A REVIEW ON SECURITY ISSUES AND SOLUTIONS OF FOG COMPUTING

Sk Mahaboob Basha,1 Gumma GopiKrishna2
1 Associate Professor, Department of Computer Science and Engineering, QIS College of Engineering & Technology
2 M.Tech., Scholar, Department of Computer Science and Engineering, QIS College of Engineering & Technology

ABSTRACT:

In contrast to the "cloud" era, the fog is a distributed computer network located at the outside limits of a company. This virtualized structure is the first fog system that can equal the amount of data, processing, and programming capabilities of similar fog platforms. While it is similar to cloud technology on a basic level, it varies since it is distributed. In contrast, Fog frameworks can process large amounts of data on-premise, are entirely adaptable, and can be deployed on many types of infrastructure. The Fog stage, as described above, is a fantastic option for high-priority tasks with strict time constraints. For example, IoT devices are essential for handling vast amounts of information quickly. These many applications for enhanced security concerning information, virtualisation, segregation, organisation, malware, and monitoring make wide-ranging use of it. This document examines current research on the security risks in Fog computing systems. A broader range of audit options was added, including such technologies as Edge computing, Cloudlets, and Micro-server farms. The majority of Fog applications are driven by the pursuit of customer satisfaction and business requirements, while security considerations are frequently ignored or relegated to an afterthought. This study also considers the impact of security problems and proposed security frameworks, providing future security-related guidance to those responsible for planning, designing, and implementing Fog architectures.

I. INTRODUCTION:

Cloud-based setups [1], which use cloud communication organisations to check and regulate managed devices, are becoming more popular. [2] introduced a fog concept for vehicle control called Control as a Service (CaaS). The developers of [3] described their system as a motion tracking platform. This concept also takes into account contemporary robots' higher-level control (e.g., anticipation of movement). Rapyuta is PaaS for cloud industrial visualization tools through Platform as a Service (PaaS). One of the main advantages of these designs is their capacity to be adapted, flexible, and more productive than conventional frameworks [6]. A cloud architecture is impractical for lower-layer control (e.g., servo control of actuators) because local processing is needed, and lesser control devices have long latency. [7], [8]. Fog computing [9] may help solve this problem, which is characterised by a decentralised computing architecture with a fog layer in the middle. By using fog virtualization arrangement, the regulatory agency doesn't need to be implemented locally, and control-system managers may remotely monitor plant conditions and effectively modify the control legislation. Furthermore, the fog totals also eliminate dirty information to assist with cloud-based investigations [10]. The instance of the cloud, according to Fog computing research, faces a multitude of potential protection problems, including [11]–[13]. Since physical frameworks may directly impact real-world circumstances, attacks on such systems are more damaging than attacks on data frameworks [14, 15]. If the framework's safety measures are not thoroughly implemented, then enemies will be able to eavesdrop, attack, and misrepresent it. The people who created [16] proved that controllers are a hazard by creating actual attacks that fool the regulators. Muddling regulator gains and obscuring signal transmissions are fundamental necessities. A combination of cryptography and control theory known as Encrypted Control [17] may be effective in the effort to secure control frameworks by lowering the risk of snooping attacks. Zero-day exploits are used in the future to conduct more severe attacks, such as listening in, to get data on control frameworks [15]. In ElGamal-based systems administration that encrypt regulatory limits, device data, and published sources, input data is retrieved from encoded sensing data and standard data without decryption. Another method of preventing replay attacks and regulator/sign misdirection attacks is to encrypt control [19]. A novel homomorphic encryption scheme known as the encrypted control framework was developed in [21], [22], using Paillier encryption. The inventors of [23] used fully homomorphic encryption in their design of a sign covering method. A safety feature utilised in charge frameworks is

www.turkjphysiotherrehabil.org
homomorphic encryption, as it has been shown before. While it may be true, the regulator boundaries shouldn't be confused with extra substance homomorphic encryption because of the fact that encryption between two information can't be carried out in ciphertext. Moreover, public key encryption algorithms that use the extra material and those that are symmetric in nature both need a great deal of computing power. Because of this, lower-layer mechanical structures are incapable of using encryption schemes of this kind.

