From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework

T.Syam Prasad[1], A.Mallikarjuna[2], S.Ramakrishna[3]
[1]*PG Scholar, Department of Computer Science, S.V University, Tirupati – INDIA*
[2]*Teaching Assistant, Department of Computer Science, S.V University, Tirupati -INDIA*
[3]*Professor, Department of Computer Science, S.V University, Tirupati- INDIA*

Abstract- **Fog computing, an extension of cloud computing services to the edge of the network to decrease latency and network congestion, is a relatively recent research trend. Although both cloud and fog offer similar resources and services, the latter is characterized by low latency with a wider spread and geographically distributed nodes to support mobility and real-time interaction. In this paper, we describe the fog computing architecture and review its different services and applications. We then discuss security and privacy issues in fog computing, focusing on service and resource availability. Virtualization is a vital technology in both fog and cloud computing that enables virtual machines (VMs) to c7oexist in a physical server (host) to share resources. These VMs could be subject to malicious attacks or the physical server hosting it could experience system failure, both of which result in unavailability of services and resources. Therefore, a conceptual smart pre-copy live migration approach is presented for VM migration. Using this approach, we can estimate the downtime after each iteration to determine whether to proceed to the stop-and-copy stage during a system failure or an attack on a fog computing node. This will minimize both the downtime and the migration time to guarantee resource and service availability to the end users of fog computing. Last, future research directions are outlined.**

Index Terms- **Cloud computing, edge computing, fog computing, live VM migration framework, virtualization.**

I. INTRODUCTION

Fog computing, an extension of cloud computing services to the edge of the network to decrease latency and network congestion is a relatively recent research trend. Although both cloud and fog offer similar resources and services, the latter is characterized by low latency with a wider spread and geographically distributed nodes to support mobility and real-time interaction. In this paper, we describe the fog computing architecture and review its different services and applications. We then discuss security and privacy issues in fog computing, focusing on service and resource availability. Virtualization is a vital technology in both fog and cloud computing that enables virtual machines (VMs) to coexist in a physical server (host) to share resources. These VMs could be subject to malicious attacks or the physical server hosting it could experience system failure, both of which result in unavailability of services and resources. Therefore, a conceptual smart pre-copy live migration approach is presented for VM migration. Using this approach, we can estimate the downtime after each iteration to determine whether to proceed to the stop-and-copy stage during a system failure or an attack on a fog computing node. This will minimize both the downtime and the migration time to guarantee resource and service availability to the end users of fog computing.

II. FOG COMPUTING

The popularity of IoT applications and the increased digitalization of our society where millions to billions of smart devices (e.g., in smart homes, smart cities, smart metering systems, intelligent vehicles and large-scale wireless sensor networks) are constantly exchanging information over the Internet have resulted in large volumes of data that need to be managed and processed. To achieve this ,cloud computing is a popular option due to its scalability, storage, computational and other capabilities to support the provisioning or de-provisioning of resources according to user requirements in real-time. However, in recent years, fog computing has been proposed to extend the cloud computing paradigm

from the core to the edge of the network. It presents a highly virtualized platform that provides computational, networking and storage services between cloud computing and end devices. For example, Zhu et al. describe fog computing as an enabler of smart applications and Internet services (including cloud) for data management and analytics. Song et al. construct a system model of fog computing by combining its features and that of graph theory to propose a dynamic load balancing mechanism based on the graph repartitioning.

A. FOG COMPUTING ARCHITECTURE AND FEATURES:

Fog computing has a distributed architecture that targets services and applications with widely dispersed deployments. Different fog computing architectures have been proposed in the literature. For example, Sarkar et al. described a three-tier architecture where the bottom tier comprises several terminal nodes (TN) (e.g., smart device and wireless sensor nodes) that transmit information to the upper tiers. Tier two is the middle tier (also referred to as the fog computing layer) comprising highly intelligent devices, such as routers, switches and gateways. The third and uppermost tier is referred to as the cloud computing tier that has several high-end servers and data center(s). Shi et al. presented a simple fog architecture comprising off ognodes in between cloud components and end devices. Similar to the architecture presented in, Lee et al. described a hierarchical fog computing architecture consisting of three components, namely: IoT nodes, fog nodes and back-end Cloud. Zhu et al. described the Cisco overview of fog computing architecture by presenting a three-layered approach consisting of distributed intelligence end-point computing (i.e., smart things network, embedded systems and sensors), distributed intelligence fog computing (i.e., multi-service edge and filed area network), and centralized intelligence cloud computing (i.e., data center cloud and core).

