Khan *et al. Journal of Cloud Computing: Advances, Systems and Applications* (2017) 6:19
DOI 10.1186/s13677-017-0090-3

Journal of Cloud Computing:
Advances, Systems and Applications

REVIEW Open Access

Fog computing security: a review of current applications and security solutions

Saad Khan*†, Simon Parkinson† and Yongrui Qin

Abstract

Fog computing is a new paradigm that extends the Cloud platform model by providing computing resources on the edges of a network. It can be described as a cloud-like platform having similar data, computation, storage and application services, but is fundamentally different in that it is decentralized. In addition, Fog systems are capable of processing large amounts of data locally, operate on-premise, are fully portable, and can be installed on heterogeneous hardware. These features make the Fog platform highly suitable for time and location-sensitive applications. For example, Internet of Things (IoT) devices are required to quickly process a large amount of data. This wide range of functionality driven applications intensifies many security issues regarding data, virtualization, segregation, network, malware and monitoring. This paper surveys existing literature on Fog computing applications to identify common security gaps. Similar technologies like Edge computing, Cloudlets and Micro-data centres have also been included to provide a holistic review process. The majority of Fog applications are motivated by the desire for functionality and end-user requirements, while the security aspects are often ignored or considered as an afterthought. This paper also determines the impact of those security issues and possible solutions, providing future security-relevant directions to those responsible for designing, developing, and maintaining Fog systems.

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

Introduction

Fog computing is a decentralized computing architecture whereby data is processed and stored between the source of origin and a cloud infrastructure. This results in the minimisation of data transmission overheads, and subsequently, improves the performance of computing in Cloud platforms by reducing the requirement to process and store large volumes of superfluous data. The Fog computing paradigm is largely motivated by a continuous increase in Internet of Things (IoT) devices, where an ever increasing amount of data (with respect to volume, variety, and velocity [1]) is generated from an ever-expanding array of devices.

IoT devices provide rich functionality, such as connectivity, and the development of new functionality is often data motivated. These devices need computing resources to process the acquired data; however, fast decision processes are also required to maintain a high-level of functionality. This can present scalability and reliability issues when utilising a standard client-server architecture, where data is sensed by the client and processed by the server. If a server was to become overloaded in a traditional client-server architecture, then many devices could be rendered unusable. The Fog paradigm aims to provide a scalable decentralised solution for this issue. This is achieved by creating a new hierarchically distributed and local platform between the Cloud system and end-user devices [2], as shown in Fig. 1. This platform is capable of filtering, aggregating, processing, analysing and transmitting data, and will result in saving time and communication resources. This new paradigm is named *Fog computing*, initially and formally introduced by Cisco [3].

Cloud computing provides many benefits to individuals and organizations through offering highly available and efficient computing resources with an affordable price [4]. Many cloud services are available in current commercial solutions, but they are not suitable for latency, portability

*Correspondence: saad.khan@hud.ac.uk
†Equal contributors
Department of Informatics, School of Computing and Engineering, University of Huddersfield, Queensgate, Huddersfield, UK

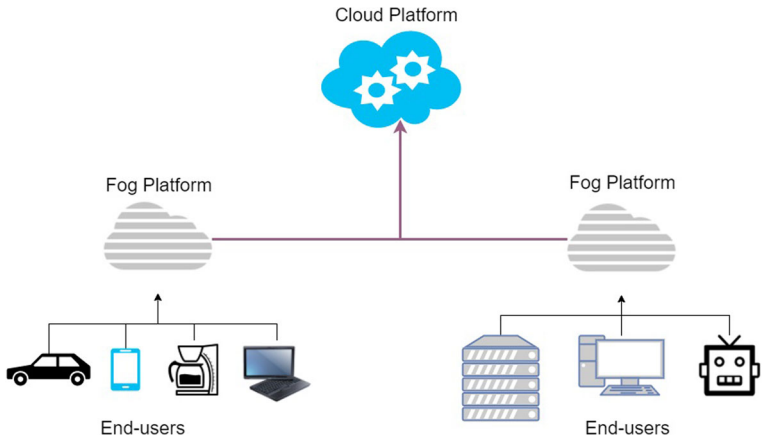

Fig. 1 Fog computing by Cisco. This figure shows how diverse set of devices can communicate with the Cloud using Fog computing

and location-sensitive applications, such as IoT, Wearable computing, Smart Grids, Connected Vehicles [5] and Software-Defined-Networks [6]. Latency depends on the speed of Internet connection, resource contention among guest virtual machines (VM) and has been shown to increase with distance [7]. Furthermore, such applications generate large volumes of varied data in a high velocity, and by the time data reaches a cloud system for analysis, the chance to inform the IoT device to take reactive action may be gone. For example, consider IoT devices in the medical domain where the latency of acting on the sensed data could 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 aforementioned issues. According to [8], a Fog system has the following characteristics:

- It will be located at the edge of network with rich and heterogeneous end-user support;
- Provides support to a broad range of industrial applications due to instant response capability;
- It has its own computing, storage, and networking services;
- It will operate locally (single hop from device to Fog node);
- It is highly a virtualized platform; and
- Offers inexpensive, flexible and portable deployment in terms of both hardware and software.

Besides having these characteristics, a Fog system is different from Cloud computing in various aspects and poses its own advantages and disadvantages. Some of the more prominent are detailed in the below list [9–11]:

- A Fog system will have relatively small computing resources (memory, processing and storage) when compared to a Cloud system, but the resources can be increased on-demand;
- They are able to process data generated from a diverse set of devices;
- They can be both dense and sparsely distributed based on geographical location;
- They support Machine-to-Machine communication and wireless connectivity;
- It is possible for a Fog system to be installed on low specification devices like switches and IP cameras; and
- One of their main uses is currently for mobile and portable devices.

Like Cloud systems, a Fog system is composed of Infrastructure, Platform, and Software-as-a-Service (IaaS, PaaS, and SaaS, respectively), along with the addition of Data services [12, 13]. The technical architecture of a Fog platform [14] is shown in Fig. 2. The Fog IaaS platform is created using Cisco IOx API, which includes a Linux and CISCO IOS networking operating system. Any device, such as switches, routers, servers and even cameras can become a Fog node that have computing, storage, and network connectivity. Fog nodes collaborate among themselves with either a Peer-to-Peer network, Master-Slave architecture or by forming a Cluster. The Cisco IOx APIs enable Fog applications to communicate with IoT devices and Cloud systems by any user-defined protocol. For developing Fog applications in PaaS environment, Cisco DSX is used to create a bridge between SaaS (which actually offers Metal-as-a-Service) and many types of IoT devices. It provides simplified management of applications, automates policy enforcement and supports multiple development environments and programming languages. The data service decides the suitable place (Cloud or Fog) for data analysis, identifies which data

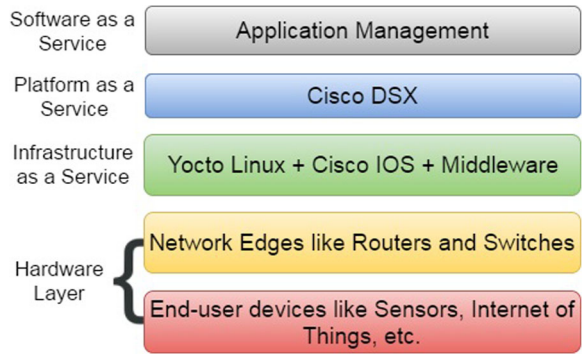

Fig. 2 Technical architecture of Cisco's Fog Computing Platform. This figure shows all components from hardware to application layer

requires action and increases security by making data anonymous.

Many researchers and commercial infrastructure developers believe that Fog platforms will be developed and released in the future to provide an enriched and more reliable infrastructure to handle the ever increasing expansion of connected computational devices. However, as with all distributed systems, the exposure to cyber threats is also prevalent and often heightened by the developer's desire to provide functional systems first, and then add-in security measures afterwards. Many researchers are adopting a *security-centric* or *secure by design* [15] philosophy for producing such distributed systems. But this viewpoint is still in its infancy and lacks in comprehensive understanding of the security threats and challenges facing a Fog infrastructure. This paper provides a systematic review of Fog platform applications, determines their possible security gaps, analyses existing security solutions and then put forwards a list of comprehensive security solutions that can eliminate many potential security flaws of Fog systems. The literature used in this paper is gathered using the *Google Scholar* search engine. The keywords used to find the literature are *"Fog computing"*, *"Fog computing applications"*, *"Fog computing security"*, *"Fog security issues"* and *"Fog security"*. The time frame of selected papers is up to June, 2017. To best of our knowledge, we reviewed all papers which were displayed in the search engine at that time. In addition to that, we broadened the survey by including several relevant research areas as Fog computing is still in its infancy stage. Other search terms were also used to search closely related developments subject areas. These include *"edge computing"*, *"cloudlet"*, *"micro data 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 also discusses the potential security threats that have not been acknowledged. Following this, a summary is provided to classify common shortcomings and to highlight their significance. We also provide a discussion of potential mitigation mechanisms. Finally, we conclude by providing a discussion of the identified shortcomings, motivating future research.

