Vol.2, No.5, Page 482- 491, 2024 https://doi.org/10.59628/jast.v2i5.1128 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

A Review for Fog-Cloud Security: Aspects, Attacks, Solutions, and Trends

Mohammed AL-Riyashi[1] *, Ammar T. Zahary[1] and Fatek Saeed[2]

[1]**Department of Information Technology, Faculty of Computer Science and IT, Sana'a University, Sana'a, Yemen.,**
[2]**Department of Cybersecurity, Faculty of Engineering and IT, Amran University, Amran, Yemen.**

*Corresponding author: Mohamed.AL-Riyashi@su.edu.ye and ict1979 @mail.com

Abstract

Nowadays, different structures are support clients to hosting their data via cloud computing. A fog-cloud is a part of cloud computing that decentralized computing pattern to get computing assets closer to the edge of the network, where data processed and analysed at the edge of the network, rather than being transmitted to joined data centre for handling, moreover, the Fog nodes could mobilization and compress web things for optimal speed. Numerous of normal techniques for protect Fog computing recently become ineffective because vulnerabilities and additional risks such as Man in the Middle (MitM), Ransomware, and Denial of the Service (DoS). To keep their security procedures, Fog systems of the forthcoming will need capabilities solution of artificial intelligence especially machine learning and deep learning. The emerging technology of fog cloud Paradigm is to must a nonstop updating and up-to-date security model. We here try to get out the core useful knowledge about Fog cloud system and their issues and many of security application in one figure No. 1.

Article Info

Keywords:
Fog-cloud Computing,Cybersecurity,Machin Learning,IoT,Deep Learning.

Article History:
Received: 16-July-2024,
Revised: 29-July-2024,
Accepted: 16-October-2024,
Available online: 31 October 2024.

1. INTRODUCTION

The admiration and use of cloud computing is growing so fast. Many companies invest in the cloud industry to use it for themselves or to afford it as a service to customers. One of the consequences of cloud development is the emergence of several security issues in both the customer ground machines and the tenants/providers. One method to protect the cloud is to use Machine Learning (ML). ML techniques have been used in a variety of ways to prevent or detect attacks and security vulnerabilities in cloud system [1]. Fog Computing requires looked as important part of cloud computing via produces proficient infrastructure to provide IoT. Where fog computing doing as third party supports the end users' orders of local processing and decrease delays in communication as latency time between the cloud and the end-users through fog machines. Then, the filtering the arriving network traffic on the fog machines is massive consideration. This equipment is exposed to crime threats. Everything such as health data, commercial, and government information transfers over fog devices. Hackers sending malicious data packets for affect those devices. It is necessary to detect these intrusions to offer protection to the customer and efficient service. Therefore, reliable Intrusion Detection System (IDS) is the basic stone to safe operational void effecting productivity of fog [2].

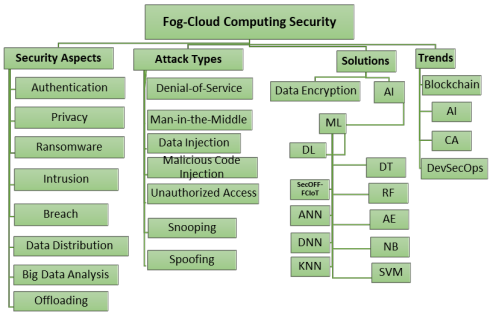

Figure 1. General Fog Computing Security.

2. SECURITY ASPECTS OF FOG-CLOUD COMPUTING

The Fog Ideas are Cloud computing construction extended style in form of fog computing, that contracts with edge network, consequently, permits a novel sequence of application and services. Fog computing important features are:

- Heterogeneity, mobility, extended number of nodes.
- Place concerns and low latency.
- Wide physical sharing.
- Principal Wireless access role as top-tier.
- Robust existence for instants programs and high-level streaming ability [3].

Furthermore, in 2012 the big name of Technology Company named Cisco, suggested first concept of Fog computing (FC) for support procedures of computing for the IoT machine's resources- constrained and saving the information conducted by IoT machines which storage affords closely to end- users. Moreover, the Fog comparing to the Cloud facing possibility higher attacks during massive computation and right-produced security assessments. In fact the FC has limited of storage size and in occupation power, then no way to take place of Cloud computing but it used as a bridge amid Cloud computing and IoT equipment. However, the FC needs own private security applications and privacy protection tools due to its properties and characteristics that diverge than cloud with equal efficiency [4] In addition, the most security aspects and have rapid concerns in Fog-cloud are: Authentication, Privacy, Denial of Service, Ransomware, Intrusion, and Data Leak Breach, as mentioned below:

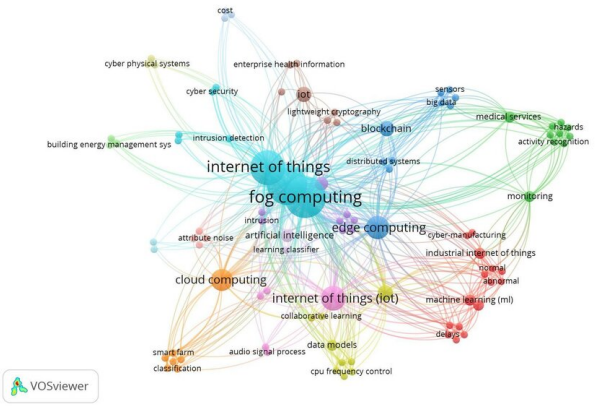

Figure 2. Fog computing-machine learning-IoT publication analysis from 2013 to 2023[5].

2.1. Authentication

Authentication is assumed as the principal security matters of Fog Computing due to the Fog provide several services to a massive number of (IoT) devices. Authentication must be practical at diverse levels throughout communication between (IoT) devices and Fog nodes. Classical authentication systems such as certificates and public key infrastructure (PKI) will not be usefully because resource- constrained IoT devices (e.g., storage, processing, and power) [4]. The decentralized network means that there needs to be an identity authentication system to possess the environments presence secured. The blockchain has constructed a new reliable huge scale support method based on the information Internet to solve the trust challenge of provide the digital economy. Blockchain new knowledge has the features needed by several application situations similar credibility and transparency, tamper prevent, traceability, and decentralization. Applications have been extended from the financial field to government services, supply chain management, energy copyright storage, and Internet of Things [6].

2.2. Privacy

The users stored data should kept privately in cloud environments where concerned a sensitive information and becomes interested issue from customer view side. The Fog Computing (FC) has its especial landscape and features, solutions doable for security and privacy-preserving in the Cloud may not be achievable in the Fog with equal efficiency. Hence, FC must have unique methods and tools to preserve the security and privacy of IoT equipment linked to it [4]. Though the increasing fame of fog services, guaranteeing the privacy and security of contents are maintain a key issue. DDoS attack is a famous risk amid the safety worries and significant investigation problem when speaking essentially around data protection in fog computing system [7].

2.3. Ransomware

Recently, ransomware become a famous type of cyber-attack which intention to disrupt the availability of a network or service by overwhelming it with traffic from multiple sources. In a fog computing system, DDoS attacks can be particularly challenging to defend against, as the decentralized nature of the system means that attacks can potentially originate from anywhere within the network [8]. Ransomware is a particular blackmail threat which exploits cryptography to hijack the objective's machine and thus order ransom payment for disinfecting the compromised device. Recently, due to financial profits, these types of extorting attacks have been developing too rapidly and affecting high monetary losses to persons and corporations. Where first ransomware attack was

detected in 1989, it identified as Acquired Immunodeficiency Syndrome (AIDS) or Trojan-PC Cyborg. Hence, the high incomes are motivating hackers to escalate the creation of new variations to avoid the security defence of the present schemes. While zero-day vulnerabilities are exploited in several of threats, but when combined with ransomware, it may be more shattering. Zero-day attacks are growing very rapidly with raise in the applications. According to cybersecurity projects, escalation in zero-day attacks perceived in 2015 is one attack per week, which may increase in 2023 to one attack per day. Afterward, it may lead to financial loss, reputational impairment, and regulatory costs [9]

2.4. Intrusion

With the rapid growing of computer networks as well applications, particularly Internet of Things (IoT) devices, recognizing malicious attacks has become concerned Problem for computer network security. Network Intrusion Detection Systems (NIDS) detects unusual traffic. Wide study has been done to increase ability and performance of NIDS. NIDS is divided into subgroups: signature-based and anomaly-based. The signature-based acquisition scheme gathers identified patterns to attack, to describe it as malicious, and to regard the other as the next usual behaviour. On another, anomaly-based the detection system describes normal behaviour, and any deviation in this case it is known a violent behaviour. Compared with signature-based acquisition systems, several studies have been done presented randomly entered access systems receive anonymous threats, like zero-day attacks [10].

2.5. Data Breach

Data breach is the major challenge in the Cloud, and an internal attack is the worst risk. Therefore, to avoid may be among with a hot based user profiling method that analyses keystrokes of user to authentication afford to the user. In the event of an anomaly in the behaviour, sound notification will be loudly and the present session in VM will be closed [1]. Due to data of end-users transmit to the cloud over fog nodes and vice versa, it concerns exciting to protect it from breach or attack as data travel. Consequently, there is a necessity need for a system to protect data security of end-user (e.g., integrity, availability, and confidentiality), where data is kept in the cloud or fog nodes or travelling between, and to decrease the data breached amount via rogue fog nodes [11]. Meanwhile Fog is closer to the edge, it has the ability to configure security that is tailored to the machines and their tasks. Also, security decisions to whether block access during a breach could be taken nearly immediately [12].

2.6. Data Distribution

The core objective of fog computing for decrease load of the cloud with latency low level in a spread method, Where Fog computing considered extension for IoT and cloud computing, which runs a vital role in offers quicker answer time and tuning traffic of network by dropping time latency though implementing each type of duty. Hence, ML worked to raise data sending processes and speed over Fog nodes, because FC sometimes has many challenges such as frailer to afford acceptable and optimal outcomes that decrease efficiency and value in performance actions. It supports in correction the structure sequence of Fog networks over real- time operation and connection operations which may be meet user's expectations [13]. The conception of IoT is to always interconnect machines over communication techniques such as wireless/wired networks, Bluetooth, GPS systems etc. Moreover Fog machines used as security tool to avoid IoT security issues, however, the wide spread network of machines is formed in order to infer and infer valuable data from raw information so that in an assumed state, this machines can achieve smartly. As the IoT network is rapidly growing, it is definitely meeting protection problems like intrusion detection, privacy, access control, and authentication. The normal algorithms of intrusion detection are digitally rigorous and need an enormous volume of storing space. So, traditional systems can't be installed on IoT devices, as these are resource-restricted. Therefore, attacks monitoring are done by using cloud computing, but network not able to be well checked instantly because cloud high latency issues. Addition, the cost of sharing and execution a framework (24*7) on the cloud may be costly. Consequently, the fog computing model is produced for monitor attacks purpose in real-time on IoT networks [14].

2.7. Big Data Analysis

The practice instantly Big Data controlling of Fog Computing for of supremacy exhaustion is acquisition attractiveness the Cloud servers in classical systems, receive sensor Big Data, perceive abnormal or each attack forms, make predictions and then increase the notifications. Cloud servers impossible to process massive growing sensor contents, due to problems of volume, security, diversity, velocity, bandwidth of network, and support real-time. Fog Computing is presented as a scheme of Distributed Computing which practices mediator Computing architecture to handling for break Cloud Computing borders [15]

2.8. Task Offloading

Offloading Security is technically interesting issue in Fog-Cloud supported IoT system, particularly once operations thru wireless linked schemes in each assets needed

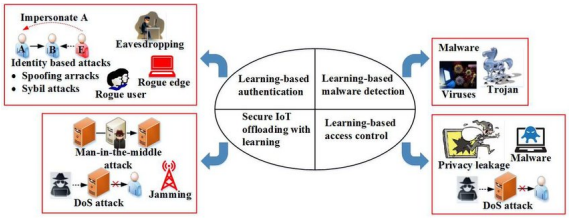

Figure 3. An illustration of the threat model in the Fog-Cloud [17]

to connection are extremely vibrant. With IoT associated scheme, a machine (intelligent mobiles, robot, CCTV, smart-meter etc.) deals with installed programs for implement responsibilities. After the assets worked via the machine become under threshold the operation is get-out. In this computational offloading process for real time, in a video chart, a call is located over video program. Through the call procedure the machine remains exhaustion storage space, memory, and battery. When any of the resources (battery level, space or processing power) to provide the call gets low, it is fallen. In this method machine is protected from completely expired. Instead of letting the device fall the procedure, a portion of content in the storing space can be shuffled to a remote machine to produce extra space on machine, or sub procedure that throw develops the processor affecting battery consume can be transferred to remote schemes. Where main purpose to optimization of resource practice in reduced response time with highest output, that called latency which runs energy balancing between data management processing, and security. In another opinion, support the machine to treat battery as disparate to dropping job [16].

3. ATTACK TYPES OF FOG-CLOUD COMPUTING

There are a several threats dedicated through fog cloud environment related to data hosted, data transportation, deployment, privacy, etc.

That's attacks have more probability to target fog cloud system and considered a critical challenges which have big impact for whole system, provider and customer as mentioned below:

3.1. Denial of Service (DoS)

Denial of service (DoS) threats are a famous type of cyber- attack which target to interrupt the availability of a network or service by overwhelming it with traffic from many equipment. In a fog computing system, DDoS attacks can be particularly challenging to defend against, as the decentralized nature of the system means that attacks can potentially originate from anywhere within the network. Hence, the main difference between DoS and DDoS attacks is: DoS attack happens once the network, service, or device are become inaccessible to its authentic users, while DDoS threat is the subclass of DoS threat and it happens in time the hacker infected various computing machines to interfere systematic traffic of an intended prey [8]. Generally, DoS attack: is an attempt to affect service availability for customers, while, DDoS is used to begin or launch a DoS attack using multiple computers. In cloud computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the offender searches to sort a device or network asset unavailable to its particular users by provisionally or permanent crippling services of a host linked to the Internet. DoS attack is typically accomplished by flooding the targeted device or resource with extreme requests in an effort to overload schemes and deny all or some real requests from being accomplishment. In a distributed denial-of-service attack (DDoS attack), the arriving traffic flooding the targeted originates from lot of various sources. This actively made it disable to prevent the attack basically by blocking a one offensive source [10].

3.2. Man-in-the-Middle

The best method for hackers to cloud offensive is by targeting the fog node, keep it is calmer due to it has a lot of limited assets. Man in the Middle (MitM) threat known as the supreme famous threat in computer networks which is a kind of risk passed out by a malicious inside operator on double workstations by spoof first device that he is the second, where sends signals due to secretly monitoring, snooping, and altering the private communication among machines of Internet of Things. There are two classes of MitM: Eavesdropping and Manipulation. Eavesdropping is passive as the attacker is just attracted in the data transmit over. In a second class of MitM named Manipulation, the opponent modifications content whereas it camouflaged such the original sender. Furthermore, motivation to identify and avert MitM is high, due to possibly the greatest famous risk in Fog computing schemes. That's because the truth that fog design is inherently alike a MitM threat, subsequently fog node is amidst the cloud and the end Thing (machine). Hence, allowing an attacker to hide in plain sight. Similarly, procedure of fog nodes intensely private data like health history, prescription and healthiness situation of any person. They deal also with another vital detail of automobiles such as direction, speed and destination. By the way, like data may evidence disastrous in the erroneous hands. Moreover, fog nodes are extra gorgeous to adversaries due to they are nearer to the attacker than to the cloud and they have fewer computing power [18].

3.3. Data Injection

The entry data from the user side may be used to implement malicious operations over code injection that

embeds several kinds of threats like cross site scripting (XSS)) and SQL injection. Where hackers use entry content as gateway to target the scheme. On other hand, input data must be checked and filtered for mitigate as an attacks [19]. Hackers counteract the privacy perceiving layer is very famous in the actual realm. One method for achieve this is for make a node governor. Data injection, malicious code usage, replay assaults, and side-channel attacks are another system. If an attacker runs over a node, for example, it will break the transmission of valid content on the network and can prevent IoT security systems from working. While If an IoT application receives awfuldata or is affected by faulty injection, it will not work as intended. Multiple sensors and other components form a sensing layer, often called sensing layer. These systems have limited storage, processing, memory and communication. The mainsecurity mechanisms in IoT networks are control, weak encryption, and node authentication. However, when somebody on the network changes or steals informationor data, it is called aninsider attack. SQL injection attacks steal information about actual-world user services by injecting malicious SQL queries into program code. The virtualization attack occurs when harm to one virtual machine expansion to another. With malware injection into the cloud, hackers can hijack cloud services, install malicious code, and even create virtual machines. So data injection means that untrusted data is sent to the interpreter as part of the command or question, and the interpreter can use the information dumped to the primary management as a security countermeasures [20] .

3.4. Malicious Code Injection

Malicious code injection threats which hacker able to manage a Fog node or equipment in IoT through embeds malicious program with the device or node memory, where considered a malicious code injection risk. The Unauthorized Access malicious code not just may achieve particular purpose, furthermore it has capability to award the opponent access and probably complete governor over IoT scheme [19]. Several sensors and many devices recoupthe sensing process, often called layers. These systems have limited storage capacity, memory, processing and communication. The main methods to protect this process in IoT networks are node authentication, weak encryption, and access control. Hacks and crimes focused on understanding the hidden process all exist in the actualenvironment. One method to do this is to complete the node manager. Other mechanisms include the use of malicious codes, data injection, reverse attacks, and side threats. For example, if an attacker uses a node, the transmission of valid messages will be disabled and may be blocked by IoT security applications. If an IoT service receives an error message or is attacked by a malicious injection, it will not work as intended [20].

3.5. Unauthorized Access

Many authors produce a novel method based on techniques of machine learning to protect data processing in cloud system. However the first and primary issue is to avoid unauthorized access to personal health data and medical records and a lot of sensitive information in another of health sector. Actually, homomorphic cryptosystems, Service-Oriented Architecture (SOA), Secure Multiparty Computation (SMC) and Secret Share Schemes (SSS) are the primary protection appliances for nearly current applications. Where the computational expenses associated with image processing operations considered the key issue in procedure of huge information investigation throw cloud by these practices. The researchers used Support Vector Machines (SVM) and Fuzzy C-means Clustering (FCM) to categorize image pixels extra professionally. Furthermore they integrate additional level, the CloudSec component, with conventional two layered design for mitigate threat of the probable leak for health care data [13]. Access control is measured to be a real utility to protect from using unauthorized and control access to fog cloud computing system professionally. Access-control necessities that contain efficiency, latency, aggregation, generality, resource restriction, privacy protection, and policy administration were categorized access control into models that are as bellow: mandatory access-control (MAC) framework, role-based access-control (RBAC) platform, attribute-based access-control (ABAC) model, usage-control-based access-control (UCON) framework, discretionary access-control (DAC) framework, and reference-monitoring access (RMAC) framework. However, able to solve all the remaining security risks too which not declared access control [21].

3.6. Snooping /Eavesdropping /Sniffing

Eavesdropping denoted where malicious hackers can hear on communication channels to seizure transferring data. Adversary has capable to read the data or the meta-data of the protocol, and probably gather knowledge about the node or the device. Encryption is incomplete solving due to node should first recognize itself, such that the consistent key can be related to ciphered connection. Which become privacy problem, as a network or a machine followed [19]. Arepeat attacks in IoT networks may be defined as replied faking, altering, or reusing the identity of the object in question. An attacker can perform a time attack whenever he wants and if he has the data encryption keys. There are many ways besides direct attack to circulate critical data [20].

3.7. Spoofing/ Fake IP

Insecure verification protocols recognized with the main security risk to fog-cloud scheme and the application of end-user machines. The IoT equipment particularly in intelligent networks is revealing to spoofing attack and tempering of data which can finally be denied by architecture, intrusion detection systems, and cryptography as Hellman key. Where video call examination among WLAN and 3G user in fog node stayed directed for man-in-the-middle attack which output displays that the threat did not expose obvious memory operation alterations and usage of CPU in fog network [21]. Many of the protocols such as TCP, HTTP and UDP are been hacked using false loop by the attacker. Client-server side gets hacked by spoofing authentic request by the impostor. Individual data is collected by the intruder which conveys password; pin number etc. hacker websites without digital signature hacked the user by breaching their personal information. For example, in medical sector, deep learning technique is prominently growing due to the improvement in technological features. The vulnerability could raise the complexity over the information. IoT is growing in many fields since it cuts time and complexity in environment. Attackers use the backdoor process to collect the data of the customer [22].

4. SOLUTIONS OF FOG - CLOUD SECURITY

Recently insights a lot of new approaches and tactics to prevent adversaries growing methods and tolls to attempt to target individual, business, and government systems and become whole assets are targeted by a different agent of hackers. Thus, here bellow a many techniques will be described shortly such as:

4.1. Data Encryption

Numerous cloud-based data encryption standards and policies published recently have contracted a vigorous role in promoting safety of cloud. As well as, many access administration methods and innovative applications for personality recognize, control and following have encouraged improved safekeeping procedures in cloud system. When pre-processed data and gotten within environment, any data packets are bow to cryptography process encryption and decryption and investigated with ML systems to identify and alarm abnormal data, afterword transport through toward cloud layer, consequently confirming just the related data are transferred through cloud environment. Moreover, proficient integrity of data verification must be achieved after and before transmission to authorize the information received and it's owner. However, the main challenge of encrypting when data backup as open video streaming is performance will be minimized in Fog scheme and effects until the features of fraternal apps. Hence, foreword to prevent loss of data attacks and Advance Persistent Threats (APTs) by used Elliptic curve cryptography as encryption system for pivotal applications. The encryption of data broadly used procedure to keep content security. To defeat the advanced asset position matters of encryption, have to use such as algorithm of AES by key in size 256-bit or confusion could be work to confirm privacy, although the protect protocol Socket Layer (SSL) could be operated for creating safe connection amongst a client and a server, where critical and sensitive data only must be encrypted, like identity of user in transport nets such as taxi, bus, and cars, data of patient in hospitality schemes, offloading data and soon [23]. Fog computing is still release structure that requires advance study. Midst all the other concerns customary in fog computing, safety is the number one in the intense problems. The fog, presence nearer to the end user, is high vulnerable than the cloud. The Biometric cryptography key is used to lock the scrambled information in the fog diagram. The Biometric cryptography procedure practises fingerprint, voice or iris as a key factor to secure the data encryption and decryption in the cloud server. Advanced biometrics are used to protect more important files and appreciated. A more instantaneous issue is that tables of privacy data are objectives for adversaries. Hence, biometric technique suggestions so density results of safety. In defeat the risks, the platforms are suitable and tough to replicate. Furthermore, this schemes going to improving for a long time into coming years [24].

4.2. Artificial Intelligence

A critical, abnormal threats and anomaly need assistant tools, techniques to recognise bucket, File, data are normal or malware contents. However, the AI techniques are best algorithms used as defence application assistant for Zero-Day-Attack which never known and not added to threats database. Furthermore, the Machine Learning (ML) contents a lot of particular usefully scheme which considered a common best approach for keeping fog cloud nods, services, and data are protected.

4.3. Machine Learning

Machine learning means the machine capability to learn by experiences. Furthermore, the importance security solutions of machine learning based IoT are various supervised Machine Learning algorithms such as Support Vector Machine (SVM), Naïve Bayes, Random Forest, Knowledge Neural Network (KNN), Decision Tree, Bagging, Neural Network, and unsupervised machine learning algorithms such as association mining, K Means, Neural Network available for smart data analysis. The primary job of Machine Learning is the data samples analyzing and make decisions depending of the learned feature pat-

tern. However, ML using for IoT security which supports resource controlled devices to interconnect securely to edge device by giving ability to the nodes/gateway for analyze entering packets and traffic in the network. On other hand, ML algorithms such as Deep Neural Network (DNN), RNN, RF, ANN, etc. are offered for authentication and access control [25]. Nowadays Machine Learning considered as the supreme commonly applied AI method in several sectors such as asset administration, security, decision making, improvement of computation, reducing latency, and power consumption, big data analysis, and accuracy of data. ML runs important character in making intelligent cities, smart platform monitoring schemes. It is used to overcome network issues comprise network routing, resource allocation, traffic administration, and security of data. It has the exposure algorithms on embedded IoT machines. The algorithm divorces the layers of a CNN and allocates the mission by property maps as intermediates. The generated Fog based item detection diagram able to lower the latency of the scheme in correlation thru a cloud-based model by (90.3%) (from $19.56ms$ to $1.89ms$) and the produced Fog-Based element identification model imaged how to expand the casing paces of the model also, displaying perfection of at each degree 30% or extra for another objective ranks of data frameworks[26]. However, Fog computing is a technol-

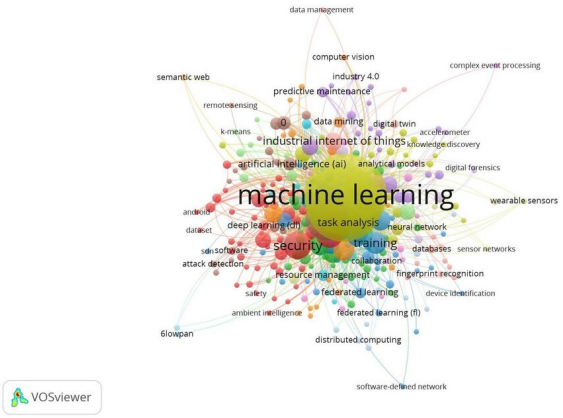

Figure 4. Fog Cloud/IoT-machine learning publication analysis from 2013 to 2023 [5].

ogy that conveys cloud applications nearer to IoT devices, but it becomes with obstacles in parts of security. Where methods of ML used for treat these issues. Fog computing protection still an important emerging research, hence, machine learning has capability to improve authorization, access control, and privacy. ML systems assembled at edge nodes could discover intrusions and anomalies. The establishing trust relationships between fog nodes and IoT devices considered an interesting on trusted management. Organizations should implement comprehensive security approaches to counter malicious fog nodes [5]. Deep learning is known a subsection of ML in AI. The DL techniques are proper to DDoS threat detection as: The DL approaches able to categorize the data and do feature extraction. Recently, many of condition for scheme detect which capable to transaction with the absence of information. However the label for genuine traffic usually exists, selective DDoS threats with various rates and patterns from gentle traffic is very exciting problem [8]. DL has the capability to resolve complex problems due to that's the most common tool for modelling issue. It can not only generate useful outcomes in which other methods fail, but it could also create very perfect models and shorten the time it takes to create a good perception in half. DL techniques, by the way, require a lot of computing power to exercise. Nowadays IoT and fog networks, data analysis to recognize meaningful trends and information is crucial, and DL algorithms are at the root of all data analytics actions. There are a lot of traditional deep learning algorithms such as: Convolutional Neural Networks (CNN), Long Short-Term Memory Networks (LSTM), Deep Neural Networks (DNN), and Recurrent Neural Networks (RNN) [27]. The Convolution Neural Network-Multiclass Support Vector Machine (CNN-MSVM) technique for investigate traffic in networks, an approach evaluated the data traffic in networking for identify and determine irregular events. However, when the data transfer in different cloud protocols, and throw many of data centres under several operating settings, it is important to do deep evaluate of the data for detect the temper action. Then, for providing cloud security might use extended machine learning technique like CNN-MSVM, where dual diverse groups of information like ISOT and UNSW, and TOR are used to testing and proficient analysis on CNN-MSVM scheme. Where training are passed out used serving all the entry information (network traffic data) inside entry layer convolution neural networks (CNN) method to afford best training methodology for data analytics concerning security of cloud. The researchers mentioned that the present methods like support vector machine and linear regression have been tried to maintain cybersecurity in the environment for purpose pre-defined threats detection by acting static verification to behaviour of user's cloud. But the main disadvantages of their static environment are functionality restricted of these security techniques [23]. The Support Vector Machines (SVM) technique and Fuzzy C-means Clustering (FCM) used to organize image pixels added proficiently. Furthermore they integrate additional level, the CloudSec segment, into the conventional two layered scheme to mitigate the threat of the probable leak for health care data. Here recommended answers to mitigation security problem in cloud-based image processing for health care sector because image processing needs perfect platform where it is frequently limits in computational time and memory space. So, it is essential to implement cost-effective solutions instead of legacy systems. Therefore these concerns let authors

used cloud computing to meet wide-ranging data processing requirements. Consequently, in house applications replaced by cloud services definitely would support healthcare organizations outsource computations to an outdoor team, so reducing operating costs, where this methods affords rapid access to on-demand services with high scalability and availability. Nowadays, several frameworks are developed to support users to process and data hosting via cloud computing. Commonly, they are settled by distributed systems, cryptosystems and often a mixture of both. In proposed paper the authors produce a novel method based on techniques of machine learning to protect data processing in the cloud system, however the first and primary issue is to avoid unauthorized access to personal health data and medical records [1]. The compost technique (Auto-IF) designed for detection of intrusion of fog system depends on deep learning method by Autoencoder (AE) and Isolation Forest (IF). The proposed technique aims binary only grouping to arriving data as fog equipment are additional anxious about differentiating threat from regular contents in auto response. They approve the suggested technique on the standard NSL-KDD dataset. Hence, the method for intrusion detection give a great accuracy result around $95.4VS$ a lot of another state-of-art intrusion detection techniques. However, suggested technique includes two phases of irregularity detection, where first stage output becomes the second phase input. Clearly test dataset is provided to the autoencoder in first phase. However, AE known a deep neural network operate used for detecting intrusion attacks, recognizes the attack and isolates the attack and normal traffic data of network into dual groups. Isolation forest in second phase, try to recognize these outlier (oddity) data points, which develops the whole accuracy [28]. Artificial Neural Networks (ANN) a technique used to detect anomalous data, where able of preventing denial of service or man-in-the-middle attacks in IoT schemes. On another hand, this method has disadvantages the main one is deals with only 3 input neurons for training, which experimented with 360 points of data, which considered a small amount of data for ANN training. The second issue with ANN is need more time for experimental versus to another ML technique, which becomes less preferred compared with Naïve Bayes or Random Forest [12]. Naive Bayesian (NB) classifiers are a type of supervised machine learning algorithm that can be used for classification tasks. They work by using Bayes' theorem to estimate the probability of a particular event occurring, given some evidence. In the context of fog computing security, a Naive Bayesian classifier could be used to identify and classify security threats based on features extracted to enhance the security of fog computing systems by providing real-time analysis from incoming data streams [12]. The Naïve Bayes Algorithm using as a novel method for IoT-based Cybersecurity of Drones security for IoT environment, where clearly a rapid improvements in drones technology affect new problems in security side, reliability, and compliance. The method presented intelligent cyber security model via machine learning algorithms to design an IoT aided drone which support network security threats detecting using Blockchain. Furthermore, Security and Privacy Layer is responsible to support the devices authentication and access control security by the technique of machine learning for purpose of prevent privacy threats like behaviour, physical and location privacy risk. Third party is covertly supervised and monitors the drone information that compromises the personal information of somebody affected. In behaviour privacy, the unauthorized object can capture somebody's behaviour and actions. Hackers using location privacy includes to monitor the position by permitted peoples. These risks can be accomplished over the authentication systems and protocols. Moreover, to alert and detect security threats the machine learning models used for device authentication. Furthermore, produced model used the Naïve Bayes model for the IoT-based cyber-security of drones. This algorithm using IoT sensors data, drones, and network information to initiated security levels patterns and recognized the security risks, where the model with this pattern, had ability to recognized threats in the dataset. Proposed model give top accuracy which reached 96.3% and satisfactory results in real-time security threats finding further the costs are calculated to assessment the performance compared with another machine learning methods which verified through two datasets [29]. A Random Forest-based anomaly detection model can discover compromised IoT machines at spread fog nodes. Testing with the dataset of UNSW-NB15, accuracy analysis presented 99.34% accomplished accuracy with rate only 0.02 false positive. The RF detects attack on IoT infrastructure which has capable to recognize irregular behavior and avoid attacks when attempt to hacked system. RF classifier returned the best results through experiment on the widely offered IoT dataset among experiments different ML systems like ANN, DT, LR, and SVM [30]. A Random Forest (RF) used as a machine learning technique for classifier which accomplishes the optimal result of finding the DoS threat. Best performances are taken from existing 41 % properties from the NSL-KDD dataset by refunded data [30]. The SecOFF-FCIoT is new method for offloading data secure purpose to ensure data secrecy, integrity, and availability through offloading actions in Fog-Cloud to intelligent city operations by implemented ML systems, authors proposed a systematic research methodology for SecOFF-FCIoT model which contain a multiple components, such as offloading, machine learning-based data analysis, decision making, secure data storage mechanisms, and secure communication channels, where machine learning model trained with real-world datasets for optimal predict data results of risk related with offloading. Furthermore, the

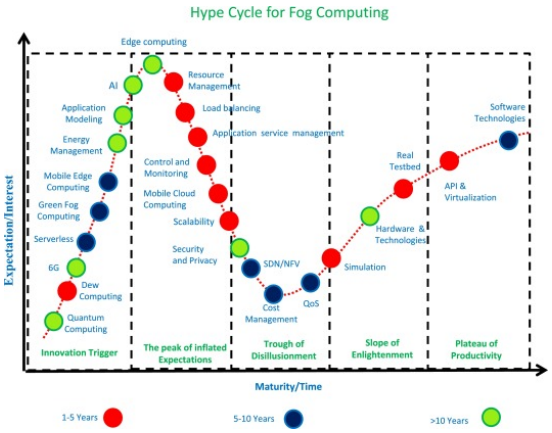

Figure 5. Fog computing hoopla cycle [31]

machine learning framework classified successfully the risk level of data offloading correctly. By the way, the offloading decision making process accomplished a high level of accuracy in recognizing sensitive data that must not be offloaded, minimizing potential security threats in the smart city applications. Moreover, the model secure communication channels and data storage mechanisms successfully protected the confidentiality and integrity of offloaded data [16].

5. TRENDS OF FOG-CLOUD SECURITY

The trends of all information presented chances for the practice of Fog and Edge computing. Fog computing platform permits computational, storage data aggregation and offloading. This enables IoT equipment to support customers with acceptable quality of service and quality of experience which need more security procedures and techniques to keep up this satisfactory while the security *and* privacy a first client's anxiety [16]. Furthermore, depends on Cloud Security Alliance, 2019 in Certificate of Cloud Security Knowledge (CCSK) Guide which mentioned their covered security trends that impact cloud which are: Blockchain, Artificial Intelligence, Certificate Authority, Software Defined Perimeter, DevSecOps, and the Internet of Things. Moreover, The Fog of Things considered a panic subject related with cloud computing field.

Figure 5 shows the hoopla cycle for fog computing that shows the revolution elicit the highest of big expectations. Here also grouped different current research sectors for three different priority levels in five years, 5-10 years, and more than 10 years associated to the existing study. At the top current studies, upcoming effective research directions are expected within 5-10 years in fog computing domain going towards Quality of Service (QoS), cost management, simulation, scalability, hardware, software technologies, load balancing, resource management, and security and privacy [31].

6. CONCLUSIONS

The paper find out the Encryption remains a strategy method in cloud domain to recover maintain of the information. But there is a problem with encryption that adjusts the information operation. Moreover the difficulty of data indexing and searching. However, the best techniques for Fog-Cloud security still AI specially ML methods where have capability for detection misuse and anomaly threats instantly and have dynamically work in various platforms, particularly the Naïve Bayes and Random Forest are the best machine learning methods for data classification either normal or anomaly activity, which produced the optimal accuracy measurement results balanced with latency.

REFERENCES

[1] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine learning for cloud security: A systematic review," *IEEE Access*, vol. 9, pp. 20 717–20 735, 2021. [Online]. Available: doi:10.1109/ACCESS.2021.3054129.

[2] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of ddos attacks in cloud," *IEEE Access*, vol. 8, pp. 181 916–181 929, 2020. [Online]. Available: doi:10.1109/ACCESS.2020.3028690.

[3] S. U. Jamil, M. A. Khan, and M. Ali, "Security embedded offloading requirements for iot-fog paradigm," in *2019 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW)*, vol. 1, 2019, pp. 47–51. [Online]. Available: doi:978-1-7281-4473-3/19.

[4] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog computing security and privacy for the internet of thing applications: State-of-the-art," *Secur. Priv.*, vol. 4, no. 2, e145, 2021.

[5] T. A. Ahanger, U. Tariq, A. Ibrahim, I. Ullah, Y. Bouteraa, and F. Gebali, "Securing iot-empowered fog computing systems: Machine learning perspective," *Mathematics*, vol. 10, no. 8, p. 1298, 2022. [Online]. Available: doi : 10 . 3390 / math10081298.

[6] H. Wang and Y. Jiang, "A novel blockchain identity authentication scheme implemented in fog computing," *Wirel. Commun. Mob. Comput.*, vol. 2020, no. 1, p. 8 849 363, 2020. [Online]. Available: doi:10.1155/2020/8849363.

[7] F. Nocera *et al.*, "Cyber-attack mitigation in cloud-fog environment using an ensemble machine learning model," in *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, IEEE, 2022, pp. 1–6. [Online]. Available: doi:10.23919/SpliTech55088.2022.9854372.

[8] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting ddos attacks: A systematic review," *Soft computing*, vol. 27, no. 18, pp. 13 039–13 075, 2023. [Online]. Available: doi:10.1007/s00500-021-06608-1.

[9] U. Zahoora, A. Khan, M. Rajarajan, S. H. Khan, M. Asam, and T. Jamal, "Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive pareto ensemble classifier," *Sci. reports*, vol. 12, no. 1, p. 15 647, 2022. [Online]. Available: doi:10.1038/s41598-022-19443-7.

[10] S.-H. Chuang, R.-C. Yang, and S.-D. Wang, "Network intrusion detection system with stream machine learning in fog layer and online labeling in cloud layer," in *2021 International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*, IEEE, 2021, pp. 53–59. [Online]. Available: doi:10.1109/ICEIB53692.2021.9686445.

[11] M. Alshehri and B. Panda, "Minimizing data breach by a malicious fog node within a fog federation," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, 2020, pp. 36–43. [Online]. Available: doi:10.1109/CSCloudEdgeCom49738.2020.00016.

[12] M. Moh and R. Raju, "Machine learning techniques for security of internet of things (iot) and fog computing systems," in *2018 International Conference on High Performance Computing & Simulation (HPCS)*, IEEE, 2018, pp. 709–715. [Online]. Available: doi:10.1109/HPCS.2018.00116.

[13] S. Das and P. Guria, "Adaptation of machine learning in fog computing: An analytical approach," in *2022 International Conference for Advancement in Technology (ICONAT)*, IEEE, 2022, pp. 1–11. [Online]. Available: doi:10.1109/ICONAT53423.2022.97%2026114.

[14] M. Sahi, M. Soni, and N. Auluck, "An intrusion detection system on fog architecture," in *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, IEEE, 2021, pp. 591–596. [Online]. Available: doi:10.1109/MASS52906.2021.00084.

[15] R. Jaiswal, A. Chakravorty, and C. Rong, "Distributed fog computing architecture for real-time anomaly detection in smart meter data," in *2020 IEEE sixth international conference on big data computing service and applications (BigDataService)*, IEEE, 2020, pp. 1–8. [Online]. Available: doi:10.1109/BigDataService49289.2020.00009.

[16] A. A. Alli and M. M. Alam, "Secoff-fciot: Machine learning based secure offloading in fog-cloud of things for smart city applications," *Internet Things*, vol. 7, p. 100 070, 2019. [Online]. Available: doi:10.1016/j.iot.2019.100070.

[17] N. Mishra, R. K. Singh, and S. K. Yadav, "Detection of ddos vulnerability in cloud computing using the perplexed bayes classifier," *Comput. Intell. Neurosci.*, vol. 2022, no. 1, p. 9 151 847, 2022. [Online]. Available: doi:10.1155/2022/9151847.

[21] J. Yakubu, S. M. Abdulhamid, H. A. Christopher, H. Chiroma, and M. Abdullahi, "Security challenges in fog-computing environment: A systematic appraisal of current developments," *J. Reliab. Intell. Environ.*, vol. 5, no. 4, pp. 209–233, 2019. [Online]. Available: doi:10.1007/s40860-019-00081-2.

[22] V. B. R. Krishnamoorthy and R. Thiagarajan, "Cyber attack detection on iot using network traffic mechanism by neural network predictive approach," *Eur. J. Mol. & Clin. Med.*, vol. 7, no. 10, pp. 3690–3698, 2020.

[18] F. Aliyu, T. Sheltami, and E. M. Shakshuki, "A detection and prevention technique for man in the middle attack in fog computing," *Procedia computer science*, vol. 141, pp. 24–31, 2018. [Online]. Available: doi:10.1016/j.procs.2018.10.125.

[19] M. Farhadi, J.-L. Lanet, G. Pierre, and D. Miorandi, "A systematic approach toward security in fog computing: Assets, vulnerabilities, possible countermeasures," *Software: Pract. Exp.*, vol. 50, no. 6, pp. 973–997, 2020. [Online]. Available: doi:10.1002/spe.2804.hal-02441639.

[20] T. Mazhar *et al.*, "Analysis of iot security challenges and its solutions using artificial intelligence," *Brain Sci.*, vol. 13, no. 4, p. 683, 2023. [Online]. Available: doi:10.3390/10.3390/brainsci13040683.

[23] E. K. Subramanian and L. Tamilselvan, "A focus on future cloud: Machine learning-based cloud security," *Serv. Oriented Comput. Appl.*, vol. 13, no. 3, pp. 237–249, 2019. [Online]. Available: doi:10.1007/s11761-019-00270-0.

[24] P. Arul and N. Shanmugapriya, "Data security in fog computing using biometric crypto system," *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, pp. 14 497–14 505, 2021. [Online]. Available: doi:14497%E2%80%9314505.

[25] H. Tyagi and R. Kumar, "Analyzing security approaches for threats, vulnerabilities, and attacks in an iot environment," in *2021 International Conference on Computational Performance Evaluation (ComPE)*, IEEE, 2021, pp. 227–233. [Online]. Available: doi:10.1109/ComPE53109.2021.9752151.

[26] S. H. Nee and H. Nugroho, "Task distribution of object detection algorithms in fog-computing framework," in *2020 IEEE Student Conference on Research and Development (SCOReD)*, IEEE, 2020, pp. 391–395. [Online]. Available: doi:10.1109/SCOReD50371.

[27] S. Askar, "Deep learning and fog computing: A review," *Available at SSRN 3962705*, 2021. [Online]. Available: doi:10.5281/zenodo.5222647.

[28] K. Sadaf and J. Sultana, "Intrusion detection based on autoencoder and isolation forest in fog computing," *IEEE Access*, vol. 8, pp. 167 059–167 068, 2020. [Online]. Available: doi:10.1109/ACCESS.2020.3022855.

[29] R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "Iot-based cyber-security of drones using the naıve bayes algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 7, 2021. [Online]. Available: doi:10.14569/IJACSA.2021.0120748.

[30] T. Pinto and Y. Sebastian, "Detecting ddos attacks using a cascade of machine learning classifiers based on random forest and mlp-ann," in *2021 IEEE Madras Section Conference (MASCON)*, IEEE, 2021, pp. 1–6. [Online]. Available: doi:10.1109/MASCON51689.2021.9563266.

[31] J. Singh, P. Singh, and S. S. Gill, "Fog computing: A taxonomy, systematic review, current trends and research challenges," *J. Parallel Distributed Comput.*, vol. 157, pp. 56–85, 2021. [Online]. Available: doi:10.1016/j.jpdc.2021.06.005.