Bonomi et al. presented a fog computing architecture comprising homogeneous physical resources, fog abstraction layer and a fog service orchestration layer (see Fig. 1). Heterogeneous physical resources consist of components such as servers, edge routers, access points, set-up boxes and end-devices with different storage and memory capacities to support additional functionalities. The platform is hosted on different OSs and software applications, thus having a wide range of software and hardware capabilities.

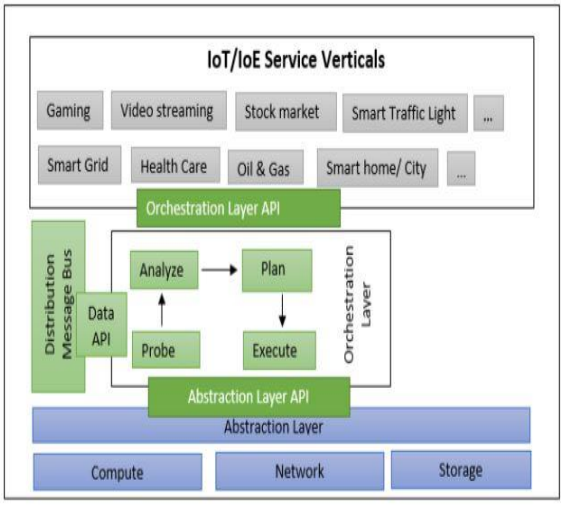

FIGURE 1. Architecture and components of fog computing.

The fog abstraction layer provides a generic application programming interface (API) for monitoring resources such as CPU, memory and network by hiding the platforms' heterogeneity and unveiling the uniform and programmable interface for seamless resource management and control – see Fig. 1. It supports virtualization and enables multiple OSs to co-exist on a single physical machine to ensure efficient use of resources. The multi-tenancy feature ensures the isolation of different tenants on the same physical machine. The orchestration layer provides a dynamic and policybased life cycle for managing fog services. The orchestration functions by providing a distributed approach as the underlying fog infrastructure and services. The fog orchestration layer consists of a small software agent (hereafter referred to as foglet). Foglet is used to monitor the current state of the deployed fog nodes by presenting a wide range of capabilities using components such as software agent, distributed storage, scalable message bus and distributed policy engine. The orchestration layer API performs four basic functions, namely: probing and application of data, analyzing the retrieved data, managing requests by planning and allocation of resources, and enforcing decision [18]. The fog platform hosts different applications such as smart cities and smart grids. Fog computing provides an improved quality-ofservice (QoS), low latency and location awareness to mobile

nodes through edge routers and access points. The latter, for example, can be positioned along highways and tracks to provide resources and services to applications that are latency sensitive (e.g., gaming, video streaming, real-time traffic monitoring systems, and emergency healthcare services). A common characteristics associated with fog computing is its deployment at the ‘‘edge of the network’’, which implies that fog computing has features that make it a nontrivial extension of cloud computing. We highlight some of these key features below:

• *Heterogeneity:* Fog computing is a virtualized platform that offers computational, networking and storage services between cloud computing and end devices. Its heterogeneity feature serves as a building block as it exists in different forms and can be deployed in wideranging environments.

• *Geographical distribution:* Fog computing has a widely distributed deployment in order to deliver high-quality services to both mobile and stationary end devices.

• Edge location, location awareness and low latency: The emergence of fog computing is partly due to the lack of support for endpoints with quality services at the edge of the network. Examples of applications with low latency requirements are video streaming in real-time closedcircuit television monitoring and gaming.

• Real-time interaction: Various fog applications, such as real-time traffic monitoring systems, demand real-time processing capabilities rather than batch processing.

• Support for mobility: Mobility support is essential for many fog computing applications to enable direct communication with mobile devices using protocols such as Cisco’s Locator/ID Separation Protocol that decouples host identity from location identity using a distributed directory system.

• Large-scale sensor networks: This is applicable when monitoring the environment or in smart grid using inherently distributed systems that require distributed computing and storage resources.

• Prevalent to wireless access: Wireless access points and cellular mobile gateway are typical examples of a fog network node.

• Interoperability: Fog components must be able to interoperate to ensure support for wide range of services like data streaming.