Related work - current fog applications

Review methodology

The Cisco Fog paradigm can be viewed in a broad and integrative manner as an enabler of many advanced technologies. It can encompass, proliferate and impact several enhanced features such as rapid analysis, interoperability among devices, increased response time, centralized or machine-to-machine management, low bandwidth consumption, efficient power consumption, device abstraction and many others. Similar approaches like Fog computing have now been taken to increase the usability and potential of Cloud platform [16]. With the advent of such wide applicability, the Fog and its similar platforms like Edge computing, Cloudlets and Micro-data centres are prone to attacks that can compromise Confidentiality, Integrity, and Availability (CIA) [17].

Cloud Security Alliance [18] have identified twelve critical security issues, including other researchers such as [6, 19, 20]. These issues directly impact distributed, shared and on-demand nature of cloud computing. Being a virtualised environment like Cloud, Fog platform can also be affected by the same threats (see Fig. 3). Our study considers following twelve security categories to formulate a systematic review:

1. **Advance Persistent Threats (APT)** are cyber attacks whereby the aim is to compromise a

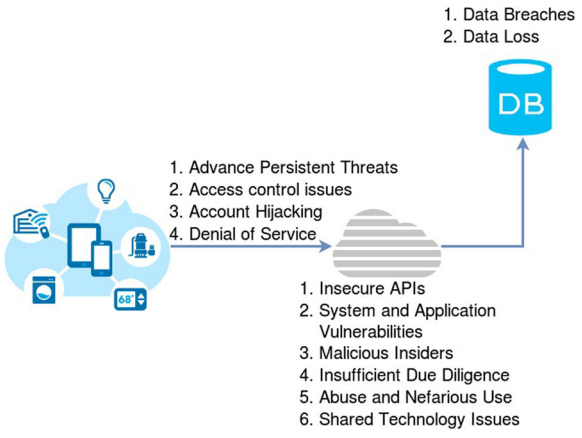

Fig. 3 Potential security issues of Fog Platform inherited from Cloud computing. This figure shows how virtualisation and other issues of Cloud platform can effect Fog platform as well

company's infrastructure with the desire to steal data and intellectual property.
2. **Access Control Issues (ACI)** can result in poor management and any unauthorised user being able to acquire data and permissions to install software and change configurations.
3. **Account Hijacking (AH)** is where an attack aims to hijack the user accounts for malicious purpose. Phishing is a potential technique for account hijacking.
4. **Denial of Service (DoS)** are where legitimate users are prevented from using a system (data and applications) by overwhelming a system's finite resources.
5. **Data Breaches (DB)** are when sensitive, protected or confidential data is released or stolen by an attacker.
6. **Data Loss (DL)** is where data is accidentally (or maliciously) deleted from the system. This does not have to be resulting from a cyber attack and can arise through natural disaster.
7. **Insecure APIs (IA)** Many Cloud/Fog providers expose Application Programming Interfaces (APIs) for customer use. The security of these APIs is pivotal to the security of any implemented applications.
8. **System and Application Vulnerabilities (SAV)** are exploitable bugs arising from software ad configuration errors that an attacker can use to infiltrate and compromise a system.
9. **Malicious Insider (MI)** is a user who has authorised access to the network and system, but has intentionally decided to act maliciously.
10. **Insufficient Due Diligence (IDD)** often arises when an organisation rushed the adoption, design, and implementation of any system.
11. **Abuse and Nefarious Use (ANU)** often arises when resources are made available for free and malicious users utilise said resources to undertake malicious activity.
12. **Shared Technology Issues (STI)** occur due to sharing infrastructures, platforms or applications. For example, underlying hardware components may not have been designed to offer strong isolation properties.

The following section reviews a wide-range of Fog applications, paying particular attention to their potential security implications. As the Fog computing is still in its infancy stage, similar technologies have also been discussed to make the survey more holistic and beneficial. The Fog systems reviewed by analysing publicly available literature have been grouped into the below subsections. Throughout this section, the twelve categories illustrated in Fig. 3 are considered and a condensed summary is provided in Table 2.

Fog computing and similar technologies

Although the term Fog computing was first coined by Cisco, similar concepts have been researched and developed by various 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 using Programmable Automation Controllers (PAC) [23], which can handle data processing, storage and communication [22]. It poses a advantage over Fog computing as it reduces the points of failure and makes each device more independent. However, the same feature makes it difficult to manage and accumulate data in large scale networks such as IoT [24].
2. **Cloudlet** is a middle part of 3-tier hierarchy "mobile device - cloudlet - cloud". There are four major attributes of Cloudlet: entirely self-managing, possesses enough compute power, low end-to-end latency and builds on standard Cloud technology [25]. Cloudlet differs from Fog computing as application virtualization is not suitable for the environment, consumes more resources and cannot work in offline mode as indicated by [26, 27].
3. **Micro-data centre** [28] is a small and fully functional data centre containing multiple servers and is capable of provisioning many virtual machines. Many technologies, including Fog computing, can benefit from Micro data centres as it reduces latency, enhances reliability, relatively portable, has built-in security protocols, saves bandwidth consumption by compression and can accommodate many new services.

Software defined and virtualized radio access networks

Fog computing can enable users to take full control and management of the network by providing Network Level Virtualization (NLV) and real-time data services. *OpenPipe* [29] utilises Fog computing to implement NLV through a hybrid model, which consists of virtual Software Defined Network (SDN) controller (located in Cloud), virtual local controllers (located in Fog), virtual radio resources (for wireless communication) and virtual cloud server. The SDN controller is a global and intelligent module, which manages the entire network. Local controllers forward data to an SDN controller, which fulfils the demand of real-time and latency-sensitive applications by deciding whether to process data on local or SDN controller, based on user policies. The Extended OpenFlow (exOF) protocol is used to connect SDN and local controllers. The benefits of proposed system include load balancing, handover event without compromising Quality

of Service (QoS), low energy consumption, and reduced latency and low network overhead. In addition, Fog nodes can compress and reorganize the web objects for optimal speed. In addition, various compelling research studies [30–32] have been presented for improving the performance of SDN and virtual machines by making use of cloudlets, which are able to perform dynamic VM synthesis, single-hop low-latency wireless access and creates the VM overlays to only load the difference of desired custom VM and its base VM. These features have been implemented by Carnegie Mellon University in a project called *Elijah* and is available on *Github* repository [33].

The use of highly virtualized environment results in a large number of shared technology security issues. For example, an insecure hypervisor can be exploited to bring down the entire Fog platform as it is a single point of failure and manages all the Virtual Machines [34]. The virtualization issues include weak tenant segregation allowing one malicious user or attacker to compromise other users' account and data, side-channel attacks [35], targeted APTs and illegal privilege escalation to gain unauthorized data or resource access. The risks associated with shared technology are critical because it takes a minor vulnerability or misconfiguration to damage all Fog services, user operations and allows attackers to gain access to exploit Fog resources. Some of the recommended solutions to eliminate virtualization-based attacks are multi-factor or mutual authentication, Host and Network Intrusion Detection System, user-based permissions model, private networks and process/data isolation [36].

Web optimization

Researchers from Cisco are utilising Fog computing to increase the performance of websites [37]. Instead of making a round trip for every HTTP request for content, style sheets, redirections, scripts and images, Fog nodes can help in fetching, combining and executing them at once. In addition, fog nodes can distinguish users based on MAC addresses or cookies, track user requests, cache files, determine local network condition. It is also possible to embed feedback scripts inside web page to measure the user browser's rendering speed. The feedback script reports directly to the Fog nodes and informs about the user's graphical resolution, current area reception (if wireless) and network congestion. In another similar paper, Fog computing significantly reduced the response time of a Cloud-based temperature prediction system [38]. Due to Fog systems, the prediction latency was decreased from 5 to 1.5 s, web-page display latency from 8 to 3 s and internet traffic throughput from 75 to 10 Kbps. Another related use of Fog computing is discussed in [39], wherein the Internet of Everything (IoE), IP addresses can be replaced with names, using Information Centric Networking (ICN) framework by enhanced cache mechanisms. Fog nodes are able to manage cache (e.g. using Steiner Tree Based Optimal Resource Caching Scheme for Fog computing [40]), with the added benefit of supporting heterogeneous devices and computing, processing and storing on the edges of the network. Another simple approach [41] would be to use Edge computing for generating user-specific pages by replicating the application code at multiple edge servers. The edge servers are capable of keeping numerous copies of data, perform content-aware data caching and content-blind data caching.