This article discusses the development of a fog technology management system that has the goal of replacing existing control systems, such as the one shown in Figure 1. The PID regulator was encrypted using ElGamal encryption in the framework to help with position control of a straight stage. While the practicality and properties of encrypted control frameworks were previously tested on Raspberry Pi [25], [26], and have even been deemed possible, a lack of validity testing was performed in realistic environments, for example, an environment that utilises current hardware and networks. The manufacturing lines will benefit from this letter since it shows the main operation of the encrypted control framework. Furthermore, permanent property damages are accepted. Stage position and PID gains are among the many aspects of the built framework that are encrypted. Also, ciphertext control inputs are decided by the fog, without the ciphertext being decoded. Regardless of whether the regulator uses encryption, the exploratory results demonstrate that the suggested control framework provides reliability and controlling execution.

II. RELATED WORK

The Cisco Fog perspective may be seen broadly and holistically as the enabling impact of many innovative tools. It is capable of incorporating, multiplying, and influencing a few enhanced features, for example, quick inspection, interoperable across devices, increased response time, integrated or device executives, reduced bandwidth consumption, profitable power utilisation, and device perception. Similar techniques, such as fog computing, are also being used to increase the usability and potential of Cloud platforms [16]. With such a broad scope, the Fog and related technologies such as Edge computing, Cloud resources, and Micro-data centres are vulnerable to attacks that violate Confidential, Identity, and Reliability (CIA) [17]. The Security Of Cloud [18] has identified twelve fundamental security problems, which are addressed by various experts, such as [6, 19, 20]. These problems directly influence the distributed computing model's circulating, shared, and on-demand character. As a virtualized environment, similar to Cloud, the Fog platform is susceptible to comparable dangers.

• Advanced Persistent Threats (APTs) are cyber-attacks designed to breach an institution's structure in order to steal data and safeguard innovation.

• Access Control Issues (ACI) may result in hopeless management, with any unauthorised person gaining access to information and credentials necessary to install programs and modify designs.

• Account Hijacking (AH) occurs when an attacker attempts to seize control of a user's account for nefarious purposes. Phishing is a technique that may be used to hijack an account.
• Denial of Service (DoS) attacks prohibit legitimate users from accessing a system's resources (data and applications) by overloading the system's finite resources.

• Data Breach (DB) occurs when an attacker delivers or steals sensitive, protected, or confidential data.

• Data Loss (DL) refers to the process through which data is accidentally (or deliberately) deleted from a system. This does not have to be the consequence of a cyberattack; it may occur as a result of a natural disaster.

• APIs that are insecure (IA) Numerous cloud/fog vendors make Application Programming Interfaces (APIs) available for client usage. Security of these APIs is essential to the security of any applications that are executed.

• System and Application Vulnerabilities (SAV) are exploitable flaws that arise as a result of software promotion configuration errors and may be used by an attacker to infiltrate and breach a system.

• A malicious insider (MI) is a person who has been granted authorised access to a network or system but has decided to behave maliciously.

• Inadequate Due Diligence (IDD) often occurs when an organisation accelerates the acceptance, planning, and implementation of any system.

• Abuse and Nefarious Utilize (ANU) often occurs when assets are made available for free and malevolent individuals use the assets to engage in harmful activity.

• Shared Technology Issues (STI) occur as a result of frameworks, platforms, or applications being shared. For instance, basic equipment components may not have been designed with solid disengagement characteristics in mind.

III. FOG COMPUTING AND TECHNOLOGIES OF A SIMILAR KIND

Although Cisco coined the phrase "fog computing," comparable concepts have been studied and developed by other groups. The following overview delves into three such technologies, highlighting some of their critical distinctions from fog systems. For edge computing, [21] and [22] provide a much more moment in time connection.

i) Edge Computing conducts minimal processing on the device via the use of Programmable Automation Controllers (PACs) [23], which are capable of handling data processing, storage, and communication [22]. It is superior than fog computing in that it eliminates weak points and increases the freedom of each device. Regardless, a comparable component makes it difficult to monitor and gather data in large-scale networks, for example, the Internet of Things [24].

ii) Cloudlet is the intermediate tier of the three-tier hierarchy "mobile device - cloudlet - cloud". Cloudlet has four distinguishing characteristics: it is fully self-contained, has sufficient compute power, has a short start-to-finish idle time, and builds on existing Cloud technologies [25]. Cloudlet is distinct from fog computing in that application virtualization is incompatible with the environment, consumes more resources, and cannot operate in an offline state, as shown by [26, 27].

iii) Micro-data focus [28] is a small but very valuable data storage area that supports many workers and is prepared to provide a large number of virtual computers. Numerous systems, like fog computing, may benefit from micro data habitats because they reduce idleness, improve dependability, are usually small, include intrinsic security protocols, reduce bandwidth consumption via compression, and can accommodate a variety of novel services.

