE. pp 1–6
140. Bezemer CP, Zaidman A (2010) Multi-tenant saas applications: maintenance dream or nightmare? In: Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE). ACM. pp 88–92
141. AlJahdali H, Albatli A, Garraghan P, Townend P, Lau L, Xu J (2014) Multitenancy in cloud computing. In: Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium On. IEEE. pp 344–351
142. Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13(2):113–170
143. Chung CJ, Xing T, Huang D, Medhi D, Trivedi K (2015) Serene: on establishing secure and resilient networking services for an sdn-based multi-tenant datacenter environment. In: Dependable Systems and Networks Workshops (DSN-W), 2015 IEEE International Conference On.IEEE. pp 4–11
144. Wood T, Cecchet E, Ramakrishnan KK, Shenoy PJ, van der Merwe JE,Venkataramani A (2010) Disaster recovery as a cloud service: Economic benefits & deployment challenges. HotCloud 10:8–15

145. DuBois L, Amatruda R (2010) Backup and recovery: Accelerating efficiency and driving down it costs using data deduplication. EMC Corporation
146. Suguna S, Suhasini A (2014) Overview of data backup and disaster recovery in cloud. In: Information Communication and Embedded Systems (ICICES), 2014 International Conference On. IEEE. pp 1–7
147. Son Y, Choi J, Jeon J, Min C, Kim S, Yeom HY, Han H (2017) Ssd-assisted backup and recovery for database systems. In: Data Engineering (ICDE), 2017 IEEE 33rd International Conference On. IEEE. pp 285–296
148. Zeng L, Xu S, Wang Y (2016) Vmbackup: an efficient framework for online virtual machine image backup and recovery. Concurrency Comput Pract Experience 28(9):2630–2643
149. Barber C, Hanser T, Judson P, Williams R (2017) Distinguishing between expert and statistical systems for application under IC H M7. Regulatory Toxicol Pharmacol 84:124–130
150. Dr.M.Sheshikala,SallauddinMohmmad, Shabana,"Survey on Multi Level Security for IoT Network in cloud and Data Centers",Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 10-Special Issue, 2018, pp. (134-146).
151. G. Sunil ,Sallauddin Mohmmad ,Kanegonda Ravi Chythanya "The Current Status and Research in Industrial Big Data analysis in Smart Intelligent Systems", International Journal of Advanced Research in Computer Science, Volume 8, No. 8,pp.603-609, September-October 2017.
152. SallauddinMohmmad,Dr.M.Sheshikala, Shabana,"Software Defined Security (SDSec):Reliable centralized security system to decentralized applications in SDN and their challenges",Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 10-Special Issue, 2018, pp. (147-152).
153. Komuravelly Sudheer Kumar, K Ravi Chythanya, N Vijay Kumar, Vahini Siruvoru, "An Enhanced Distributed Accountability for Data Sharing in the Cloud Computing Technologies:, IJET Nov 2018 "International Journal of Engineering & Technology", Vol.7, No. 1.8; Page No.233-235
154. J. Bhavana, Komuravelly Sudheer Kumar: "A Study on the Enhanced Approach of Data Mining Towards Providing Security for Cloud Computing", Indian Journal of Public Health Research & Development, November 2018, Vol.9, No. 11; Page No. 1176-1179.