Using Fog platform for optimising web-services will also introduce web security issues. For example, if user input is not properly validated, the application becomes vulnerable to the code injection attacks, such as SQL injection, where SQL code provided by the user is automatically executed resulting in the potential for unauthorised data access and modification. This could result in the compromise of entire Fog system's database or the forwarding of modified information to a central server [42]. Similarly, due to insecure web APIs, attacks like session and cookie hijacking (posing as a legitimate user), insecure direct object references for illegal data access, malicious redirections and drive-by attacks [43] could force a Fog platform to expose itself and the attached users. Web attacks can also be used for targeting other applications in the same Fog platform by embedding malicious scripts (cross-site scripting) and potentially damage sensitive information. A potential mitigation mechanism is to secure the application code, patch vulnerabilities, conduct periodic auditing, harden the firewall by defining ingress and egress traffic rules and add anti-malware protection.

Provisioning 5G mobile networks

Mobile applications have become an integral part of modern life and their intensive use has led to an exponential growth in the consumption of mobile data, and hence the requirement for 5G mobile networks. Fog computing can not only provide a 5G network with better service quality, but they can also help in predicting the future need of mobile users [44]. Inherently, Fog nodes are distributed within the proximity of users; a characteristic that reduces latency and establishes adjacent localized connections. Broadly speaking, the diverse and multiple topological and mesh network connections among Mobile network, Fog nodes, and Cloud platform make Fog system beneficial for 5G technology, NLV and SDN [45]. Fog computing is also able to handled load balancing issues of a 5G network [46]. When many users are simultaneously requesting computation in a large-scale network, creating small cells of Fog nodes based on the size of requested task and system parameters can improve load balancing. This joint optimisation of multiple users can improve the Quality of Experience (QoE) and network performance by 90% of up

to 4 users per small cell. Edge computing is also being used for reducing network latency, ensuring highly efficient service delivery and offering an improved user experience by utilising programmable nature of NLV and SDN [47].

Without properly securing the virtualised infrastructure of Fog nodes in a 5G network, providers risk not being able to achieve the desired performance. A single compromised Fog node in the 5G mobile network can generate the potential entry point for a Man-in-the-Middle (MITM) attack and interrupt all connected users, leak data, abuse the service by exceeding the limit of data plan and damage sibling Fog nodes. A MITM attack can be launched by a malicious internal user and can exploit the Fog platform by sniffing, hijacking, injecting and filtering data incoming from the end-user [48]. This will consequently affect the data communication of the underlying network (E.g. the 5G network). The most common way of eliminating such issues is to encrypt communication with either symmetric or asymmetric algorithms, mutual authentication, using the OAuth2 protocol, and ensuring the isolation of compromised nodes and certificate pinning as discussed by [49].

Improving throughput for smart meters

By deploying Smart Grids, large amounts of data is collected, processed and transmitted from smart meters using data aggregation units (DAU). Meter data management system (MDMS) use the generated data to forecast future energy demands. According to [50], the data aggregation process takes a long time due to the low bandwidth capacity of hardware, but can be improved with the help of Fog computing. First, a Fog-based router is connected with smart meters that accumulate the data reading of all sub-meters within a pre-defined time. Secondly, all values are transmitted to a second Fog platform, which performs data reduction processes. This Fog-based approach was tested on a general purpose Cisco routers and IOx, which are able to distinguished between Fog and non-Fog network packets. This method creates Advanced Metering Infrastructure (AMI) that can reduce the amount of communication data and overheads within the network, resulting in an improvement in response time. A similar architecture is created in [51] for AMI, where Fog computing helped in reducing latency, delay jitter and distance while improving location awareness and mobility support.

Although sophisticated database software and high storage capacity hardware are used for aggregation and processing, data can easily be replicated, shared, modified and deleted by any malicious intermediate or fake external node using a Sybil (forging identities) attack, which can undermine the CIA of data [52]. In addition, it is difficult for a Fog platform to centrally define, set and maintain access control attributes of user ownership in a large amount of moving data. Fog nodes are continuously processing, analysing and accumulating data to produce information and it becomes difficult to retain data integrity and prevent data loss. The tolerance at which a failure occurs is also very low as the exact point of error is hard to identify in a system. To eliminate these issues, security policies and strategies should be integrated into Fog systems to track energy consumption information along with contingency plans and disaster recovery modules [53, 54].

Improving healthcare systems and their performance

Fog computing is also applied in healthcare and elderly care systems, where self-powered wireless sensors transmit data to Fog nodes, as a pose to sending them directly the Cloud. Using a large number of sensors, it is possible to create a smart healthcare infrastructure, where semantic tagging and classification of data is performed in the Fog layer, providing the refined data to a Cloud system for further processing [55]. Another system uses a similar approach and integrates a Fog-computing-informed paradigm within a Cloud for medical devices, providing a good Quality of Service (QoS) and governance [56]. Both architectures are in the context of the OpSIT healthcare project in Germany. With the help of Fog computing, healthcare systems provide services from a nearby location, store heterogeneous data, consists of smart low power devices, and are able to switch among various communication protocols as well as facilitating distributed computing [57]. Another application of Fog computing in healthcare includes Electrocardiogram (ECG) feature extraction to diagnose cardiac diseases [58]. This involves medical sensors transmitting data to a Fog layer that stores data in distributed databases, extract ECG features, and providing a graphical interface to display results in real-time. The proposed system is highly portable and results indicate a 90% increase in bandwidth efficiency over current solutions. The detection of a person having a stroke is of key importance as the speed of medical intervention is life critical. Two fall detection systems have been implemented using Fog platform, named U-FALL [59] and FAST [60]. Both systems distribute computational tasks between Fog and Cloud platforms to provide an efficient and scalable solution, which is essential as it allows for a quick detection and notification of a patient fall.

Patient health records contain sensitive data and there are multiple points in any Fog platform where they can be compromised, such as by exploiting any system and application vulnerability, unauthorised data access while in storage or during transmission, malicious insiders threat and while sharing data with other systems [61]. Medical sensors are continuously transmitting data to Fog platforms, through either wired or wireless connection.

It is quite possible to compromise patient privacy, data integrity and system availability by exploiting sensors and their underlying communication network. Wireless sensors usually work in open, unattended and hostile environments. This ease-of-access has the potential to increase the chances of attacks like DoS, report disruption, and selective forwarding attacks [62]. In addition, if the Fog node manages sensitive data and lacks access control mechanisms, it might leak the data due to account hijacking, unintended access, and other vulnerable points of entry. To avoid such issues, strict policies should be enforced to maintain a high-level of control using multi-factor or mutual authentication, private networks and partial (selective) encryption.

Surveillance video stream processing

Fog computing can play an important role, where the efficient processing and instantaneous decision-making is required. Take an example of tracking multiple targets in a drone video stream as stated in [63]. Instead of sending live video feeds to a Cloud-based application, it is directed towards the nearest Fog node. Any mobile device such as tablets, smart-phones and laptop can become Fog node, run tracking algorithms and process raw video stream frames, hence removing the latency of transmitting data from the surveillance area to the Cloud. Results show that the addition of a Fog platform reduced an average of 13% of total processing time. The surveillance video processing can also be performed by using Edge computing and its potential in finding missing children [64]. Pushing video feeds of every camera sensor directly to the Cloud is not possible, but with the help of distributed edge servers and their processing power, each video can be processed individually and the Cloud system can gather the final results to yield a much faster output. Proximal algorithm [65] can also be implemented in the Fog nodes of a large-scale video streaming service, and can resolve joint resource allocation issue.

A video data stream generated by a camera sensors is sent to the respective Fog nodes, where it is stored and processed. The privacy of the stream should be maintained as it contains audio and visual data, which are transmitted to heterogeneous clients. Here, not only is the security of Fog node is important, but the network and all end-user devices involved in the transmission should also be considered, especially against APTs. If a Fog platform or network contains any bugs due to lack of diligence, the crucial video stream might be viewed, altered and even destroyed. It is important that Fog node ensures a secure connection between all communicating devices and protect multi-media content by obfuscation techniques, fine-grained access control, generating a new link for video stream, selective encryption and limiting the number of connections [66].