Su et al. proposed a Steiner tree approach based on a caching scheme, where fog servers initially produce a Steiner tree when caching resources to minimize total path, weight and cost, in order to reduce resource caching costs. The comparison between the workings of the Steiner tree in fog computing and the traditional shortest part scheme suggested that the former achieves better efficiency. Zhu et al. deployed fog computing to process and transmit video applications and services, ranging from proxy-assisted rate adaptation to intelligent caching for on-demand video streaming. This enhances the quality of experience (QoE) and virtual desktop infrastructure interactive system of real-time video for surveillance cameras. Truong et al. proposed a new Vehicular Adhoc Network (VANETs) architecture by combining Software Define Network (SDN) and fog computing to offer an optimized low-latency deployment. Gazis et al. presented an industrial context of deploying fog computing by introducing an adaptive operational platform to provide an end-to-end manageability for fog computing infrastructure, according to the operational requirements of the individual process. Femtocloud systems were proposed in to offer a dynamic, self-configuring and multi-device mobile cloud from a cluster of mobile devices to provide cloud services at the edge. The evaluations suggested that the approach can provide reasonably efficient computational capacity. In advanced metering infrastructure, the amount of collected and processed data has increased exponentially, therefore, the centralized cloud approach is no longer adequate. Yan and Su proposed using fog computing in existing smart meter infrastructure to provide a reliable and costeffective solution.

B INTERACTION BETWEEN FOG COMPUTING, CLOUD COMPUTING AND INTERNET OF THINGS

Fog computing brings cloud computing closer to Internet of Things (IoT) devices. The advent of IoT has resulted in an increasing number of use cases that generate significant volume of data, compounding the challenges of dealing with big data from a number of geographically distributed data sources. To efficiently analyze these time-sensitive data, fog computing was proposed. To harness the benefits of IoT and speed up awareness and response to events,

we require a new set of infrastructures as current cloud models are not designed to handle the specifics of IoT (i.e., volume, variety and velocity of data). Specifically, billions of previously unconnected devices are now generating over two exabytes of data every day and it has been estimated that by 2020, 50 billion ‘‘things’’ will be connected to the Internet. Therefore, fog computing has been identified as a viable solution.

A framework that combines IoT, cloud computing, and fog computing for smart human security. This framework provides a wearable computing system by harnessing the pervasive nature of IoT, omnipresence feature of cloud, and the extension of fog computing to provide security cover for people. In a similar vein,integrated fog computing and cloud computing by considering mobility, reliability control and actuation, and scalability to demonstrate that fog computing can be used as the underlying platform for IoT applications.presented an architecture for secure E-health applications using big data, IoT, and cloud convergence to enable telemonitoring. This approach uses CloudView Exalead as a search platform that offers access to information present in the infrastructural level for search based application online and at the enterprise level. Cirani et al. proposed a fog node and IoT hub, distributed on the edge of multiple networks to enhance network capability by implementing border router, cross-proxy, cache, and resource directory. IoT operates at both the link layer and application layer to enable resource discovery and seamless interactions among applications. Table 1 summarizes the features associated with fog computing, cloud computing, and IoT.

III. PROPOSED FOG COMPUTING APPLICATION TAXONOMY

Different fog computing applications have been suggested in the literature, therefore, in this section, we present a taxonomy of such applications. Luan et al. described fog as a surrogate of cloud that can be used to deliver location-based service application to mobile device users (e.g., showcasing its application in

TABLE 1. Summary of fog computing, cloud computing, and IoT features

Features	Fog computing	Cloud computing	Internet of Things
Target User	Mobile users	General Internet users	Stationary and mobile devices
Number of server nodes	Large	Few	Large
Architecture	Distributed	Centralised	Dense and distributed
Service Type	Localized information service limited to specific deployment location.	Global information collected worldwide	Information specific to the end device
Working Environment	Outdoors (i.e., streets, fields, tracks) or Indoor (i.e., home, malls, restaurants)	Indoors with massive space and ventilation	Outdoor and Indoor
Location awareness	Yes	No	Yes
Real-time interactions	Supported	Supported	Supported
Mobility	Supported	Limited Support	Supported
Big data and duration of storage	Short duration as it transmits big data	Months and years as it manages big data	Transient as it is the source of big data.
Major service provider	Cisco IOx	Amazon, Microsoft, IBM	ARM, Atmel, Bosch

shopping centers, parklands, inter-state bus, and vehicular fog computing networks). Demonstrated the role of fog computing in three scenarios, namely: connected vehicle, smart grid and wireless sensor and actuator networks. Dsouza et al. used the Smart Transport System (STS) as a use case, where STSs are heterogeneous distributed systems designed to constantly monitor traffic activities and transmit data between commuters and smart devices in real-time to pre-empt traffic and safeguard commuters. Demonstrated the application of fog computing in healthcare, highly latency intolerant augmented reality domain and its use for improving website performance by caching and pre-processing. Saharan and Kumar identified four areas of fog computing’s application, namely: wireless and actuator networks, smart grid, smart traffic lights and connected vehicles, and IoT. proposed a hybrid environment service orchestration that provides resilient and trustworthy fog computing service beyond the 5G network. In our taxonomy, we categorize fog computing applications into real-time and near real-time applications – see Fig. 2. Fog computing can also be introduced in a network (for non-real-time application) to reduce the amount of traffic in the core; however, this is beyond the scope of this work. Real-time applications are low-latency and function within a pre-defined timeframe which user senses as immediate or current. Near real-time applications, on the other hand, are those that are subject to time delay introduced by data processing or network transmission between the moment

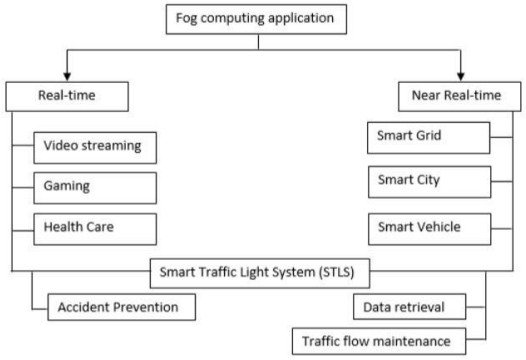

FIGURE 2. Proposed fog computing application taxonomy.

an event occurs and the use of the processed data. Near real-time is often determined by subtracting the current time from the processing time that is nearly the time of the live event. In this section, we present popular use cases of both real-time and non-real-time applications.

A. REAL-TIME USE CASES

1) VIDEO STREAMING

Transmissions of video applications and services are more efficient in a fog computing implementation, due to the capability of fog computing to provide location awareness, low latency, mobility, and real-time analytics. Several smart devices support smart surveillance that can be used by law enforcement officers to display live video streams of events of interest. For example, Hong et al. described a video surveillance application that requires a three-level hierarchy system to perform motion detection with smart camera, face recognition with fog computing instances, and identity aggregation with cloud computing instances. proposed Aqua computing, inspired from water cycle, which can take the form of either fog or cloud computing. The proposed architecture consists of clones placed at the edge of the network that serve end users in a video streaming scenario to act as a buffer. used fog computing to transform video applications and services to support on-demand video delivery. Such an approach enhances interactions in a virtual desktop infrastructure system and provides real-time video analytics for a surveillance camera. Other potential benefits of deploying fog computing to improve video streaming performance such as intelligent caching and adaptive streaming were also highlighted. identified key requirements of fog computing that complements cloud computing to support an intelligent network node. This helps to improve the quality of transmitted video by ensuring an intelligent soft handoff of mobile user and radio-aware resource management.

2) GAMING

The advent of cloud computing has provided a platform for computer gaming without users (players) worrying about hardware requirements. Cloud gaming providers in recent times have been rapidly expanding or leveraging cloud infrastructure to provide game-on-demand (GoD) service to users over the Internet. It is offered remotely by enabling an interactive gaming that can be accessed and decoded by end devices such as smartphones or tablets. Wang and Dey described a cloud server based mobile gaming approach, cloud mobile gaming, where most of the workload for executing the game engine are placed on the cloud server. The mobile device only sends and receives user gaming commands to and from the servers. identified faster response time and higher QoS as key goals to be achieved in ensuring high gaming QoE. Due to the stringent requirements of gaming, cloud gaming is inherently susceptible to latency due to game graphics being rendered online. investigated how the response latency in cloud gaming would affect user experience and how it varies between games. Then, a model was developed on how to predict the real-time strictness of a game based on players' input and game dynamics.

Having established the impact of latency on cloud gaming and the inability of cloud to meet the stringent latency requirements, proposed a new hybrid platform by extending the existing cloud infrastructure and deploying more diverse geographically distributed devices equipped with specialized resources. To guarantee a high QoE in cloud gaming due to the high popularity of Massively Multiplayer Online Gaming (MMOG), proposed a lightweight system, which consists of super nodes that extend video games to nearby players to significantly reduce latency and bandwidth consumption. A receiver-driven encoding rate adaptation was also proposed to increase the playback continuity and deadline-driven buffer scheduling strategy. The experimental result obtained from PlanetLab and PeerSim demonstrated the

efficiency and effectiveness of the system deployment.