Fog Applications

By providing Network Level Virtualization (NLV) and continuous data services, fog computing enables users to assume complete management and leadership of the network. OpenPipe [27] implements NLV using a hybrid architecture that includes a virtual Software Defined Network (SDN) controller (located in the Cloud), virtual neighbourhood controllers (located in the Fog), virtual radio assets (for distant communication), and a virtual cloud worker. The SDN controller is a global, intelligent module that manages the whole network. Nearby controllers route data to an SDN controller, which meets the requirements of ongoing and idleness-sensitive applications by determining whether to process data on the neighbourhood or SDN controller based on user
strategy. To connect SDN and neighbourhood controllers, the Extended OpenFlow (exOF) convention is utilised. The suggested system's benefits include load balancing, rapid handover without sacrificing Quality of Service (QoS), reduced energy consumption, decreased inerntance, and minimal network overhead. Similarly, Fog hubs may reduce and restructure web items for optimal performance. Additionally, various convincing research considerations [30–32] have been presented for optimising SDN and virtual machine performance through the use of cloudlets, which enable dynamic VM combination, single-jump low-idleness remote access, and enable VM overlays to load only the distinction between the desired custom VM and its base VM. These components were developed by Carnegie Mellon University as part of a project named Elijah, which is available on Github vault [33].

**Optimization of the web**

Cisco scientists are experimenting with fog computing to boost the performance of websites [37]. Rather of repeating the process for each HTTP request for content, templates, redirections, scripts, and images, Fog hubs may assist in bringing, aggregating, and executing them on the go. Additionally, fog hubs may differentiate users according on their MAC addresses or treats, monitor user requests, store documents, and identify the surrounding network's state. Additionally, it is possible to include feedback scripts inside a web page to monitor the user program's delivery pace. The feedback script communicates directly with the Fog hubs, informing them of the user's graphical objective, the current area gathering (if remote), and network congestion. In a related study, fog computing was shown to significantly reduce the reaction season of a cloud-based temperature forecast system [31]. Due to Fog technologies, forecast idleness was reduced from 5 to 1.5 seconds, web page inactivity was reduced from 8 to 3 seconds, and web traffic throughput was increased from 75 to 10 Kbps. Another application of fog computing is discussed in [30], where IP addresses may be replaced with identities in the Internet of Everything (IoE), using the Information Centric Networking (ICN) architecture and updated reserve elements. Fog hubs may manage resources (for example, by using the Steiner Tree Based Optimal Resource Caching Scheme for Fog Computing [40]), with the added benefit of enabling heterogeneous devices and calculating, analyzing, and storing at the network's edges. Another simple technique [41] is to utilise edge computing to generate user-explicit pages by simulating the application code among many edge workers. The edge workers are prepared to maintain multiple copies of data, to conduct content-aware data reserving and to store content-dazzled data.

**Establishment of 5G mobile networks**

Mobile apps have become an integral part of modern life, and their focused use has resulted in an exponential increase in mobile data usage, necessitating the creation of 5G mobile networks. Not only can fog computing improve the service quality of a 5G network, but it may also aid in forecasting future mobile user needs [14]. Innately, Fog centres are dispersed within users' vicinity, a feature that reduces idleness and establishes adjacent restricted relationships.

**Enhancing smart metre throughput**

By transmitting Smart Grids, a large amount of data from smart metres is collected, processed, and sent through data gathering units (DAU). Meter data is used by the board system (MDMS) to predict future energy needs. As shown in [5, the data collecting measure occupies a significant portion of the day owing to the equipment's limited bandwidth capacity, but may be enhanced with the use of fog computing. To begin, a fog-based switch is connected to smart metres, which combine the data collected from all sub-meters within a specified time period.

**Data collection and pre-processing**

For Android smartwatches paired with a smart tablet, the FIT (Fog Interface for Tablets) [74] collects, records, and cycles voice data from Parkinson's sufferers. Instead of transmitting the whole sound data, the FIT focuses highlights such as loudness, short timescale energy, zero-intersection rate, and horrible speech and cloud ships for long-distance research. The programme was applied to six patients, allowing for large amounts of sound data to be processed in a short amount of time, thanks to its use of Fog computing. A different paper offers a novel programming framework and framework for edge-based portable apps, which may help the application developer to create portable applications that are adaptive and customizable. As the system processes data before transmission, it also addresses geo-specific considerations for applications that need information to remain safe when it is idle.