Vehicular networks and road safety

A new Vehicular Adhoc Networks (VANET) architecture has been proposed using Fog computing, called Fog-based Software Defined Network (FSDN) VANET [67]. The components of FSDN are SDN Controller (SDNC), SDN Wireless Nodes (vehicles), SDN Road-Side-Unit (Fog device), SDN Road-Side-Unit Controller (RSUC) and Cellular Base Station (BS). SDNC controls entire network along with Fog Orchestration and Resource Management for the Fog. RSUC is a group of Fog devices that performs data forwarding operations. BS also delivers Fog services and operates under the control of SDNC. Fog nodes and other devices communicate in the form of policy rules and content. SDNC receives vehicle information from BSs and transportation information from RSUs. Fog enabled BSs and RSUs making it possible to provide faster services without contacting SDNC. Other similar implementations have been proposed in [6, 68], where either Fog devices are connected centrally with SDNC and Cloud or interconnected with each other in a Machine-to-Machine manner. To increase road safety, a Fog-based intelligent decision support driving rule violation monitoring system [69] has also been developed. The proposed system has three layers: lower, middle and upper. The lower layer is able to detect hand-held devices during driving and vehicle number using camera sensors, and send the information to nearest Fog server. In the middle layer, Fog server confirms if driver is intentionally violating the rules and communicates the vehicle identifier information to Cloud server. Finally, in upper the layer, Cloud server issues a traffic violation decision and alert the relevant authorities.

The security issues of Fog platforms in vehicular and road networks are similar to those associated with 5G mobile networks in terms of issues resulting from shared technology. Furthermore, vehicular networks do not have fixed infrastructure, and due to the volume of connections, there are multiple routes between the same nodes. Such networks are exposed to potential DoS and data leak attacks due to a lack of centralized authority [70]. DoS attacks on a Fog platform, either from end-users or external systems, can prevent legitimate service use as the network becomes saturated. In addition, all communication is wireless and hence susceptible to impersonation, message replay, and message distortion issues [71]. Protection from these attacks is significant as human life is involved. The most common way of eliminating such issues is by implementing strong authentication, encrypted communication, key management service, perform regular auditing, and implement private network and secure routing.

Intelligent food traceability

Fog computing is also being used as a solution for food traceability management, where the aim is to remove poor

quality products from the supply chain using value-based processing [72]. A food item can be physically traced using various attributes, such as location, processing and transportation devices. The quality of a food item is determined by distributed food traceability through Cyber Physical System (CPS), which makes decisions based on Fuzzy rules. Both food traceability and quality information is sent to the Fog network, where the entire food supply chain is traceable. At this point, the Fog network holds complete information about all tracked food items and subsequently transmits food quality information to the Cloud system which can be viewed by stakeholders using the Internet.

The attackers could obstruct supply chain operations by exploiting location and transportation processes of this system. If a Fog node is compromised by means such as account hijacking or exploiting system and application vulnerabilities, the data can be falsified, which could ultimately result in the sale of substandard and low-quality food products. A network containing a large number of wireless sensors, and Machine-to-Machine (M2M) communications instigates a broad range of security concerns. One such example is resonance attack, where sensors are forced to operate at different frequencies and transmit incorrect data to a Fog node. This attack impacts the real-time availability of network and data, along with tolerance level [73]. Such systems should be protected by integrity checks, detecting deception attacks, redundancy to prevent single-point 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, records and processes speech data from patients with Parkinson's disease. Instead of transmitting the entire audio data, FIT extracts features like volume, short-time energy, zero-crossing rate and spectral centroid from speech and sends to the Cloud for long-term analysis. The application was tested on six patients and Fog computing made it possible to remotely process large-amount of audio data in a reduced duration. Another work extends the features of Mobile Edge Computing (MEC) into a novel programming model and framework [75] allowing mobile application developers to design flexible and scalable edge-based mobile applications. The developer can benefit from the presented work as the framework is capable of processing data before its transmission and considers geo-distribution data for latency-sensitive applications.

Smartphones and tablets host large amount applications and can result in many complexities in terms of quality and security. Each applications has to legitimate access to user's private data (often granted by the user during installation), which has been identified as the driving force in many cyber attacks [76]. Fog platforms that are configured and executing on a mobile operating system should be protected, especially in case of open-source platforms, as one malicious application can compromise Fog operations and the connected network along with user's personal data [77]. Malware-based attacks can potentially corrupt and damage the CIA of data and communication. A recent survey identified that there are many potential security solutions, such as anti-virus, firewall, Intrusion Prevention System, constant data backups, software patching, and frequently creating system restore points and performing behaviour analysis techniques through dynamic monitoring [78].

Augmented brain computer interaction

A real-time brain state detection system has been implemented using a multi-tier Fog computing infrastructure [79]. The Fog platform is the data hub and signal processor that receives and processes data streams generated by electroencephalogram (EEG) headset and motion sensors. The Fog server extracts time-frequency characteristics from signals and dispatches them to the brain state classifiers. The benefits of the proposed system are demonstrated through playing a multi-player online game called EEG Tractor Beam. Another similar system is developed in [80], where a multi-tiered Fog and Cloud system, linked data, and classification models have been used for EEG-based Brain-computer interfaces (BCI). The Fog servers are used for real-time data processing, caching, computation off-loading, managing heterogeneity and forwarding data from mobile devices and sensors to the Cloud system. Fog computing also have many potential applications in telehealth systems [81], which can perform quick mining and perform analysis on a raw data stream gathered from different wearable sensors. Fog nodes compress data and are physically located nearby, aiding to reduce bandwidth and power consumption.

The CIA of every data stream should be ensured regardless of whether it is generated from a camera or EEG sensor. Essentially, every Fog system should consider appropriate user access controls, data encryption and Transport layer security (TLS) protocol [82] to secure data access, privacy, and transmission. If any sensor device, Fog node, network or even all are compromised by attacker due to some vulnerability or lack of diligence, the original data will remain disclosed. Currently, brain signals acquired by an EEG sensor are used to play games, which do not require high security. However, for future sensitive applications, it is vital to implement encryption algorithms such as Elliptic curve cryptography to protect against Advance Persistent Threats (APTs) and data loss threats.

Managing resources in micro data-centres

Apart from enabling advanced technologies, Fog computing can perform many system-level tasks such as computation resource management, prediction, estimation and reservation. It can also perform data filtration based on policy, pre-processing and enhance security measures. A similar framework has been provided by [83] for IoT devices resource management in micro data-centres. It consists of six layers:

- Physical, virtual 'Things' and wireless sensors;
- Activity, power, response and service monitoring;
- Pre-processing data by analysis, filtering, reconstruction and trimming;
- Storing, distributing, replicating and de-duplicating data;
- Providing security by encryption/decryption and integrity checks; and
- Transporting pre-processed data to the cloud.

The framework also contains a resource estimation and pricing model for new IoT customers. Another article [84] suggests that Fog computing can enable dynamic real-time analysis, integrated security, reliability and fault tolerance. The Fog platform is highly flexible and scalable as processing nodes (mobile devices) can frequently join and leave a network. This property also allows the support for more programming models and diverse system architectures to quickly manage substantial data.

Fog platforms that are used for the managing computation resources of other systems are highly prone to shared technology issues (discussed in "Software defined and virtualized radio access networks" section). Another critical threat is that of the malicious insider, who can violate access control on user-to-user, user-to-administrator, administrator-to-user and administrator-to-administrator levels. As virtualized environment are loaded into memory, it can also be exploited by resource abuse (privilege escalation and escaping attacks), account hijacking (exploiting authentication protocols or social engineering) and DoS attacks due to large number of users requesting resources use at the same time. Such attacks could result from inefficient and insufficient resource policies as well as a lack of user activity monitoring. In this case, identity-based encryption algorithms [85] and Role-Based Access Control model, as suggested by NIST [86], can be implemented to increase security.

Saving energy in Cloud computing

As Cloud operations require large amount of continuous energy, different types of applications are investigated in [87] using Raspberry Pi based servers, which can be installed and configured as a Fog platform to reduce energy consumption. According to the results, applications that continuously produce static data within end-user premises and have low connection rate (e.g. video surveillance), can save significant energy using Fog computing. The authors also claim that the consumption of energy mostly depends on the amount of idle time, number of downloads, updates and data pre-loading, whereas actual content and number of network hops among users do not have vital impact. Another study [88] provides a systematic framework for creating a complete infrastructure consisting of a Cloud platform, Wide Area Network (WAN), Fog platforms and Local Area Network (LAN) in an optimal manner. They also designed a numerical model to prove that Fog computing significantly improves the performance of cloud computing by trading power consumption-delay with workload allocation. Similarly, to reduce the energy consumption in mobile-phones, researchers used used *call graph* to offload computation to edge servers by optimally managing and allocating communication resources [89].

This particular application encourages the use of Fog platforms in storing and processing specific (user-defined) kinds of the (private) data locally in the Fog nodes, reducing the communication cost and delay. However, the presence of such private data puts the Fog platform in a sensitive position. As previously mentioned there are many threats, which are capable of compromising CIA of data such as malicious insiders can read, alter and delete data. These issues can be resolved through the use of encryption, authentication (uniquely validating and verifying each user), data classification based on sensitivity, monitoring and data masking [90].

Disaster response and hostile environments

Fog computing can aid human search and rescue operations conducted over large geographical area in the occurrence of natural disaster [91]. Heterogeneous Commodity-Off-The-Shelf (COTS) Fog devices with low power consumption with wireless support are used in the implementation of the system. Different Quality of Service (QoS) metrics such as energy consumption, mobility, localization, optimal path calculation, data distribution among Fog devices and performance are measured in the simulated post-disaster model to evaluate the system. Similar work suggests that *VM-based Cloudlets* [92] and *tactical Cloudlets* [93] can offer significant benefits in hostile environment (e.g. military operations) as they are deployed in close proximity and can be placed inside vehicles for portability, ensuring continuous service, perform data filtering, reduces information leakage and support heterogeneous devices.

Disaster recovery is a sensitive area whereby Fog systems and connected devices are supposed to work in extreme circumstances. In this case, the integrity and availability of the system are more important than

confidentiality. Wireless security protocols can carry out checksum (detect data errors), encrypt packets with minimal resources [94] and provision fine-grained access control to strictly validate users (terminating unwanted connections). Furthermore, in case of emergency and key management to prevent losing decryption keys, these mechanisms should be considered to retain availability and integrity without compromising the overall performance of system.

Summary of security issues

Table 1 presents the relationship of the surveyed Fog application areas and the categories of security issues. A description of each category can be found in "Review methodology" section. Although the table has been populated based upon interpreting published literature, it should be noted that in some cases it is possible that the authors may not have communicated specifics of their application which mitigate a potential security threat category. The table identifies that none of the surveyed application areas have taken the necessary precautions to minimise the potential impact and risk of each category of security threat.

Table 2 provides a summary of security controls in respect to each application area. This table highlighting the potential impact on Fog platforms with respect of CIA model. The development of security measures in Fog systems is rapidly progressing, and some of the current publications do not contain sufficient detail to provide a thorough evaluation. This results in some of the knowledge gaps being speculative and futuristic and based on the latest research activity. It is important to note that due to continuous increase in attack vectors, it is not an exhaustive list and some security issues may have been missed. With the advancement in Fog infrastructure development, new security issues will need to be identified and acknowledged.

Existing security solutions for Fog computing

As determined in the above sections, the introduction of Fog platform functionality between end-users and the Cloud systems creates a new point for vulnerabilities, which can potentially be exploited for malicious activities. Unlike for Cloud systems, there are no standard security certifications and measures defined for the Fog computing. In addition, it could also be stated that a Fog platform:

- Has relatively smaller computing resources due to their very nature and hence it would be difficult to execute a full suite of security solutions that are able to detect and prevent sophisticated, targeted and distributed attacks;
- Is an attractive target for cyber-criminals due to high volumes of data throughput and the likelihood of being able to acquire sensitive data from both Cloud and IoT devices; and
- Is more accessible in comparison with Cloud systems, depending on the network configuration and physical location, which increases the probability of an attack occurring.

The real-world applications of Fog computing and similar technologies, which are surveyed in "Related work - current fog applications" section, are mostly motivated by functionality. However, it has also been identified that in most cases potential security measures against that can be implemented to mitigate threats are ignored. A potential

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

Application area	APT	ACI	AH	DoS	DB	DL	IA	SAV	MI	IDD	ANU	STI
Virtualised radio access	✓	✓	✓		✓			✓	✓		✓	✓
Web optimization			✓			✓	✓					
5G mobile networks					✓	✓			✓		✓	✓
Smart Meters		✓				✓			✓			
Healthcare systems		✓	✓	✓	✓		✓	✓	✓			
Surveillance Video processing	✓				✓					✓		
Vehicular networks and Road safety				✓	✓							✓
Food traceability			✓			✓		✓				
Speech data						✓			✓			
Augmented Brain Computer	✓	✓			✓					✓		
Managing resources		✓	✓	✓					✓	✓	✓	✓
Energy reduction					✓	✓						
Disaster Response and Hostile environment		✓		✓						✓		

Table 2 Summary of potential security issues found in Fog applications

Attack category	Possible threats	Possible solutions	Impact
Virtualization issues	Hypervisor attacks VM-based attacks Weak or no Logical Segregation Side channel attacks Privilege Escalation Service abuse Privilege escalation attacks Inefficient resource policies	Multi-factor Authentication Intrusion Detection System User data isolation Attribute/identity based encryption Role-Based Access Control model User-based permissions model Process isolation	As all services and VMs are executing in a virtualized environment, its compromise will have adverse effect on all Fog services, data and users
Web security issues	SQL injection Cross-site scripting Cross-site request forgery Session/Account hijacking Insecure direct object references Malicious redirections Drive-by attacks	Secure code Find and patch vulnerabilities Regular software updates Periodic auditing Firewall Anti-virus protection Intrusion Prevention System	Exposure of sensitive information, attacker can become legitimate part of network, and enable malicious applications to install
Internal/external communication issues	Man-in-the-Middle attack Inefficient rules/policies Poor access control Session/Account hijacking Insecure APIs and services Application vulnerabilities Single-point of failure	Encrypted communication Mutual/Multi-factor authentication Partial encryption Isolating compromised nodes Certificate pinning Limiting number of connections Transport layer security (TLS)	Attacker can acquire sensitive information by eavesdropping and get access to unauthorized Fog resources
Data security related issues	Data replication and sharing Data altering and erasing attacks Illegal data access Data ownership issues Low attack tolerance Malicious Insiders Multi-tenancy issues Denial of Service attacks	Policy enforcement Security inside design architecture Encryption Secure key management Obfuscation Data Masking Data classification Network monitoring	High probability of illegal file and database access, where attacker can compromise both user and Fog system's data
Wireless security issues	Active impersonation Message replay attacks Message distortion issues Data loss Data breach Sniffing attacks Illegal resource consumption	Authentication Encrypted communication Key management service Secure routing Private network Wireless security protocols	Vulnerable wireless access points can compromise communication privacy, consistency, accuracy, availability and trustworthiness
Malware protection	Virus Trojans Worms Ransomware Spyware Rootkits Performance reduction	Anti-malware programs Intrusion Detection System Rigorous data backups Patching vulnerabilities System restore points	Malware infected nodes will lower the performance of the entire Fog platform, allow back-doors to the system and corrupt/damage data permanently

reason for this is that the security issues facing Fog systems is an infant research area, and only few of solutions are available to detect and prevent malicious attacks on a Fog platform. The below section provides an overview of such systems.

Privacy preserving in Fog computing

Research into preserving privacy in sensor-fog networks [95] consists of the following summarised steps to secure sensor data between end-user device and Fog network:

- They collect sensor data and extract features;
- Fuzzing of data by inserting Gaussian noise in data at a certain level of variance to lower the chance of eavesdropping and sniffing attacks;
- Segregation by splitting data into blocks and shuffling them to avoid Man-in-the-Middle (MITM) attacks;
- Implementing Public Key Infrastructure for encrypting each data block; and
- Transmit segregated data to Fog node, where data packets are decrypted and re-ordered.

The system also includes a feature reduction ability for minimising data communication with Fog nodes to help minimise risk. This work is of significance as it focussed on preserving personal and critical data during transmission. The proposed technique can be improved by selecting an encryption and key management algorithm, focussing on those that play an important role in maintaining the privacy of data. In addition, there is

little discussion on the required computational overheads for performing extensive data manipulation (fuzzing, segregation, encryption, decryption and ordering, reordering) before and after the communication. This could be of significance when designing and producing a Fog system as the required computation overheads might not be available. Another important aspect to notice here is that sensors transmit data continuously, possibly over longer periods of time, and the proposed privacy framework might overload or even crash the underlying Fog system.

Mitigating insider data theft

One study [96] provides a solution for protecting data from malicious insiders using components of Fog and Cloud computing. It combines behaviour profiling and decoy approaches to mitigate security threats. If any profile exhibits abnormal behaviour, such as the increase of accessing different documents at unusual times, the system will tag the access as suspicious and block the respective user. Decoy is a disinformation attack that includes fake documents, honeyfiles, honeypots and other kinds of baiting data that can be used to detect, confuse and catch the malicious insider. This research domain is significant as it demonstrates potential altering and mitigation methods to defend against data theft. More specifically, they demonstrate that the proposed technique can correctly identify abnormal behaviour with an average accuracy greater than 90%. However, the experiment is performed with a limited amount of data. More specifically, eighteen students from a single university over the duration of four days. Hence, the results in terms of accuracy they claim might not reproducible or universal. Their technique can be improved by increasing the population size and running the experiment over longer timespan [97]. Furthermore, the computational requirements of such an approach are not mentioned. The paper provides no details on the quantity of data that is stored, as well as the CPU time and memory required during analysis. Such behaviour profiling techniques are often performed in a traditional client-server architecture where computation resources are freely available. It is not clear how this technique is able to be executed on a Fog node without having adverse affects on core functionality. The technique can be further improved through critically analysing and selecting feasible machines learning techniques and training data required for behaviour profiling. This carries more importance due to the presence of a large number of user and files. Similar behaviour profiling and decoy techniques are used in other works [98, 99] to detect and prevent malicious insider threat.The behaviour profiling, monitoring and user matching process would not exert any burden on Cloud resources and prevent actual data theft without exposing any sensitive data. As an added benefit, all of these operations will occur on-premise and execute relatively faster due to low bandwidth latency.

Policy-driven secure management of resources

One piece of work introduces a preliminary policy management framework for the resources of Fog computing to enhance secure interaction, sharing and interoperability among user-requested resources [100]. The system is divided into five major modules:

- Policy Decision Engine (PDE) for taking action based on pre-defined policy rules;
- Application Administrator (AA) to manage Fog multi-tenancy;
- Policy Resolver (PR) for attribute-based authentication;
- Policy Repository (PRep) holding rules and policies; and
- Policy Enforcer (PE) to detect any discrepancies in policy implementation.

AA is responsible for defining rules and policies (stored in PRep) while considering multiple tenants, applications, data sharing and communication services. When a certain service request is made from a user, it is sent to a PR that identifies the user based on specific set of attributes and access privileges against a requested resource. The user attributes and their respective permissions are stored in a database. PDE takes user information from the PR, extracts rules from the PRep, analyse them and enforce through the PE. The eXtensible Access Control Markup Language (XACML) is used to create rules and the OpenAZ framework for building PDE. Despite being in an initial phase, this policy framework has potential to become an integral part of real-time distributed systems in future, where there is a strong need for access, identity and resource management abilities. However, this framework is limited to only those systems, which are able to allocate dedicated resources within Fog platforms for the bulk of computations required by various modules to execute the framework. Fog platforms should be capable of handling highly time-sensitive applications, but the proposed validation process might take longer to make decisions. Another flaw in their technique is that the solution itself is inherently vulnerable to DoS attacks due to the complex authentication process in PR and PDE. If an attacker establishes a large amount of connections simultaneously, repeats the 'validation process' in the same connection continuously or responds to the authentication protocol in a low and slow manner [101], the Fog resources will become exhausted and rendered unavailable for the intended users. However, these security concerns can be reduced by building a performance model that is collecting values of memory, CPU and disk

utilization and periodically comparing with estimated values [102]. In case the system identifies an anomaly, the user would be redirected to the *Shark Tank* cluster, which is essentially a proxy to closely monitor the user but can grant full application capabilities.

Authentication in Fog platform

Insecure authentication protocols between Fog platforms and end-user devices have been identified as a main security concern of Fog computing by [19]. The author's claim that the IoT devices, especially in smart grids, are prone to data tampering and spoofing attacks and can be prevented with the help of a Public Key Infrastructure (PKI), Diffie-Hellman key exchange, Intrusion detection techniques and monitoring for modified input values. Furthermore, the authors demonstrate the high importance and impact of MITM attack on Fog computing by launching a Stealth attack on video call between 3G and the WLAN users within a Fog network. Results show that the attack did not cause any visible change in memory and CPU consumption of Fog node, hence it is quite difficult to detect and mitigate. The authors recommend that the risk of such attacks can be prevented by securing communication channels between the Fog platform and the user through implementing authentication schemes.

Based on the current state of authentication in Fog platform, Fog platforms are missing rigorous authentication and secure communication protocols as per their specification and requirements. In a Fog platform both security and performance factors are considered in conjunction, and mechanisms such as the encryption methodologies known as *fully homomorphic* [103] and *Fan-Vercauteren somewhat homomorphic* [104] can be used to secure the data. These schemes consists of a hybrid of symmetric and public-key encryption algorithms, as well as other variants of attribute-based encryption. As homomorphic encryption permits normal operations without decrypting the data, the reduction in key distribution will maintain the privacy of data. Other research work provides a similar framework to secure smart grids, regardless of Fog computing, called the Efficient and Privacy Preserving Aggregation (EPPA) scheme [105]. The system performs data aggregation based on the homomorphic Paillier cryptosystem. As the homomorphic ability of encryption makes it possible for local network gateways to perform an operation on cipher-text without decryption, it reduces the authentication cost (in terms of processing power) while maintaining the secrecy of data.

Using advance encryption standard (AES)

This paper [106] concludes that AES is a suitable encryption algorithm for a Fog platform. Multiple metrics have been considered for the performance evaluation: user load against CPU time and file size against encryption/decryption time and memory utilization. According to the results, encryption time was nearly the same for both smartphone and laptop using small amount of data, such as 500 Kb, 5 Mb, and 10 Mb. Although, AES encryption is universally accepted [107] and is feasible for Fog computing, due to low hardware specifications and smaller computations, the experiment does not compare AES with any other available encryption algorithm. In addition, the size of the encryption key plays an important role in strengthening the encryption. Furthermore, the experiment should also have compared the performance and efficiency vector of different key sizes; 128, 192 or 256-bits. Their work lacks evidence and justification as only three sample files are used in whole experiment. Using small sample size might not provide the deep insight to whether AES is a suitable algorithm for Fog networks and storage or not. Furthermore, only textual data is used for encryption/decryption processes and it is unclear if the same results can be replicated with images or any other data format. Moreover, the Fog platform consists of heterogeneous devices with different specifications and single algorithm might not be able to cover all possible scenarios. Encryption is already an additional task for the Fog platform and also consumes large amounts of resources. The selection of encryption algorithm (whether symmetric, asymmetric or hybrid) should be performed in accordance with provider and infrastructure requirements.

Conclusion

It is evident in the above sections that the recommended security solutions are individually not sufficient to protect the CIA of Fog platform. Hence, the current security state of Fog networks do not satisfy the modern day security requirements. Broadly speaking, the literature briefly provides the solutions to data integrity, insider threat, managing resource access policy, user authentication and encryption. However, there is a pressing need to resolve critical issues stemming from shared technology, lack of access control, user account management, service downtime, data loss/breach, insufficient vulnerability patching and poor system monitoring. Any of these stated threats can allow attackers to risk the CIA of Fog network and connected devices. One potential solution to these issues can be to reuse well-established and proven security protocols of other similar technologies. The Fog platform components and their operations are not entirely new because they mimic Cloud (as stated in "Introduction" section). The main challenge here is to link and modify the security measures and apply them in accordance with the requirements of Fog platform. The existing security measures have gone through rigorous testing, and using them has the potential to ensure that any Fog system satisfies necessary industrial security standards.

Recommended security measures and future challenges

In the light of above literature review, this section presents the security knowledge gaps that should be covered to build a reliable, applicable and trustworthy Fog platform. Despite having large potential and number of applications, there is a lack of security solutions available for Fog system developers and designers. However, as Cloud computing and many similar technologies (albeit centralised systems) resemble the working mechanism of Fog computing, they can provide a deeper insight into the security threats and solutions. Even though each Fog deployment has a different set of security requirements, applications and sensitivity, the following subsections provide a comprehensive, efficient and applicable security solutions, which are gathered and tested on various systems. They can also be used as generic best practise guidelines while developing the Fog software, so that the security is enabled from within the platform. Table 3 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.

Data encryption

Recommendation: 1 *The data needs to be secured before (at rest in source location), during (in motion through network) and after (at rest in destination location) communication among IoT devices, the Fog network and Cloud platform.*

Future challenge: 1 *Added data security measures typically cause significant reduction in computational resources available for normal Fog-based operations [108]. In addition, the cipher-text can consumes more disk space than original text and further influences the working mechanism of application and database layers.*

Data encryption is a widely used mechanism to protect data confidentiality. To overcome the higher resource allocation issues of encryption, only sensitive and critical information should be encrypted, such as user's identity in vehicular networks, patient data in healthcare systems, cached data and so on. For data at rest, the AES algorithm with 256-bit key size or obfuscation can be used to ensure privacy, while the Secure Socket Layer (SSL) protocol can be used for establishing secure communication between a server and a client [109, 110]. In addition, efficient data integrity checks [111] should be performed before and after communication to validate the received information and it's sender. The important aspect here is to clearly distinguish between archival data and sensitive information. Encrypting archival data like public video streaming will reduce the performance of Fog system and impact upon the performance of sibling applications. It is, therefore, essential for the designer of a Fog system to adequately assess the importance of the data and implement security measures where necessary.

Preventing cache attacks

Recommendation: 2 *Fog platforms maintained for Cache management system are prone to software cache-based side channel attacks such as exposing cryptographic keys, which may lead toward leaking sensitive information.*

Future challenge: 2 *Prevention of cache-based attacks is either too expensive for practical implementation or the solution only protects against a specific kind of attack. Research shows that cache interferences is the most common type of attack, whose elimination requires both hardware and software modifications [112].*

Fog systems that are used for enhancing the performance and power efficiency of other systems using advanced memory caching techniques can be probed via Cache Side Channel Attacks [113], resulting in the exposure of sensitive data within connected systems. The cache holds data that is frequently used and could contain personal user information. Fog platforms used in this manner should include security solutions like *Newcahe* [114] and *STEALTHMEM* [115]. These solutions are alternative low-level implementations of a security-centric memory cache system that can better protect residing data. For new cache designs, solutions like *Partition Locked cache* and *Random Permutation cache* [116] can relieve Fog network from cache interferences attacks. In addition, the mechanism to prevent

Table 3 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-tenancy		✓	✓		✓		✓		✓		✓	✓
Backup and recovery						✓				✓		

modifications in smart meter data in the advanced metering infrastructure would be to retain collected data in Fog node for specific duration of time before release. Even though these security solutions are expensive and difficult to implement, Fog platform developers should consider them as it is important not to rely on standard default implementations that may result in significant weaknesses.

Network monitoring

Recommendation: 3 *Fog systems that are continuously handling private data (e.g generated by IoT device) from end-user to Cloud platform and vice versa, should monitor and detect anomalous activity in network through automated enforcement of communication security rules and policies.*

Future challenge: 3 *A Fog network is usually connected to large number of small devices. The data generated by a single device may be small, but when the streams of multiple devices are combined, the amount of overall data becomes significantly challenging to handle [117]. Hence, filtering each network packet would instigate the necessity to increasing processing and memory capacity.*

Each Fog platform should implement resource efficient network monitoring mechanisms. They should be considered as an integral part of every Fog system, so that malicious activity can be identified and terminated before any real damage occurs. The fundamental underlying process comprises of scanning dynamic and large networks to mark suspicious and malicious network packets based on pre-defined rules and policies. A Fog platform can deploy efficient tools like *CLOUDWATCHER* [118] for partial network monitoring by selecting specific devices and *PayLess* [119] for scanning SDN communication with minimal computing resources. The network scanning process can be classified as static, dynamic or a combination of both. Scanning is typically achieved by assorting Firewalls, Anti-viruses and Intrusion Detection and Prevention Systems [120–122]. For further improvement, the network monitoring applications can start operating in distributed and intelligent manner. They can use Artificial Neural Networks (ANNs) and rule matching [123] for threat detection as a large number of heterogeneous (IoT) devices are transmitting and processing heterogeneous data on multiple levels (hypervisor, operating system, and applications). Furthermore, due to the localised nature of Fog devices, the implementation of Virtual Private Networks (VPNs) can also help in isolating the network from external attacks.

(Zero day) Malware protection

Recommendation: 4 *Fog systems should protect themselves against both new and existing malware-based attacks, which can occur in the form of virus, trojan, rootkit, spyware and worms to avoid unwanted infection and serious damage.*

Future challenge: 4 *The ever increasing complexity of malware attacks, lack of modern day threats detection, possibility of more zero day vulnerabilities, and the and sparse nature of connected (mobile) devices presents significant protection challenges. The Fog system also requires a lightweight, cross-storage host agent and a network-based detection service to fully defend against these threats [124].*

Most Fog systems are missing appropriate malware protection schemes as they requires dedicated and continuous allocation of network and computation resources, which might not be available in every Fog platform. With the presence of a large number of end-users and zero days threats, any user's device or malicious tenant could (unknowingly) inject and spread malware, which as a result could compromise the entire network. As many Fog systems are also deployed on smart-phones and tablets such as in BCI applications, they can become a source of malware infection [125]. One suitable solution would be a physical malware detection device [126] as it would use minimal Fog resources. By increasing the Fog platform specifications, tools like BareCloud [127] can be deployed, which can automatically detect evasive malware. Furthermore, machine learning techniques [128–130] can be applied to identify zero day attacks with higher accuracy. These techniques essentially train algorithms like support vector machines with a benign software model and after that, any abnormal behaviour can trigger the detection event. Apart from stealing data or modifying core system functionality, the presence of malware can decrease system performance. Hence, it is vital to continuously scan for compromised nodes and deploy counter-measures to prevent the inclusion of malicious nodes and end-user devices. Those designing and developing Fog systems would need to consider the potential of underlying operating system [131] to become compromised and considering how their system, and its physical implications can be protected to minimise damage. For example, in the health-care domain, it would be essential that if a Fog system became compromised, that critical data and functionality would still be protected by having strong integrity checks and make sure that the system is quarantined as soon as malicious activity appears within the host operating system.

Wireless security

Recommendation: 5 *The internal and external wireless communications of Fog platform with end-user devices need to minimise packet sniffing, rouge access points and similar challenges by implementing both encryption and authentication procedures.*

Future challenge: 5 *Fog platforms are mainly composed of wireless sensors and IoT devices [132]. Due to the volume*

and visibility of each wireless capable device, it is difficult to ensure the security of the Fog network. If not hidden and secured, the wireless network gives unprecedented freedom to attackers to intercept sensitive data in transmission.

Many wireless devices, such as health monitoring, camera sensors, RFIDs and mobile phones are connected with Fog platforms and are continuously transmitting private data from nearby locations. It is important that their communication is encrypted using Wi-Fi security algorithms like *WiFi Protected Access* (WPA), WPA2 [133] etc. Wireless access points are usually visible to all devices without any connection. If they are not properly secured, attacker can become part of network (Sybil attack), use bandwidth illegally (Flood Attack) and intercept network traffic using MiTM attack to alter or even terminate data communication [134]. In case of medical applications, insecure wireless connection might also put human life at risk. It is therefore of critical importance to implement wireless protocols like 802.11 or it's amendments: 802.11a and 802.11g. In addition, different intrusion detection techniques can be used for protecting the communication of heterogeneous 5G mobile networks as discussed in a recent survey paper [135].

Secured vehicular networks

Recommendation: 6 *In order to increase road safety and real-time application of vehicular networks, they should protect themselves from internal and external security threats.*

Future Challenge: 6 *A vehicular Fog network is volatile as the connection with end-user is established for only a shorter period of time, which makes it difficult to verify identities. The amount of connections, heterogeneous data and factors of multi-hop connection can increase to a large scale, which will render even a robust security system useless. [136].*

When using a Fog platform to support vehicular network, the security protocols should not be limited to BSs, SDNCs and RSUCs, but should also encompass Fog devices that are actually processing, storing and forwarding vehicular data. A Fog system should secure itself by authenticating user identity, check for data consistency and integrity, service availability, ability to revoke any connection and anonymous key management as well as enhance the protection of connected systems by monitoring and inserting real-time constraints [137]. If Fog nodes are capable of performing user authentication and message integrity checks, it will eliminate message suppression, fabrication, replay and alteration attacks [138]. The process should be anonymous and stateless like STAMP [139], so that the user's location and identity is kept private, even from the Fog network. The implementation of such security measures between vehicles and Fog nodes will prevent primitive attacks before they reach and exploit cloud system too, and would help in improving the overall road safety.

Secured multi-tenancy

Recommendation: 7 *Fog computing should enable highly constrained access control on both data and network, along with fair resource allocation mechanisms to protect confidentiality and integrity within a multi-user environment.*

Future Challenge: 7 *When a large number of end-users start to share Fog applications and resources, the performance, scalability, data security, user identity management, monitoring and the potential arising from insiders threats becomes difficult to manage in a Fog network [140].*

As mentioned above, Fog platforms are a highly virtualized environment, supporting multi-tenancy and are capable of provisioning resource management facilities to Cloud systems. Many security concerns are driven by multi-tenancy implementations, such as co-resident data, malicious tenants, eavesdropping, memory escaping and hopping and misconfiguration [141, 142]. Fog platforms should implement multi-factor authentication mechanisms based on either the role or identity of end-users, logically segregate data and resources and aggressively analyse the activities of both administrator and tenants. Another system called *Secure and Resilient Networking* (SeReNe) service can provide a Fog platform with programmable environment to adjust it's topology, bandwidth allocation, and traffic policies [143]. Furthermore, as many devices are connected, Fog system should be able to fairly allocate compute resources among users meanwhile preventing virtualization-based (hypervisor and VM) attacks (as shown in table 2) to keep the infrastructure available.

Backup and recovery

Recommendation: 8 *Depending upon the kind of application, Fog platforms should have data backup and recovery modules. Such system should mirror copies of data on-site, off-site or both on a regular basis. It will benefit both customers and company to keep the operations running from using previous backups, minimising service disruptions.*

Future Challenge: 8 *The Fog platform has a high frequency of data throughput and relatively low amount of stored data, but this does depend on the requirements and application. The challenge is that data backup and recovery is a costly process [144] and requires acute focus on data selecting, mapping, testing and determining accessibility roles in case of recovery process.*

In case of natural disaster, system failure or cyber-attack, Fog platforms can loose all data and hence there is a need for primary and secondary backups. The selection of data that goes into backup depends upon the sensitivity, demand and its role in day-to-day operations. According

to [145], it is important to not duplicate the data before backup. It will decrease costs and notably reduce the consumption of resources during backup process and recovery. There are also many methods available to improve the process 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 (SBBR) [146]. Further improvements for the Fog platform are backup and recovery procedures for SSD-assisted database systems [147] and VM images [148] as a whole. For mobile and wireless Fog platforms, the situation might get challenging as the system would require portable and on-site backup storage or will need a significant amount of network bandwidth to transmit data to the off-site location.

Security with performance

Recommendation: 9 *A balanced trade-off between the level of functionality and integrated security is vital for Fog network performance. It will enable fully featured applications meanwhile protecting the CIA of data and networks against internal and external threats.*

Table 4 Summary of recommended security solutions and impact on CIA

Solution category	Resolves	Benefits
Data Encryption	Malicious insiders Data Breach Data Loss Insufficient Due Diligence Spyware/malicious processes	If data is breached either at rest, processing or motion, encryption will keep the original data hidden from unauthorized recipients
Preventing cache attacks	Insecure API Service and application vulnerabilities Sensitive data Leakage Sniffing attacks	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
Network monitoring	Advance Persistent Threats Access control issues Denial of Service attack Malicious Insiders Insufficient Due Diligence Abuse and Nefarious use of resources Data Breaches Attack detection	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
Malware protection	Account Hijacking Insecure API Service and application vulnerabilities Data corruption/damage risks Shared Technology Issues Performance degradation	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
Wireless security	Advance Persistent Threats Access control issues Data breach Eavesdropping attacks Illegal bandwidth consumption	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
Securing vehicular networks	Advance Persistent Threats Access control issues Account/Session Hijacking Denial of Service attacks User identity protection	Increases road safety by preserving data communication integrity while keeping the user identity and location data private
Secured multi-tenancy	Access control issues Account Hijacking Insecure APIs Malicious Insiders Abuse and Nefarious use of resources Data Breaches Segregation 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
Backup and recovery	Data Loss Data unavailability issues Insufficient Due Diligence Malware infection Data integrity issues	In case of natural disaster, malware infection or DoS attack, the data will remain available to users and system along with its integrity

Future Challenge: 9 *A poor security system implementation can have significant performance issues. Hence, it is important to carefully choose, in-accordance with the requirements, what security features to integrate, the degree and extent of usage, required components and defining performance benchmarks.*

It is not always the case that improving the security posture of a system does not necessarily mean to compromise on performance. It is a matter of trade-off between features and elimination of unneeded security measures to make effective use of available resources. A Fog network is capable of sharing data loads, and their computing resources can also be increased on-demand, although it might not be the case for every single Fog platform. This might be a reason why many security solutions mentioned in Section Existing security solutions for Fog computing do not consider the lack of Fog resources as an issue, as the computing power can be expanded. The security solutions should become an integral part of every Fog platform because if they are insecure, their performance might decrease eventually due to attacks like malware infection, resource abuse, etc. A large number of IoT devices sending data towards Cloud systems creates a subtle role for intermediate processing on a Fog platform. If security solutions are built within Fog software and not as a bolt-on addition, it might help to reduce the resource utilisation as well. Although the main purpose of a Fog platform is to offload tasks for better performance, the security measures should be taken into account as an integral part of the Fog system for keeping CIA of all kinds of data. Therefore, the main challenge for Fog platform developer is to build a system that can efficiently provision security without making eminent sacrifices in performance.

Conclusion and future work

The purpose of this study was to review and analyse real-world Fog computing applications to identify their possible security flaws. To provide a holistic review, Fog related technologies like Edge computing and Cloudlets are also discussed. It was discovered that most Fog applications do not consider security as part of system, but rather focus on functionality, which results in many Fog platforms being vulnerable. Literature also details that Fog computing has a wide potential and range of applications that all demand a high level of security to protect the CIA of the customer data. Fog platforms are a relatively new paradigm, and this study can help readers and developers to foresee security measures and their challenges, while envisaging the design of new Fog systems. Table 4 summarises the discussion of how recommended security solutions (see Section Recommended security measures and future challenges) might be able to prevent, detect and pro-actively defend against the threats stated in Table 2. The aim of these security solutions is to protect the CIA of entire Fog system and its users. Additionally, Fig. 4 illustrates the possible security solution categories with respect to various components of Fog infrastructure, residing between IoT devices and Cloud.

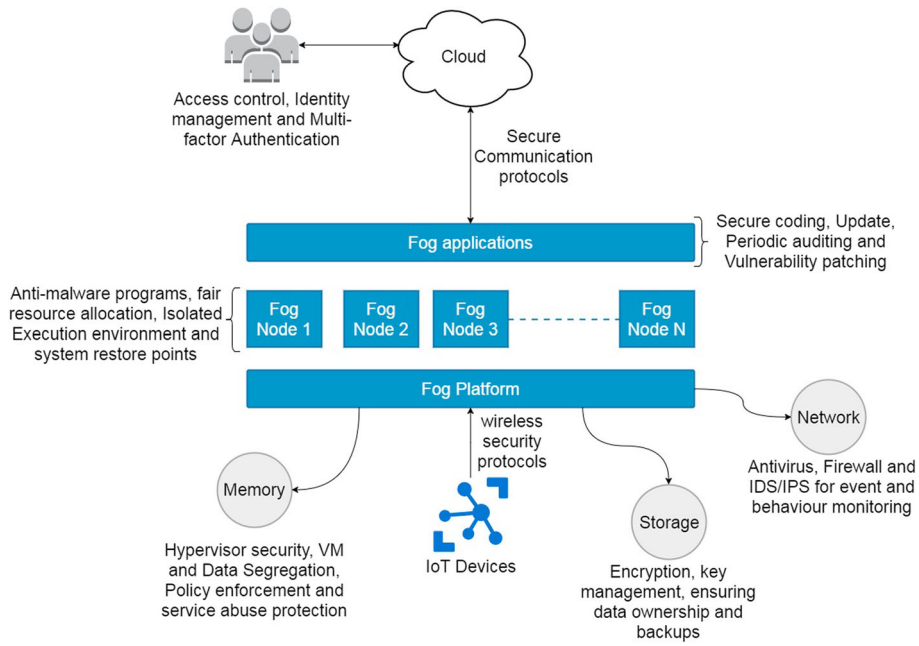

Fig. 4 Fog Computing Platform and the deployment of security solutions on various components of the Fog system. This figure shows how and where proposed security solutions can be placed and help in eliminating various security flaws

Future work could lead towards the development of a knowledge-based supplementary and aid system, which can provide decision support services for developers in designing a secure and performance efficient Fog infrastructure. Such a decision support system would require a large systematic knowledge acquisition of best practices, known security threats and their solutions, which can be formalized as either statistical-based system or rules, policies and facts [149]. The system would also require an inference engine that can provide and explain suitable solution or advice, considering the given application scenario (current context) and available knowledge. A Fog platform is connected with both end-users and Cloud platform along with processing, storing and transmitting large volumes of data by consuming limited amount of resources. It is therefore of key importance that security measures are correctly adhered to overcome the potential limitations identified in this paper. Hence, the use of a decision support tool that is capable of advising security measures to developers can prevent the occurrence of vulnerabilities pro-actively and save the Fog platform from potential damage.

Authors' contributions

This research work is a part of SK Ph.D. work, which is being conducted under the supervision of SP. The paper presents extensive review about the Fog computing applications, current security threats and proposes comprehensive techniques to increase the security of overall Fog platform. The work presented in this paper were carried over the past 8 months. All authors read and approved the final manuscript.

About the Authors

Saad Khan is pursuing Ph.D. in the School of Computing and Engineering from University of Huddersfield, UK. His research interests are in developing secure Fog/Cloud platforms with better performance, increasing the efficiency of security solutions by using artificial intelligence techniques, and other closely related areas.

Simon Parkinson is a Senior Lecturer in Informatics within the school of Computing and Engineering at the University of Huddersfield, UK. His research interests are artificial intelligence and cyber security, focussed on various aspects such as access control, vulnerability management, learning domain knowledge and mitigation planning.

Yongrui Qin is a Lecturer of Knowledge and Information Systems in School of Computing and Engineering, University of Huddersfield, UK. His main research interests include Internet of Things, Web of Things, Semantic Web, data management, data mining and mobile computing.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 15 May 2017 Accepted: 8 August 2017
Published online: 16 August 2017

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 J Comput 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/fog-computing-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 countermeasures. 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 and 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. Aciiçmez 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 Netw 10:3049–3058
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) Multi-tenancy 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 ICH M7. Regulatory Toxicol Pharmacol 84:124–130