3) HEALTHCARE

IoT applications have provided a structured approach towards improving our health care services. This is achieved by deploying ubiquitous monitoring systems and transmitting the data to fog devices in real-time before sending the information to the cloud for further analysis and diagnosis. utilized fog computing as a smart gateway to provide sophisticated techniques and services such as distributed storage and embedded data mining. A case study of electrocardiogram feature extraction that plays a vital role in the diagnosis of cardiac diseases was presented. The experimental result suggested that deploying fog computing achieves a low latency and real-time response with more than 90% bandwidth efficiency. Persuasive health monitoring is one of the key application areas of biomedical big data research for making early predictions to support smart healthcare decision making. a real-time fall detection algorithm, U-Fall, which consists of three major modules, front-end, back-end and communication module. Both front-end and back-end make independent

detection results. However, a collaborative detection will increase the accuracy and reduce the false alarm rate. An experiment demonstrating the use of the U-Fall algorithm in fog computing that automatically detects pervasive fall during health monitoring to mitigate stroke was presented. Results obtained suggested that a high sensitivity and specificity was achieved. Similar to the work in, FAST, a distributed analytics system based on fog computing to monitor and mitigate stroke, was proposed in.

In order to facilitate easy access to healthcare service for the elderly, a body sensor network in fog computing was proposed in. The fog computing gateway is used to enhance the system by offering different services such as ECG feature extraction, distributed database and graphical interface to ensure obtained health data are visualized and diagnosed in real time. a smartphone-based service, Emergency Help Alert Mobile Cloud (E-HAMC), which uses fog services for pre-processing and offloading purposes to provide an instant way of notifying relevant emergency department (e.g., ambulance) from the stored contact details. This service also sends the incident location to facilitate patient tracing. And evaluated the use of fog data in carrying out data mining and analytics on raw data collected from different wearable sensors used for telehealth applications. deployed fog computing as the intermediary layer between cloud and end users in their framework. A security solution, cloud access security broker (CASB), was also introduced as an integral part of health fog to implement certain security policies.

4) SMART TRAFFIC LIGHT SYSTEM (STLS)

Smart traffic lights interact locally with a number of sensor nodes to detect the presence of cyclists, bikers or pedestrians, as well as estimating the speed and distance of approaching vehicles. This information can be used to prevent accidents by sending early warning signals to approaching vehicles. described the use of video camera that senses the presence of an ambulance flashing light during an emergency to automatically change street lights and allow the emergency vehicle to pass through traffic. identified three major goals of STLS, namely: accident prevention, steady traffic flow maintenance, and retrieval of relevant data to evaluate and improve the system. Accident prevention is a real-time process, while traffic flow and data retrieval are regarded as near real-time and batch processes. Wireless access points and smart traffic light units are deployed along the roadside to provide communication such as vehicle-to-vehicle, vehicle to access point, access point to access point (see Fig. 3).

B. NEAR REAL-TIME USE CASES

1) SMART GRIDS

The current call for smart grids can be linked to the fact that the present-day energy demands have outpaced the rate

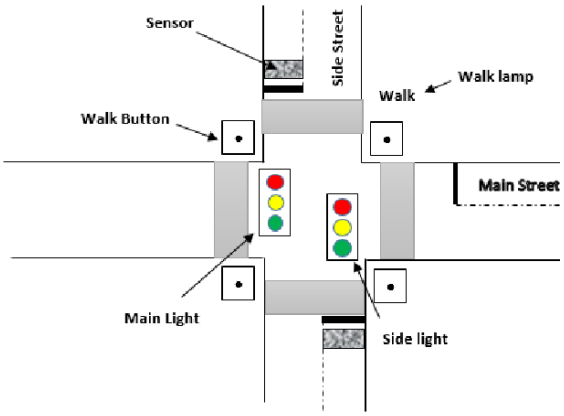

FIGURE 3. Smart Traffic Light System.

at which energy is generated by conventional methods as well as the need to reduce gas emission to control or curtail climate change. A cloud-assisted remote sensing approach to measure and collect smart grid operational information to enable seamless integration and automation of smart grid components. Cloud computing feature that uses a centralized demand response scheme, where customers and suppliers communicate directly with the cloud has proven to be bandwidth inefficient. Therefore, a distributed approach by presenting a macro-grid and micro-grid to act as fog devices. Customers communicate with the nearby fog devices rather than the remote cloud. Fog devices, on the other hand, communicate frequently with the customers and occasionally with the cloud. presented a Cyber-Physical Energy System (CPES) to improve the efficiency, reliability and performance of power grid by managing demand and supply dynamics intelligently. A prototype of this was implemented in fog computing platform to support interoperability, scalability and remote monitoring.

2) SMART CITIES

A smart city is one key IoT application that ranges from smart traffic management to energy management of buildings, etc. The smart city concept has drawn great interest from both science and engineering sectors, and from both research and practitioner communities, as a means to overcome challenges associated with rapid urban growth. described smart city as a city that is vastly controlled and made up of ubiquitous computing whose economy and governance are driven by innovation and creativity. However, some of these IOT applications and devices in a smart city require high computation and storage capacities, and pose interoperability challenges. For example, identified the complexity associated with a cloud centralized architecture involving smart city that consists of road traffic control, parking lot management and environmental monitoring over a distributed territory. identified fog computing that is close to the edge of the network as the solution as well as integrating all components in a unified platform to enable smart home applications with elastic resources. Smart city was described in as a public space in the edge that optimizes energy consumption and improve the quality of life of citizens. In the work of a hierarchical distributed fog computing that supports a huge number of infrastructural component and services for future smart cities was presented. A smart pipeline monitoring system use case was discussed, which is based on fiber optic sensors. Sequential learning algorithm was used to detect events threatening pipeline safety.

3) SMART VEHICLES

The advent of mobile cloud computing has necessitated the study of its agents such as vehicles, robots and humans that interact together to sense the environment, process the data and transmit the results. described connected vehicle that communicates with their internal and external environment such as Vehicle-to-Vehicle (V2V), Vehicle-to-Sensor on-board (V2S), Vehicle-to-Road infrastructure (V2R) and Vehicle-to-Internet (V2I). Vehicle cloud has been identified as the leading application that facilitates safe driving, urban sensing, content distribution and intelligent transportation to render benefits such as sensing urban congestion and collaborative reconstruction of footage in a crime scene.

A significant attribute of vehicular cloud as compared to the Internet cloud is its reliance on the sensors they carry, rather than cloud computing resources. described a vehicular fog computing that utilizes vehicles as an infrastructure for computing and communication that involves the collaboration of many end-user clients or nearuser edge devices. described a vehicular fog as the equivalent of Internet cloud in vehicles and the core system environment that will enhance autonomous driving. VANET is a mobile ad-hoc network that uses vehicles as mobile nodes. proposed a new architecture for VANET by combing SDN and fog computing to cater for future VANET demands and support surveillance services by considering resource manager and fog orchestration models. presented a solution to insufficient parking space as a result of rapidly increasing number of vehicles by proposing a shared parking model in a vehicular network using both fog and cloud environments. Simulation results indicated a high efficiency and reliability in determining vacant parking slot.

IV. FOG COMPUTING SECURITY AND PRIVACY CHALLENGES

Security assessment of fog computing can be guided by the confidentiality, integrity and availability (CIA) triad model, which are the critical components that must be considered during the design and deployment of a system. While confidentiality and integrity are closely related to data privacy, availability entails the ability to remotely access resources offered by cloud servers and fog nodes when needed. Apart from the security challenges fog computing inherited from the cloud, its heterogeneous feature and deployment location(s) at the edge of the network have made it susceptible to some additional challenges. Potential issues likely to be encountered with the deployment of fog computing identified by are authentication, access control, intrusion attack and privacy.predicted that the current security issues associated with a virtualized environment would be a potential security concern for fog devices hosting applications. identified challenges associated with hardware and platform standardization required for homogeneity to facilitate federation. demonstrated that a man-in-the-middle attack could compromise and replace a genuine gateway before inserting malicious codes into the system. In this section, we present an overview of security and privacy issues as applicable to the use cases.

A. SECURITY ISSUES IN FOG COMPUTING

The shareability and distributed feature of fog computing have made authentication a key issue when offered to a large number of end devices by front fog nodes. Security solutions proposed for cloud computing will not directly suit fog computing as its working surroundings may face threats that do not exist in a typical cloud deployment. Authentication takes place during the process of establishing a connection to ascertain the accessing rights and identity of a connecting node. identified authentication at different levels of the gateways as the main security issue in fog computing. Authentication and authorization issues in the context of smart grid and machine-to-machine communication for fog computing were presented in a chosen ciphertext attack (CCA) on fog computing and proposed a solution by first presenting the CCA security model of OD-ABE (attributed-based encryption with outsourced decryption) prior to describing their CCA-secure OD-ABE scheme. presented a threat model by reviewing the scope and nature of potential attacks. They identified the most important asset at the edge, predicted possible attacks that can be directed towards such asset, and categorized potential target into network infrastructure, service infrastructure (edge data center and core infrastructure), virtualized infrastructure and user devices. Different devices and communication elements deployed in fog computing range from wireless to Internet-connected mobile devices, etc. Therefore, the attacker can target any of these components. Denial of Service (DoS), man-in-the-middle attacks, and rogue gateway attacks were identified as possible attacks on network infrastructure, while service infrastructure at the edge data center can be exposed to physical damage, privacy leakage, privilege esca

TABLE II. THREAT MODEL DISTRIBUTION FOR FOG COMPUTING COMPONENT (ADAPTED FROM [64])

Fog components / Security issues	Network Infrastructure	Service Infrastructure (edge datacentre)	Service Infrastructure (core infrastructure)	Virtualization infrastructure	User Devices
DoS	✓			✓	
Man-in-the-middle	✓				
Rogue component (i.e., datacentre, gateway or infrastructure)	✓	✓	✓		
Physical damage		✓			
Privacy leakage		✓	✓	✓	
Privilege escalation		✓		✓	
Service or VM manipulation		✓	✓	✓	✓
Misuse of resources				✓	
Injection of information					✓

manipulation and rogue infrastructure have been identified as possible security threats. Virtualized infrastructure within the core of all edge data center is vulnerable to misuse and exploits associated with DoS, primary leakage, privilege escalation and VM manipulation. Finally, user devices can be subjected to security issues with regards to injection of information and service manipulation. Table 2 summarizes the threat model distribution in fog computing component as identified in. To mitigate some of the security issues presented, strategies such as multicast authentication using Public Key Infrastructure (PKI) and deployment of intrusion detection system (IDS) [4] were suggested. A decoy information technology technique was proposed by to withstand malicious insiders by disguising information to prevent attackers from identifying customer's real sensitive data.

B. PRIVACY IN FOG COMPUTING

Defined privacy as the protection of data-in-transit from passive attacks to ensure sensitive information

are not accessed or disclosed to an unauthorized person. Typical of most public remote storage facilities, sensitive and personal information outsourced to or stored in cloud computing could be compromised or leaked. In addition, researchers have also raised concerns about the far-reaching arm of legislation such as the PATRIOT Act for U.S.-based cloud service provider. Fog computing, on the other hand, presents a higher privacy risk as the deployment is extended to the edge of the network. explained that privacy risks such as data privacy, usage privacy and location privacy exist in the fog computing nodes located in the vicinity of the end users, and these nodes are more susceptible to information theft when compared with cloud servers located at the core of the network.

Identified from existing literature that sensor networks are vulnerable to content-based privacy threats and context-based privacy threats. They then proposed a redundant fog loop to preserve the location privacy of the source node to confuse the adversary from accurately determining the real source node. To mitigate malicious eavesdropping on data-in-transmit, proposed a fog friendly framework based on public key encryption with an infrequent key update to avoid high overhead. Also proposed the use of attributebased encryption and deployment of secure middleware for privacy-aware information sharing, with the aims of preventing service providers from accessing users' data without authorization. Privacy issues in smart grid were presented in, and a privacy-preserving aggregation scheme using multidimensional data aggregation approach based on homomorphic Paillier cryptography was proposed.

C) INFRASTRUCTURAL FAILURE IN FOG COMPUTING

To ensure availability of fog computing service and resources, the fog architecture must ensure reliability and resilience. discussed the reliability improvement of fog computing by periodically carrying out check-pointing to resume after failure and rescheduling failed tasks or replicating to exploit executing in parallel. Due to the dynamic nature of fog computing, check-pointing and rescheduling may not be a good fit as this may introduce some latency and cannot adapt to changes.

V. DISCUSSION

The adoption of fog computing has the potential to enhance QoE for real-time applications that are transmitted within a pre-defined timeframe. Fog computing's interoperability feature ensures wide support for different applications. Its interactions with cloud computing and IoT also ensure that location of fog devices at the edge is close to the source of the data to speed up processes and response to events. The data can be further (pre)processed and subsequently analyzed in the cloud. In this paper, we categorized the uses of fog computing deployment into real-time and near real-time applications. Batch applications, on the other hand, are handled by cloud computing. Our review shows that fog computing is an emerging research topic. Specifically, from an initial singledigit publication count in 2012 and 2013, the number of academic publications in fog computing have increased in 2015 and 2016, which is an indication of the increase interest in this topic. Typical of any new consumer technologies, security and privacy concerns are two key concerns in fog computing. For example, DDoS attacks while not new are one hard-to-mitigate attacks in fog and cloud computing.

VI. CONCLUSION AND FUTURERESEARCH

In this paper, we reviewed academic literature on the paradigm shift from cloud to fog computing published between January 2012 and December 2016. We then presented a taxonomy of different fog computing applications by grouping them into real-time and near real-time. The low-latency requirement of these applications necessitates the extension of the cloud to the edge of the network; thus, resulting in fog computing. Both cloud and fog computing are highly virtualized platforms that provide resources, such as computation, networking and storage. The requirements of high availability by end users motivates the design of the smart pre-copy live migration in Xen presented in this paper. The proposed approach estimates the downtime during the iterative pre-copy stage to determine whether to proceed to the stop and copy stage. This will guarantee a minimum downtime. Future work will include deploying the framework in a real-world or test environment, with the aims of validating and refining the framework.

Fog computing, being in its infancy stage, has a number of challenges due to its architectural design. For example, it is susceptible to trust and authentication issues due to its distributed feature. Cyber-attacks such as DDoS attacks can also be detrimental to fog computing's availability as the capacity of each fog node is limited. Therefore, there is a need for more research in the areas of authentication, access control and intrusion detection in fog computing.

Extending cloud to the edge of the network will involve deploying fog nodes close to the end users. This significantly increase the number of devices deployed which results in an increase in energy consumption. Therefore, effort should be expanded into promoting green computing to help reduce global warming.

ACKNOWLEDGEMENTS

The authors thank the three anonymous reviewers for providing constructive and generous feedback.

REFERENCES

[1] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, ''Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework,'' J. Netw. Comput. Appl., vol. 67, pp. 147–165, May 2016.

[2] M. Díaz, C. Martín, and B. Rubio, ''State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing,'' J. Netw. Comput. Appl., vol. 67, 99–117, May 2016.

[3] A. Botta, W. de Donato, V. Persico, and A. Pescapé, ''Integration of cloud computing and Internet of Things: A survey,'' Future Generat. Comput. Syst., vol. 56, pp. 684–700, Mar. 2016.

[4] S. Yi, Z. Qin, and Q. Li, ''Security and privacy issues of fog computing: A survey,'' in Proc. 10th Int. Conf. Wireless Algorithms, Syst., Appl. (WASA), Qufu, China, 2015, pp. 685–695.

[5] M. Aazam and E.-N. Huh, ''Fog computing and smart gateway based communication for Cloud of Things,'' in Proc. IEEE Int. Conf. Future Internet Things Cloud (FiCloud), Barcelona, Spain, Aug. 2014, pp. 464–470.

[6] V. Medina and J. M. García, ''A survey of migration mechanisms of virtual machines,'' ACM Comput. Surv., vol. 46, no. 3, 2014, Art. no. 30.

[7] A. Shribman and B. Hudzia, ''Pre-copy and post-copy VM live migration for memory intensive applications,'' in Euro-Par 2012: Parallel Processing Workshops (Lecture Notes in Computer Science). New York, NY, USA: Springer, 2012, pp. 539–547.

[8] U. Deshpande, Y. You, D. Chan, N. Bila, and K. Gopalan, ''Fast server deprovisioning through scatter-gather live migration of virtual machines,'' in Proc. 7th IEEE Int. Conf. Cloud Comput. (CLOUD), Anchorage, AK, USA, Jun./Jul. 2014, pp. 376–383.

[9] C. Jo, E. Gustafsson, J. Son, and B. Egger, ''Efficient live migration of virtual machines using shared storage,'' in Proc. 9th ACM SIGPLAN/SIGOPS Int. Conf. Virtual Execution Environ., Houston, TX, USA, 2013, pp. 41–50.

[10] M. Mishra, A. Das, P. Kulkarni, and A. Sahoo, ''Dynamic resource management using virtual machine migrations,'' IEEE Commun. Mag., vol. 50, no. 9, pp. 34–40, Sep. 2012.