**Recent Fog computing security solutions**

www.turkiphysiotherrehabil.org
In the previous sections, we've established that the inclusion of Fog functionality between end-clients and Cloud frameworks introduces yet another point of vulnerability, which may be used for malicious purposes. Unlike for cloud frameworks, Fog computing lacks security certifications and standards. Additionally, a Fog platform may be described as having somewhat less complex computational resources due of their nature, and thus it is difficult to perform a complete deployment of security solutions that can identify and avert sophisticated, targeted, and distributed attacks. Because of high data throughput and the likelihood of securing sensitive data from both cloud and IoT devices, this objective is appealing to digital criminals. Moreover, it is more accessible than cloud frameworks, depending on the organization's configuration and physical location, which increases the risk of an attack. Many Fog computing applications and similar advancements that have been detailed in the "Related work - contemporary fog applications" portion of this paper focus on functionality. In many cases, it has been discovered that security measures that might protect against these risks are ignored. A potential explanation for this is because there are very few research solutions available to help identify and prevent malicious attacks on Fog platforms, since Fog-specific security problems are still in their infancy. Beneath this are explanations of certain frameworks.

**Fog computing that respects privacy**

Research on keeping information safe in sensor-fog networks [15] has shown the following methods to protect sensor data between the end-client device and the Fog infrastructure:

- They gather sensor data and concentrate highlights;
- Fuzzing of data by inserting Gaussian commotion in data at a certain degree of fluctuation to bring down the shot at eavesdropping and sniffing assaults;
- Segregation by splitting data into squares and shuffling them to keep away from Man-in-the-Middle (MITM) assaults;
- Implementing Public Key Infrastructure for encrypting every data block; and
- Send isolated data to Fog hub, where data bundles are unscrambled and re-requested.

**Preventing the theft of insider data**

A separate study [6] discovered a way to safeguard information from backstabbing employees by combining features of Fog and cloud computing. It combines detection and prevention techniques to counter the threats of malpractice. If any user account displays unusual behaviour, such increased browsing of different records at unusual times, the framework will mark the admission as suspicious and flag the relevant user. To mislead and acquire the malicious insider, imitation may include counterfeit records, honey files, honeypots, and other types of baiting data. This area of study is vital since it offers clues as to what measures may be taken to prevent the theft of data. This system can detect abnormal behaviour more accurately than 90% of cases. Even yet, the experiment is done with a limited data set. Additionally, eighteen students from one institution were tested over the course of four days. After this, the reliability of the results they promise is debatable and uncertain. In order to enhance their method, it should be expanded in population size and the experiment conducted over a longer period of time [9]. The computing requirements of this method are not stated, either. The article does not detail the data storage capacity, memory requirements, or processing time. In conventional customer worker engineering, such behaviour profiling techniques are done when resources are freely available. This technique is difficult to apply to a Fog hub without impacting centre functioning. The process may be made even better by first studying and choosing the viable machine learning methods and the necessary training data required for doing data analysis. This is significant since there are so many clients and data involved. There are a variety of methods for identifying and reducing the risk of malicious insiders in various works [9, 29], including the use of comparative behaviour profiling and false tactics. If you use Cloud resources in the conduct profiling, monitoring, and client matching process, you eliminate the risk of theft without having to expose confidential data. Further, these activities will take place on-premises and execute faster because to reduced bandwidth inertia.

**IV. CONCLUSION**

As you can see in the previous sections, the individual security solutions proposed for the CIA of Fog technology are insufficient to secure it. The traditional security space of Fog systems are not sufficient to address the
demands of today's cutting-edge safety requirements. The writing addresses integrity of the information, insider threat, asset access policy, client authentication, and encryption in the short term. Regardless, it is imperative to establish the fundamental elements resulting from the shared invention, client account handling, administrative data, data devastation/breach, inadequate weakness patching, and disarmed framework keeping an eye on. Any of these risks may provide aggressors the opportunity to jeopardise the CIA of Fog and the linked systems. Reusing other technologies' established security procedures may be one answer to these problems. Since they imitate Cloud, the Fog platform components and their activities are not entirely novel (as expressed in "Introduction" section). To perform the test successfully, researchers will have to join and tune the security gauges, as well as apply them in line with the needs of the Fog platform. Any Fog framework's security is assured by utilising the security mechanisms that have been fully tested.

REFERENCES: