mathematics

MDPI

Article

Securing IoT-Empowered Fog Computing Systems: Machine Learning Perspective

Tariq Ahamed Ahanger [1,*], Usman Tariq [1], Atef Ibrahim [1], Imdad Ullah [1], Yassine Bouteraa [1] and Fayez Gebali [2]

[1] College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; u.tariq@psau.edu.sa (U.T.); aa.mohamed@psau.edu.sa (A.I.); i.ullah@psau.edu.sa (I.U.); y.bouteraa@psau.edu.sa (Y.B.)

[2] Electrical and Computer Engineering Department, University of Victoria, Victoria, BC V8P 5C2, Canada; fayez@uvic.ca

* Correspondence: t.ahanger@psau.edu.sa

Abstract: The Internet of Things (IoT) is an interconnected network of computing nodes that can send and receive data without human participation. Software and communication technology have advanced tremendously in the last couple of decades, resulting in a considerable increase in IoT devices. IoT gadgets have practically infiltrated every aspect of human well-being, ushering in a new era of intelligent devices. However, the rapid expansion has raised security concerns. Another challenge with the basic approach of processing IoT data on the cloud is scalability. A cloud-centric strategy results from network congestion, data bottlenecks, and longer response times to security threats. Fog computing addresses these difficulties by bringing computation to the network edge. The current research provides a comprehensive review of the IoT evolution, Fog computation, and artificial-intelligence-inspired machine learning (ML) strategies. It examines ML techniques for identifying anomalies and attacks, showcases IoT data growth solutions, and delves into Fog computing security concerns. Additionally, it covers future research objectives in the crucial field of IoT security.

Keywords: machine learning; security; Fog computing; Internet of Things

MSC: 68

Citation: Ahanger, T.A.; Tariq, U.; Ibrahim, A.; Ullah, I.; Bouteraa, Y.; Gebali, F. Securing IoT-Empowered Fog Computing Systems: Machine Learning Perspective. *Mathematics* **2022**, *10*, 1298. https://doi.org/10.3390/math10081298

Academic Editors: Ioana Boureanu and Liqun Chen

Received: 11 February 2022
Accepted: 7 April 2022
Published: 14 April 2022

1. Introduction

IoT devices have grown considerably, infiltrating practically every aspect of the human social world [1]. IoT devices usher in the smart environment in the form of smart homes, intelligent industry, and smart healthcare in which everything is connected to the Internet ubiquitously [2]. As an illustration, there are *smart medical bio-sensors* which not only monitor health from remote locations but also administer medicines in a real-time manner [3,4]. Other instances include *smart bridges* which can monitor vehicular load [5], *smart power grids* for detecting disruptions and power management distribution [6], and *smart machinery* which have built-in sensors for task automation. In addition to being ubiquitous, IoT devices are actively employed in practically every aspect of life, and the numbers are startling. The number of internet-connected devices surpassed the world's population of around 6.7 billion people in 2008. According to estimates, there will be 6.1 billion mobile phone users and 50 billion items linked to the Internet by 2022 [7]. By 2027, it is expected that industries will have 27 billion automated machines. When the attention is shifted to the volume of data created, one may see the beginning of the Zettabyte era [8]. In 2013, 3.1 zettabytes of data were created by devices connected to the Internet. It was 8.6 zettabytes in 2014, and it is predicted to be close to 400 zettabytes by 2022 [9]. Though the life-changing advantages are numerous, the security and privacy

problems of a system with a plethora of devices built separately and connecting via diverse protocols, as well as generating zettabytes of data in the cloud, are significant [10]. It is astonishing to learn what type of information is kept in the cloud and how easy hackers can access it. According to the Global Cloud Index [11], which discusses the different categories of cloud-oriented data, 7.6% of research on file-sharing platforms included private information. In 4.3% of all research articles, keywords related to personal information, including tax ID numbers, phone numbers, addresses, and social security numbers, are found. Moreover, payment-oriented data of debit card numbers, bank account information, and credit card numbers are found in 2.3% of articles. Finally, protected health information for patient diagnoses, record registration numbers, and treatments are found in 1.6% of research articles. As the number of individuals using IoT devices increases, more people become susceptible to fraudsters as the data collected by the IoT devices is vulnerable to attacks. The amount of security breaches has risen considerably, with recent examples including the hacking of a water treatment plant [12], the Saudi Aramco $50 Million Data Breach (Source: https://purplesec.us/recent-cyber-security-attacks/ (2 February 2022)), the Kaseya Ransomware Attack (Source: https://purplesec.us/recent-cyber-security-attacks/ (2 February 2022)), phishing, ransomware, supply chain attacks (Source: https://purplesec.us/recent-cyber-security-attacks/ (2 February 2022)), and the planning of robberies using data from wearable devices [13,14]. According to the Cybercrime Report (Source: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (2 February 2022)), the cost of cybercrime consequences reached $6 trillion per year by 2021.

Conspicuously, the current article discusses the security and privacy issues that have arisen as a result of the fast growth of IoT devices and the systems that enable them, i.e., *Fog computing.* Figure 1 shows the basic framework model for IoT-Fog computing [15].

The paper is structured as follows: The fundamentals of IoT security are detailed in Section 3. Artificial-intelligence-inspired ML strategies for securing IoT and Fog computing systems are described in Sections 4 and 5, respectively. Section 6 provides future directions in the current domain of study. Finally, in Section 7, the article is concluded.

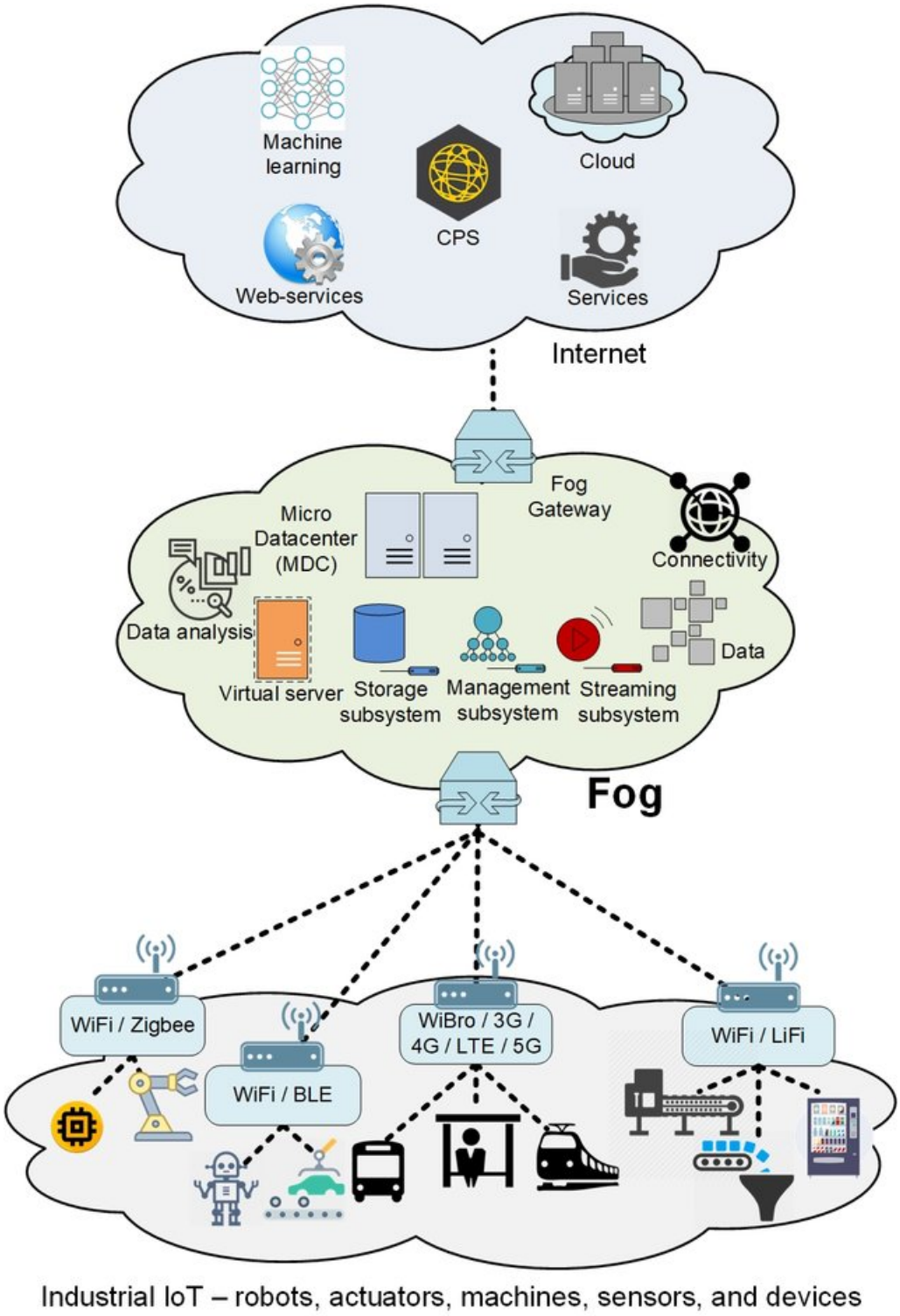

Figure 1. IoT-Fog computing framework.

2. Information Sources

Performing a literature review necessitates extensive searching of electronic sources. To increase our chances of identifying the most relevant research publications, the following databases have been identified and selected:

1. IEEE eXplore
2. ACM Digital Library
3. Wiley Interscience

4. ScienceDirect
5. Springer
6. Semantic Scholar

Other Resources: In order to locate relevant papers not included in the scope of the current systematic review, the following supplementary resources were accessed:

1. Bibliographies of primary research to find relevant articles
2. Reports on technical issues
3. Edited books and textbooks

2.1. Search Criteria

The most prominent scientific digital resources were considered for the investigation to compile a list of relevant research publications. The articles have been fetched from various digital libraries such as ScienceDirect, IEEE Xplore, Springer, Taylor and Francis (T&F), ACM, Sage, Wiley, InterScience, and Google Scholar. Finding relevant research articles from the literature relies heavily on "Search string construction" and "Search keywords selection". Fog computing, Security, Machine Learning, Framework, Application, and Architecture were the most commonly used terms to characterize the search phrase. The phrase was created by combining with the boolean operators AND and OR. The used string is as follows:

("Fog Computing" OR "Machine Learning (ML)") ("Fog Computing" or "Security") AND ("Fog Computing" OR "Attacks" OR "Fog Application" OR "Architecture")

Based on the aforementioned strings, more than 700 articles were selected, which included redundancies, invalids, and editorials. Using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Source: http://prisma-statement.org/Protocols/ (2 February 2022)) approach for systematic literature review, numerous restrictions were employed to refine the search criterion as mentioned ahead.

Restrictions

Research on Fog computing and Fog-based security is very recent, and few articles were published before 2015. As a result, there were just a few studies before 2015. The first-round paper selection criteria included non-peer-reviewed and non-ISI publications from various journals and conferences, with over 520 papers selected. A research screening procedure was used to eliminate brief articles, non-peer-reviewed papers, book chapters, and low-quality studies that could not provide any technical or scientific information. Eighty-two peer-reviewed publications from high-impact journals and conferences were chosen for this systematic review. For the final selection of high-quality papers, the following criteria were adopted:

1. The journal and conference are included in the index.
2. A survey or review of research is introduced in the publications.
3. The papers are prepared in the English language.
4. The papers follow the peer-reviewed process.

Fog computing security is a large field of study, with several studies appearing in various publications and conference proceedings. A quality assessment was conducted on the remaining articles following the exclusion and inclusion criteria to identify the most relevant research. External validity, internal validity, and bias were all evaluated. Quality evaluation forms were used to ensure that only high-quality research publications were considered for the current systematic review.

2.2. Extraction of Data

Data extraction from all of the 154 papers evaluated in the current review was assessed. The following set of criteria was adopted for data abstraction.

1. All of the 154 publications were evaluated by one of the writers to extract the necessary information.
2. A random sample of data extraction was used to ensure that the data extraction was consistent.
3. All disagreements that arose throughout the cross-checking process were dealt with in a series of meetings.

3. Fundamentals of IoT Security and Privacy

3.1. Concerns

IoT security issues depict vulnerabilities at many locations in the IoT network and the safeguards that are applicable at each tier based on the "*IBM Point of View on IoT security*" (Source: https://www.ibm.com/in-en/cloud/internet-of-things (2 February 2022)).

1. *Sensation module*: Hackers are able to cause considerable harm when access is granted to devices including healthcare sensors and pacemakers [16]. As a result, (1) unauthorized data acquisition, (2) device malware of unauthorized access, (3) malware for incorrect data transmission, (4) Denial of Service (DoS) attacks, and (5) unauthorized information acquisition are all potential risks in the sensation layer.
2. *Networking module*: The network's manageability, scalability, and availability are critical for IoT deployment. IoT devices become ineffective if monitoring applications cannot obtain data in a time-sensitive manner. It is fairly usual to attack the network by transmitting a large amount of data all at once to overload the network and allow for DoS attacks.
3. *Service module*: The service module functions as a link for the hardware module and the application module. Important functions, including information management and device management, are impacted by an attack on the service module, resulting in end users not being served. Service module security includes data integrity, user authentication, communication security, and access control.
4. *Application module*: The application module is the most vulnerable aspect of the IoT network since it sits at the IoT-Fog-cloud's top-of-stack and serves as a gateway to all the underneath modules. Specifically, the gateway reflects the application module via which IoT devices can be accessed to initialize security attacks. If the interface's authentication and authorization methods are compromised, the ripple effects may extend to the edge. Because attackers might obtain sensitive information through phishing or related attacks, the end-user is a prospective attack method. In addition, SQL injection, default credentials, cross-site scripting, and insecure password recovery techniques are common on the web and application interfaces. The Open Web Application Security Project (OWASP) summarizes the Top 10 IoT vulnerabilities [17]. A detailed description of corresponding vulnerability is shown in Figure 2 (Source: https://owasp.org/www-project-internet-of-things/ (2 February 2022)).

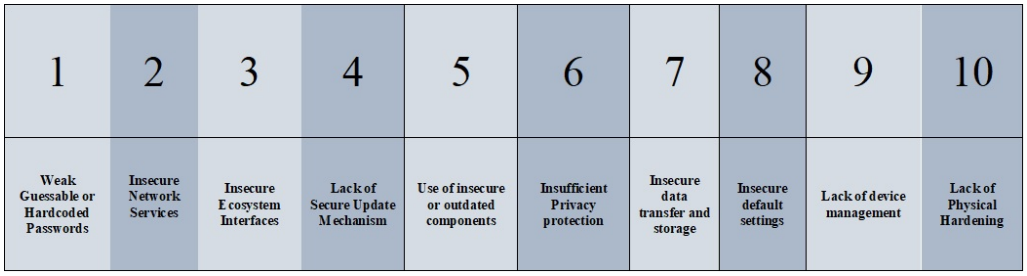

Figure 2. OWASP Top 10 IoT Vulnerabilities; Source: https://www.appsealing.com/owasp-iot-top-10/ (2 February 2022).

IoT Privacy Concerns

According to a 2015 Hewlett Packard Internet of Things research study (Source: https://www.hp.com/us-en/hp-news/press-release.html?id=2037386#.YjX4zepBzIU (2 February

2022)), 80% of IoT devices have privacy issues. Specifically, more than 249 vulnerabilities have been identified, with about 31 per device. Many gadgets capture personal data including name, payment information, birth-date, address, light and sound information, health information, and activities within the house. Many IoT devices transfer information unencrypted within the house network, and data is transmitted to the cloud, which is vulnerable to expose data to the public. Lauren Zanolli [18] wrote in FastCompany on the Internet of Things becoming a *privacy hell*. The Wall Street Journal [19] discusses legal threats that are present in the IoT. Figure 3 depicts the fundamental IoT threat model. In the presented work on privacy in the IoT [20], Ogonji et al. classify the privacy risks as follows: (a) identification, (b) lifecycle transitions, (c) inventory attack, (d) privacy-violating interaction and presentation, (e) localization, (f) profiling, and (g) linkage. Each of these have been detailed ahead.

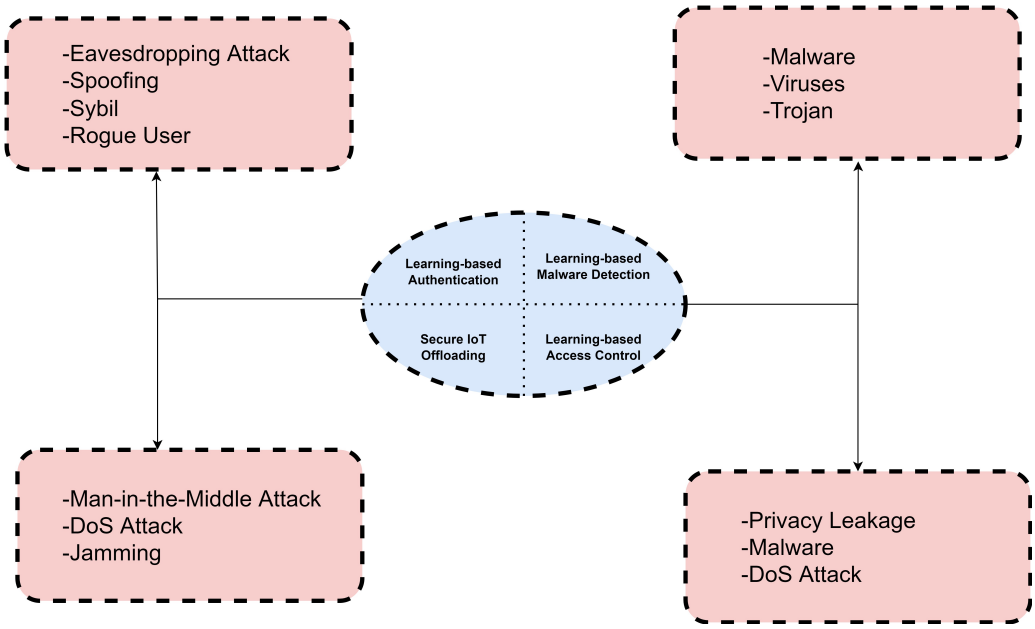

Figure 3. IoT threat model.

1. *Identification*: The threat of identifying an identifier, such as a name and location, with an individual is known as identification.
2. *Localization*: The vulnerability of identifying and registering a person's whereabouts in space-time coordinates is known as localization. Most IoT devices collect information which might disclose illnesses, vacation plans, work schedules, and personal details.
3. *Profiling*: Profiling is the danger of leveraging data from IoT devices to categorize individuals into groups. It might result in pricing discrimination, unwanted advertising, social engineering, or erroneous automated choices.
4. *Interaction and presentation that infringes on privacy*: This is the risk of conveying personal data in such a way that it is exposed to an unintended audience. For illustration, anyone using a wristwatch on public transportation may unwittingly allow passersby to read the SMSes because the data appear on the screen as they arrive.
5. *Lifecycle transitions*: Configurations and data are backed up and restored when smart devices undergo lifecycle transitions. In the process, incorrect data may end up in the wrong device, resulting in a privacy breach. For example, images and movies stored on one device may be viewed on another.
6. *Inventory attack*: Hackers can query gadgets to generate an inventory of objects in a certain area since smart things are queryable via the Internet. For example, hackers can find whether a home has a smart meter, a smart thermostat, or smart lighting.
7. *Linkage*: This a technique in which data from several sources, acquired in various situations, are combined to obtain insights about a subject.

4. IoT Security Using ML

ML is widely employed in IoT data analysis. Tahsien et al. [21] highlights use cases where ML is applied for the manufacturing, utilities, insurance, and healthcare industries. Vital tasks in IoT security include *pattern identification*, *determining outliers*, *value prediction*, and *attribute abstraction*. Table 1 lists some of the major ML techniques, including DBSCAN (Density-Based Spatial Clustering of Applications with Noise), FFNN (Feed-Forward Neural Network), CCA (Canonical Correlation Analysis), CART (Classification And Regression Trees), KNN (K-Nearest Neighbor), and PCA (Principal Component Analysis), which were employed by global researchers for such tasks. The primary goal of most of the papers examined is to detect a security breach. Conspicuously, Table 1 becomes extremely important from a data protection standpoint. The use cases may be further separated into the following categories when it comes to recognizing outliers: *data anomaly detection*, *intrusion detection*, and *malware detection* are the three types of detection. Intrusion detection can be defined as the ability to monitor and react to computer misuse [22]. Anomaly detection is the identification of an undesired event or observation. On the other hand, malware indicates when malicious software perpetrators dispatch to infect computing nodes. Because *anomaly detection* is a classification issue, the most popular ML classification techniques are used, such as Artificial Neural Networks (ANN), Support Vector Machines (SVM), Bayesian Networks, Decision Trees, Random Forest, and Naive Bayes. Moreover, ANN has been applied in a variety of innovative applications. However, ANN is not commonly utilized for malware detection since training takes longer. By summarizing results from the publications in the current domain on each ML technique, the use-case-based technique is presented in Table 2.

Table 1. ML solutions for IoT Security.

Reference	Use Case	Algorithm	Domain	Limitations
[23]	Pattern discovery	DBSCAN	Importance of using DBSCAN technique for attack detection	It is not effective for data clusters having similar densities
[24]	Pattern discovery	K-means	Fundamentals of K-means are discussed in security	It is effective only when data is numerical
[25]	Discovery of unusual data points	Random Forest	Random forest technique for security risk assessment	A large delay was registered
[26]	Discovery of unusual data points	PCA	PCA-based feature reduction for remote sensing secure applications	Minimal accuracy was registered
[27]	Discovery of unusual data points	Naive Bayes	Exploration of probabilistic attack detection	Data dependence reduces the accuracy
[28]	Discovery of unusual data points	KNN	The utilization of KNN for nearest neighbor detection	The value of K should be fixed initially
[29]	Discovery of unusual data points	Support Vector Machine	Prediction-based attack detection	It is less effective for time-sensitive applications
[30]	Prediction of values & categories	Support Vector Regression	The detection of UAV-specific attacks	There was a delay and accuracy was minimal
[31]	Prediction of values & categories	FFNN	Novel vision for data security in smart soil application	The domain of applicability is limited
[32]	Prediction of values & categories	CART	Uncertainty detection and quantification for security	It is not reliable as it based on probability
[33]	Prediction of values & categories	Linear Regression	Linear regression analysis for data variability	The attack detection effectiveness is limited
[34]	Feature extraction	CCA	The fundamentals of feature extractions are discussed	Security is minimally addressed

Table 2. ML techniques for outlier identification.

Use Case	Reference	ML Technique
Malware Detection	[29]	SVM
Malware Detection	[25]	Random Forest
Anomaly Detection	[27]	Naive Bayes
Anomaly Detection	[35]	ANN
Intrusion Detection	[26]	PCA
Intrusion Detection	[28]	KNN
Intrusion Detection	[27]	Naive Bayes

4.1. ML Techniques for IoT Security

1. *Random Forest for malware detection*: Agrawal et al. [36] employed the Random Forest technique on Android data of 49,101 instances with 39 attributes in the proposed work for detecting the Android virus. The major objective was to estimate Random Forest's accuracy for assessing Android applications and classifying them as nondangerous or dangerous. The authors assessed the detection accuracy when the Random Forest algorithm's attributes were modified, such as the depth of each tree, the number of trees, and the number of attributes. Based on six-fold cross-validation, the results concluded that the Random Forest technique performed with enhanced efficacy, with an overall accuracy of over 98.9% and an error rate of 0.2% for forests with more than 39 trees. Moreover, a root mean squared error of 1.69% for forests with 160 trees was registered.
2. *SVM-based malware identification*: Nakhodchi et al. [37] reviewed several techniques for the identification of malware. These include taint-analysis-based, behavior-based, and signature-based detection. It is depicted that Linear SVM is performed well among ML techniques used for Android Malware Detection. Event information on the device in a behavior-based identification framework, including storage utilization and power consumption, is assessed. ML techniques are used to evaluate the data to discover aberrant patterns.
3. *PCA, Naive Bayes, and KNN Intrusion Detection*: Saharkhizan et al. [38] presented a new framework for detecting intrusion based on two-level dimension reduction. Specifically, a two-tier categorization phase is described to detect malicious activities, including remote-to-local and user-to-root attacks. To minimize the dimensions in the dataset, the proposed framework employed Linear Discriminate Analysis (LDA) and Principal Component Analysis (PCA). Moreover, the authors incorporated a two-tier categorization phase with Naive Bayes to detect suspicious activities.
4. *Classification-based anomaly detection*: In the study on creating an IoT gadget for women's safety, Ramalingam [39] described a gadget that assesses whether or not the wearer is in danger. The gadget sends information on the person's physiology and bodily posture. Body temperature and the galvanic skin response (GSR) are the communicated physiological signals. The data from a 3D accelerometer are used to estimate body position. The theory says that when a person is confronted with a threatening scenario, adrenalin secretion impacts several physiological systems, resulting in increased blood pressure, heart rate, and perspiration. As measured by GSR, skin conductance rises as a result of this. A classifier examines the data to decide whether or not the subject is in a risky scenario, such as rape.

4.2. Securing IoT Systems Using ANN

Yousefi et al. [35] discussed the utilization of ANN to anticipate the IoT element state and how to minimize the expenses of IoT administration. The authors have depicted that edge security setups are labor-intensive. A probabilistic neural network backed up by a multilayered perception network was incorporated in the proposed methodology. The research demonstrated that a probabilistic neural network could be utilized to detect the

device's status. Moreover, by employing a multilayer perceptive network, historical values can be compared for enhanced accuracy. Bagaa et al. [40] suggested utilizing ML within an IoT gateway to enable system security. The main objective was to employ ML-based ANN techniques in the gateway to monitor subsystem modules and the complete system in the application layer. After warming up the system with training data, the researchers tweaked the sensors for 10 minutes to add incorrect data. The neural network recognized the distinctions between the legitimate and incorrect input when it was run against the system. It included a temporal instance between transmissions to simulate attacks. The authors predicted if the data was genuine or invalid for the 259 samples. The authors concluded that using ANN is extremely useful for providing enhanced security.

5. Secure Fog Computing

While most of the assessment and ML for IoT details is conducted in the cloud servers, there is a growing tendency to move the computation at the node-edge. As a result, the current section focuses on using ML techniques for the Fog computing framework.

5.1. Fog Computing: Fundamentals

According to the OpenFog Reference Architecture for Fog Computing (Source: https://site.ieee.org/denver-com/files/2017/06/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf (accessed on 2 February 2022)), *Fog computing is defined as an edge-level framework for decentralizing control, storage, and computation capabilities at the user edge*. Wired or wireless access, low latency, and location awareness are vital aspects of Fog computing platforms. There are various advantages, including:

1. *Analytics in real time:* The instances where time-sensitive analysis is required are increasing as IoT adoption develops. For illustration, a security camera may catch a possible burglar loitering at a residence or a fraudster obtaining data regarding unauthorized accounts. It may be too late when data are loaded to the cloud and examined. In these cases, near-instant intelligence is required, which Fog computing may supply.
2. *Increased security:* Because Fog is closer to the edge, it may establish security that is specific to devices and their operations. Furthermore, security choices on whether or not to deny access during a breach may be made instantly.
3. *Edge data thinning:* Fog absorbs raw data and makes judgments or delivers insights based on it. It only delivers pertinent, condensed data up the chain of command. As a result, the data quantity sent to a centralized repository is drastically reduced.
4. *Cost savings:* Due to the scattered nature of installations, Fog may have greater setup costs. However, the whole system's operational expenses and prolonged advantages would be substantial.

5.2. ML for Secure Fog Computing

Secure Fog computing has been researched considerably for privacy, access control, and authorization. Table 3 has been formulated to depict the state-of-the-art comparative analysis in the current domain of study. The analysis is prediction-oriented and reaction-oriented at the Fog computing nodes. Because greater computer power is required, the Fog nodes closest to the user will employ reaction-oriented analysis, whereas the nodes further away from the edge will most likely have predictive analytics. The underlying idea is that computer power is greatest in the cloud and decreases as one moves down the information processing hierarchy. ML techniques can be executed on nodes with sufficient computing power to perform that layer's task. Models for ML are built at edge nodes closer than the cloud. To aid execution, the models might be assessed as intermediary nodes. Table 4 [41] depicts a collection of ML methods utilized in Fog computing in various sectors. Zhang et al. [42] described a hierarchical decentralized Fog computation framework to integrate a large number of infrastructure components and services in future smart cities. The author's design is a three-layered model, with the cloud as the first layer and the sensors

as the final layer. The *Fog layer* is the second layer. The Fog layer comprises computing nodes to receive raw data from the sensors. The Fog computing layer serves two vital tasks. One task uses ML techniques to identify possible danger patterns in incoming data streams from sensors, while the other uses feature extraction to reduce the quantity of data supplied upstream. The publication [42] depicts the inclusion of anomaly identification. Anomaly detection techniques, such as DBSCAN, Random Forest, Naive Bayes, and KNN, have been employed. Fog nodes receive data from nodes below them, and the data comprise information from hundreds of sensors spread over several places. The MAP (maximum aposteriori) and HMM (hidden Markov model) techniques are utilized in the study to classify and notify if a dangerous event occurs. The techniques discussed in the preceding section for IoT security are equally applicable to Fog computing. Malware detection using SVM by Agrawal [36], malware detection using Random Forest by Nakhodchi et al. [37], and intrusion detection by Saharkhizan et al. [38] may all be conducted on Fog nodes rather than on the cloud. Anomaly detection using ANN by Yousefi et al. [35] specifically mentions using ML at the gateway layer. Table 5 shows another comparative analysis of the state-of-the-art literature review for IoT security using ML techniques.

Table 3. ML use cases for Fog computing environment.

Use Case	ML Technique
Industry	Predictive models
Industry	Anomaly detection
Industry	Optimization technique
Retail	Time series clustering
Retail	Statistical technique
Self-Driving Cars	Reinforced learning
Self-Driving Cars	Anomaly detection
Self-Driving Cars	Image processing

Figures 4–6 depict the VOS visualization for the publications in IoT-Fog computing, IoT-machine learning, and IoT-Fog-machine learning environments from a security perspective. VOSviewer is a software tool for constructing and visualizing bibliometric networks (Source: https://www.vosviewer.com/ (2 February 2022)). Specifically, 2010–2021 was considered for assessing the research publications. Moreover, for abstracting research papers in the current domain, the Web of Science repository was utilized, as it is the most widely adopted research publication repository. Summarizing the aspects as mentioned above, some of the common Fog vulnerabilities are depicted in Figure 7 (Source: Puthal, D., Mohanty, S. P., Bhavake, S. A., Morgan, G., & Ranjan, R. (2019). Fog computing security challenges and future directions (energy and security) are also discussed (IEEE Consumer Electronics Magazine, 8 (3), 92–96.)

Table 4. State-of-the-art comparative analysis.

Ref.	Highlights	Trust	Privacy	Auth	Accessible	Confidential	Integral
[43]	Proposed a risk-based trust model for the IoT environment.	Y	N	N	N	Y	N
[44]	Performed a Fog-based hierarchical trust mechanism.	Y	N	N	N	Y	Y
[45]	A broker-based trust mechanism approach in Fog.	Y	N	N	N	N	N
[46]	Secured trust establishment among vehicles.	Y	N	N	N	Y	Y
[47]	Reliable and lightweight trust evaluation mechanism.	Y	N	N	N	N	N
[48]	A data protection scheme was used for Fog computing.	Y	N	N	N	N	N
[49]	Fog-based public cloud computing	N	Y	N	N	N	Y

Table 4. *Cont.*

Ref.	Highlights	Trust	Privacy	Auth	Accessible	Confidential	Integral
[50]	Introduced secure positioning protocols by preserving location privacy.	N	Y	N	N	Y	Y
[51]	Data confidentiality and location privacy were focused on.	N	Y	N	N	Y	Y
[52]	Fog-based vehicular ad hoc network (VANET).	N	Y	N	N	N	N
[53]	Preservation of the privacy of the end users over a radio network.	N	Y	N	N	N	N
[54]	An efficient and secure mutual authentication method for the cloud-Fog-edge system architecture.	N	N	Y	N	N	N
[55]	Fine-grained access control and privacy were provided for Fog computing.	N	N	N	Y	Y	Y
[56]	Fog devices' security can be ensured through key management and authentication schemes.	N	N	Y	N	Y	Y
[57]	Introduced policy-based resource management in the Fog network.	N	N	Y	N	Y	Y
[58]	Ensured secure communication among the various IoT devices.	N	N	Y	N	Y	Y
[59]	Introduced anonymous mutual authentication amongst the Fog users and Fog servers.	N	N	Y	N	Y	Y
[60]	Highlighted privacy preservation and security methods for Fog-based image processing applications.	N	N	Y	N	Y	Y
[61]	An efficient and elliptic cryptographic-based mutual authentication technique for IoT-based resource-constrained devices.	N	N	Y	N	Y	Y
[62]	CP-ABE-based multiauthority data access control scheme in Fog-cloud computing systems.	N	N	N	Y	Y	Y
[63]	Employing a lightweight privacy preserving data aggregation method for Fog and IoT systems.	N	Y	N	N	Y	Y
[64]	A promising CP-ABE-based access control method for a Fog computing environment.	N	N	N	Y	N	N
[65]	Fog-based decentralized multiauthority attribute-based data access control.	N	N	N	Y	N	N
[66]	A distributed multitenancy approach to access control.	N	N	N	Y	N	N
[67]	Deliberated two-factor lightweight and privacy preserving authentication method for resource-constrained IoT devices.	N	N	Y	N	N	N
[68]	A hybrid and fine-grained access control solution.	N	N	N	Y	Y	Y
[69]	Access control mechanisms proposed for Fog computing and ad hoc MCC.	N	N	N	Y	Y	Y

Table 5. ML techniques for IoT threat reduction. Y, Yes; –, No.

Reference	Year	ANN	CNN	RNN	AF	RBM	DBN	GAN	EDL	Threat
[70]	2015	Y	–	–	–	–	–	–	–	Routing attack detection
[71]	2014	–	–	Y	–	–	–	–	–	Malicious behavior detection
[72]	2009	Y	–	–	–	–	–	–	–	Data tampering
[73]	2013	Y	–	–	–	–	–	–	–	Spoofing attack detection
[74]	2017	–	–	–	Y	–	–	–	–	Malware detection
[75]	2015	Y	–	–	Y	–	–	–	–	Impersonation attacks
[76]	2018	–	–	–	Y	–	–	–	–	Impersonation attacks
[77]	2016	Y	–	–	–	–	–	–	–	Cyber attacks
[78]	2017	–	–	–	Y	–	–	–	–	Cyber attacks
[79]	2017	Y	–	–	–	–	–	–	–	DDoS attack detection
[80]	20N6	–	–	–	–	–	Y	–	–	Malicious attack detection
[81]	2017	Y	–	–	–	–	–	–	–	Authentication
[82]	2016	–	Y	–	–	–	–	–	–	Malware detection

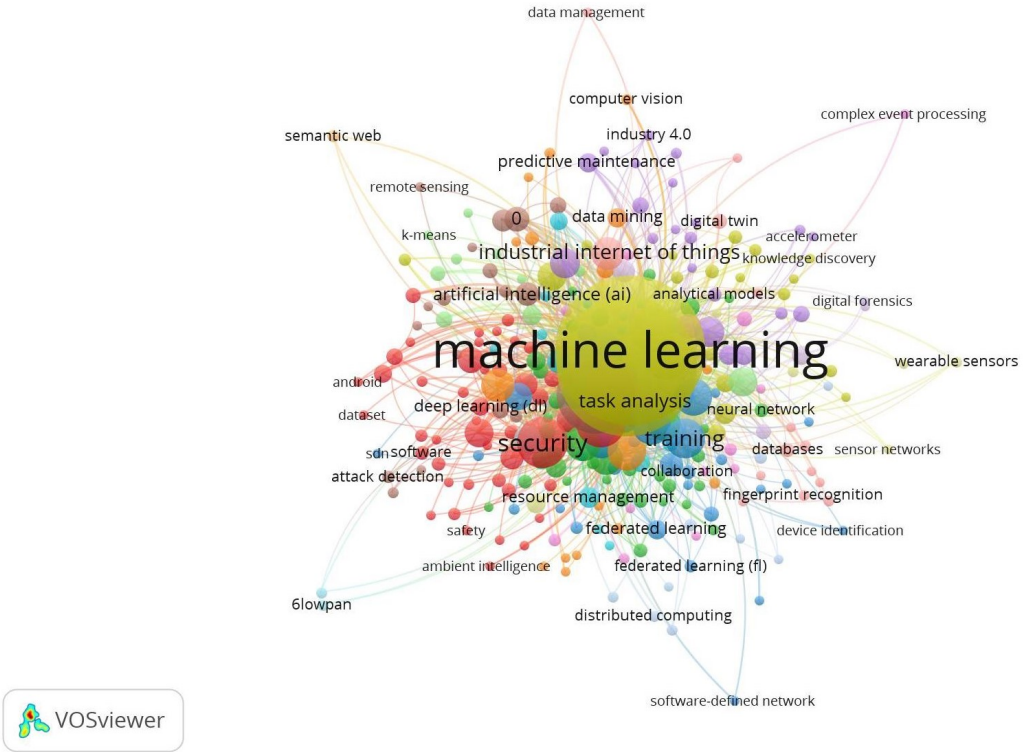

Figure 4. IoT-machine learning publication analysis from 2010 to 2021.

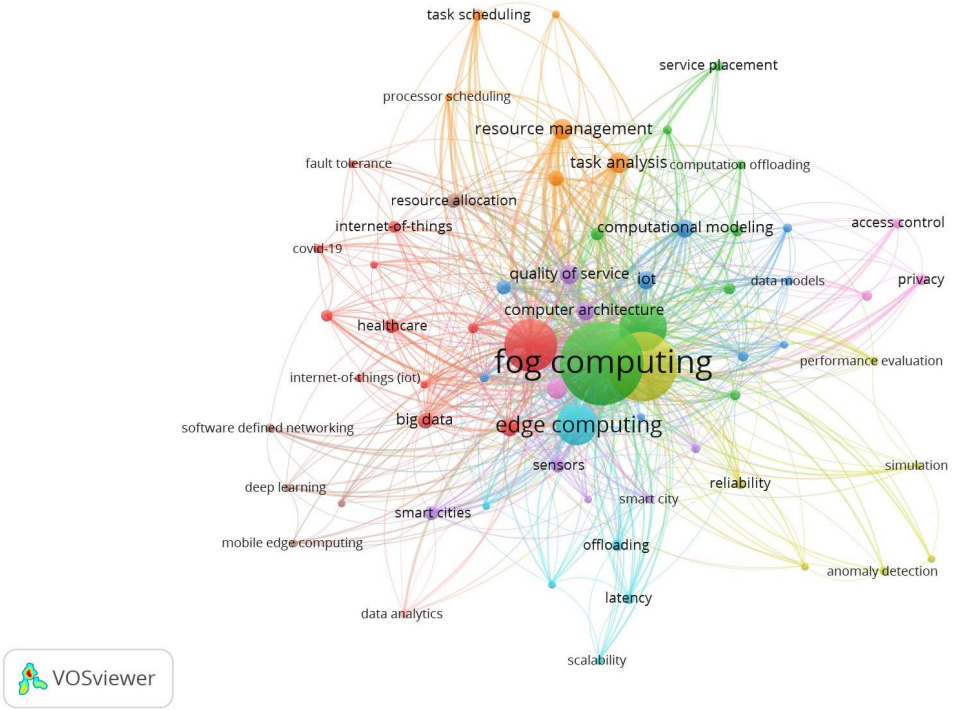

Figure 5. IoT-fog computing publication analysis from 2010 to 2021.

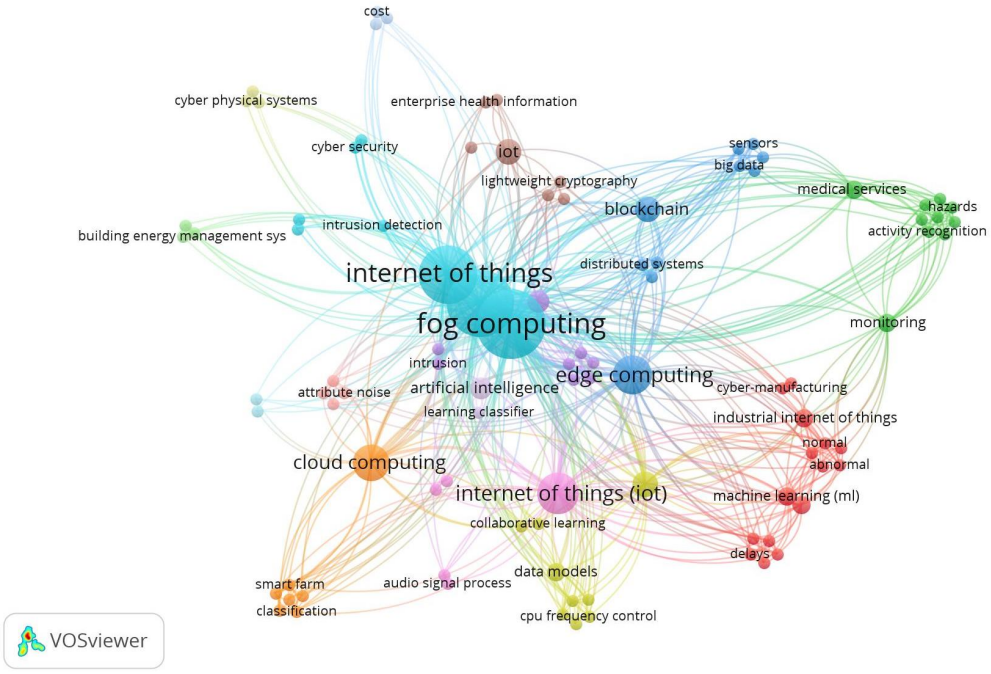

Figure 6. IoT-machine learning-Fog computing publication analysis from 2010 to 2021.

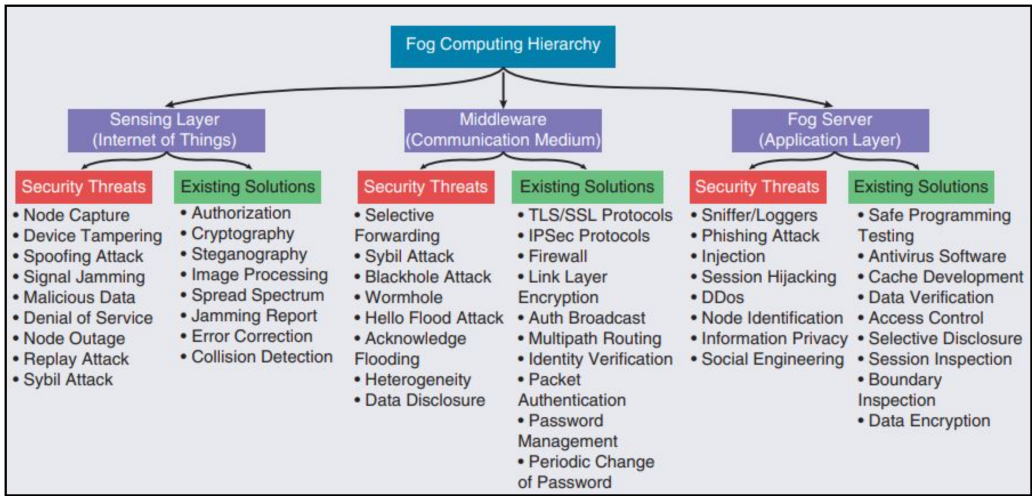

Figure 7. Fog computing challenges.

6. Research Directions

There are several important issues that Fog computing must deal with in a security context. Finally, a summary of possible study directions is provided.

6.1. Management of Trust

Identifying reliable Fog nodes in the Fog platform is difficult. Malicious activity is usually a good indicator of whether or not a Fog node is trusted or untrusted. For a Fog node, the malevolent nature is not specified. Therefore, defining and categorizing all of the Fog system's harmful properties is critical. The system can be vulnerable to regulation if one or more Fog nodes are trusted or seen as suspicious. That is why a high-level trust management model is a must in today's business environment. Cloud-Fog-IoT systems necessitate mixing dispersed and central environments, which presents another research challenge. As a result, the IoT environment necessitates using a Fog platform for trust management. As a result, it remains a difficult study topic. Even more importantly, the architecture and service delivery methods of the Fog and cloud computing platforms necessitate alternative trust management systems. Fog is widely dispersed, but the cloud is concentrated. Because the cloud platform has its security architecture, deploying trust management in that environment is easier than deploying trust management in the Fog platform, which is more open and lacks in-place security mechanisms. Because of this, the Fog environment is prone to malicious attacks. Additionally, trust in the cloud environment is one-way, but trust in the Fog environment is two-way. As part of the Fog platform, the Fog node and the IoT devices must have a trusting connection before communicating. Since the Fog and the IoT platforms are intertwined, creating an appropriate trust mechanism for both is very problematic.

6.2. Confidentiality Assessment

The Fog nodes are located close to the end users, so they store sensitive or private information. As a result, it is not easy to provide a safe connection between Fog and IoT devices and create a secure computing environment. Before transmitting it to the Fog nodes, we might consider encrypting any user-sensitive data. Traditional encryption and decryption procedures need a lot of CPU power, but IoT devices confront difficulties encrypting and decrypting users' sensitive data because of their resource limits. One Fog node may be able to handle sensitive data from several Fog users or multiple applications. After the data aggregation stage, there is a potential that diverse sources of data will be mixed up. At the Fog API or middleware level, correct data encapsulation strategies may be enforced to solve this issue. End-user devices, which are commonly involved in sharing sensitive resources such as location and personal information with other spatially linked devices, have another difficult challenge in the Fog environment: providing context-aware

services. Therefore, data protection must be in place in such a situation. Because of this, it is difficult to maintain the anonymity of one's identity and whereabouts in the Fog environment.

6.3. Authentication

Strong authentication and secure communication protocols are lacking from the Fog platform, which limitation is a blatant reality. An unsettling warning has been sent out to the scientific community. There has not been much investigation into authentication techniques in Fog computing. The Fog platform is still unable to be dealt with. To build and construct a new authentication technique for Fog computing, one must consider the following requirements and how they can work seamlessly with the Fog platform.

1. Users, end devices (IoT), applications, and service providers must all be able to use the same authentication mechanisms on the cloud-Fog platform.
2. IoT devices have a limited number of resources and must be able to scale up and down with a secure, environmentally friendly, efficient, and scalable solution. Conventional authentication procedures are inefficient. Different context-specific devices and applications demand high levels of security and performance.
3. Nodes in the Fog network depart and join dynamically. Hence, this need must consider the dynamic behavior of the Fog environment.
4. As a result, the Fog network's scalability must be ensured using low-complexity-based authentication.
5. A dynamic approach to authentication and reauthentication must be maintained.
6. The Fog system and IoT devices should use a cryptographic lightweight encryption technique that can easily handle the low processing capacity of IoT devices as an efficient authentication mechanism.
7. In exchange for its high usability and low cost, authentication should be user-friendly.

6.4. Access Management

Access control approaches in the Fog computing environment have not received much attention from researchers. However, there has already been much research conducted in this area. This means that we must continue developing an effective strategy for creating the correct sort of access and control models to provide a safe platform for heterogeneous Fog devices. Several access control models were discussed in the description section, each with a specific set of features or qualities while also highlighting several disadvantages and limits specific to the Fog environment. Cloud, Fog, and IoT security experts agree that attribute-based encryption (ABE) is a viable option for securing access to data in these types of settings. The ABE method should be reconstructed due to the heterogeneous Fog system features to minimize the primary issues (latency, policy management, fine-grained quality, and being enforced by the cryptographic technique) among cloud-Fog-IoT computing environment users. On the other hand, in the Fog system, data originate and are encrypted and decrypted by small, low-power devices. Deploying systems for limiting access to these devices would be a significant burden, necessitating a significant amount of processing power. In the meantime, Fog devices are being installed near the end devices. On the other hand, the Fog devices are far more powerful than the end-user IoT gadgets. ABE-based access control with outsourced capacity might work in the Fog environment to get over the constraints of IoT devices. For example, dynamic Fog computing has many devices joining and exiting simultaneously. As a result, the policy and characteristics of the users would be dynamically re-evaluated. ABE-based access control systems must aid in generating, changing, and canceling user characteristics. Designing the revocation process for ABE-based access control would provide new difficulties, and how Fog works with the cloud environment throughout the revocation process would require more research. As a result, the following criteria must be taken into account while creating a new access control technique for the Fog platform:

1. Fog is a completely virtualized platform by design, and it allows a wide range of settings for the Fog network to operate.
2. Due to the nature of sharing resources across untrusted tenants, a side-channeled attack may occur in this instance. As a result, a top priority is building an access control system that can work effectively and securely in a virtualized platform and multitenant environment.
3. Access control for the Fog environment must be safe, efficient, and attribute-based, considering minimal computation with outsourced capabilities and characteristics that can regulate user revocation capability.
4. A lightweight and fine-grained access control mechanism is needed because of the resource limits faced by IoT devices.

As a result, an access control mechanism must operate in a both central and dispersed architectural context correctly.

6.5. Attacks and Threats

As we discussed before, there are several security and privacy concerns with Fog computing. Because of the large number of interconnected devices and the spread architecture of the network, an attack or threat is always a possibility. Several dangers and attacks and their influence on the Fog environment have previously been mentioned in the descriptive section. The dynamic computing environment of Fog would make it difficult to detect, identify, and mitigate these risks and attacks. Research gaps and a lack of security solutions to detect and identify these risks and attacks need to be solved to establish a trustworthy Fog platform. As a result of our research into a variety of threats and attacks, we have identified the following concerns that must be addressed:

1. Complex trust issues and insecure authentication and authorization systems are to blame for these problems.
2. Fog nodes, or servers in the Fog layer, may be dynamically created, deleted, joined, and left.
3. Fog nodes constantly leave and rejoin, making detecting malicious or rogue nodes a difficult operation.
4. Creating a large-scale, geographically dispersed IDS implementation with low-latency need and high mobility Fog computing system is a difficult challenge.
5. It is necessary to use hybrid detection approaches to catch malicious activity in a dispersed context.
6. Designing high-security and low-cost threat and attack detection in the Fog environment is a major challenge because of Fog devices' resource limits. For example, we must be able to identify and prevent attacks from both Fog nodes and Fog users simultaneously.

6.6. Secure 5G Fog Network

The 5G network will be used to link Fog gadgets. New security difficulties arise when connecting Fog devices to the 5G network, particularly in the authentication process. The old one-way or mutual authentication technique is no longer relevant because of how authentication works between the user and service. We need a mixed authentication strategy in this situation. In the future, Fog will be important for communicating with gadgets and objects that use 5G. Suppose a resident in a smart city or smart house requires an ambulance to take him to a nearby specialist hospital where he may undergo remote surgery. It is necessary to use a hybrid security method to protect the entire application environment, as numerous parties are engaged in this procedure. Authentication in an emergency such as this needs a robust system. A 5G-enabled Fog computing environment is especially critical since user data may flow via numerous third-party devices, network equipment, and access networks that the user does not trust. As a result, in a 5G-enabled Fog network, we must look at hybrid authentication approaches and privacy protection. Some of the thematic open research challenges are depicted in Figure 8.

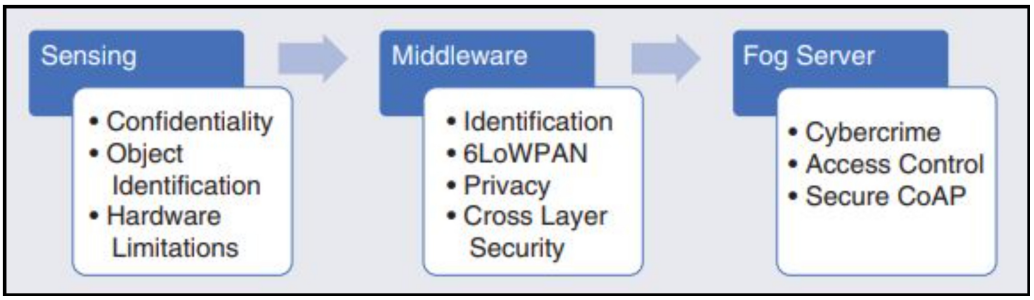

Figure 8. Fog computing: open research issues.

7. Conclusions

Through examining state-of-the-art research works on IoT security vulnerabilities, the current paper has addressed multiple ML approaches utilized in IoT security. First, the article lay out the backdrop for IoT expansion, including several instances of usage, scalability, and the massive quantity of data created. It then went over the most pressing security concerns with IoT devices and the underneath network. The focus then shifted to IoT security using ML approaches. First, the study defined the core ML tasks used in protecting IoT systems by evaluating various papers and websites. It then summarized publications on ML for IoT security, emphasizing anomaly detection, intrusion detection, and malware detection. The paper then went into Fog computing and ML approaches for the Fog environment. By being more context-aware, being able to spot concerns, and having reaction-oriented processing, ML at Fog nodes makes the IoT network more secure. For future works, IoT and Fog computing security mechanisms, compression approaches for IoT data, resource management of edge and Fog computing systems, and cloud computing would be among the priorities.

Author Contributions: Conceptualization, T.A.A. and F.G.; Data curation, Y.B.; Formal analysis, U.T.; Funding acquisition, A.I.; Investigation, U.T.; Methodology, T.A.A.; Project administration, I.U.; Resources, U.T.; Software, A.I., I.U. and Y.B.; Supervision, F.G.; Validation, A.I.; Writing—original draft, T.A.A.; Writing—review & editing, I.U. All authors have read and agreed to the published version of the manuscript.

Funding: Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia, project number (IF-PSAU-2021/01/17867).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: This submission does not include human or animal research.

Data Availability Statement: There are no data associated with this article.

Acknowledgments: The authors extend their appreciation to the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number (IF-PSAU-2021/01/17867).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gill, S.S. A Manifesto for Modern Fog and Edge Computing: Vision, New Paradigms, Opportunities, and Future Directions. In *Operationalizing Multi-Cloud Environments*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 237–253.
2. Ammi, M.; Alarabi, S.; Benkhelifa, E. Customized blockchain-based architecture for secure smart home for lightweight IoT. *Inf. Process. Manag.* **2021**, *58*, 102482. [CrossRef]
3. Xiang, G.; Zhu, X.; Ma, L.; Huang, H.; Wu, X.; Zhang, W.; Li, S. Clinical guidelines on the application of Internet of Things (IOT) medical technology in the rehabilitation of chronic obstructive pulmonary disease. *J. Thorac. Dis.* **2021**, *13*, 4629. [CrossRef] [PubMed]
4. Muller, H.; Mayrhofer, M.T.; Van Veen, E.B.; Holzinger, A. The Ten Commandments of ethical medical AI. *Computer* **2021**, *54*, 119–123. [CrossRef]
5. Shapiro, A. 'Embodiments of the invention': Patents and urban diagrammatics in the smart city. *Convergence* **2020**, *26*, 751–774. [CrossRef]

6. Pong, P.W.; Annaswamy, A.M.; Kroposki, B.; Zhang, Y.; Rajagopal, R.; Zussman, G.; Poor, H.V. Cyber-enabled grids: Shaping future energy systems. *Adv. Appl. Energy* **2021**, *1*, 100003. [CrossRef]
7. Edwards, C. Real-time advanced analytics, automated production systems, and smart industrial value creation in sustainable manufacturing Internet of Things. *J. Self-Gov. Manag. Econ.* **2021**, *9*, 32–41.
8. Moh, M.; Raju, R. Machine learning techniques for security of Internet of Things (IoT) and fog computing systems. In Proceedings of the 2018 International Conference on High Performance Computing & Simulation (HPCS), Orléans, France, 20 July 2018; pp. 709–715.
9. Ungurean, I.; Gaitan, N.C. Software Architecture of a Fog Computing Node for Industrial Internet of Things. *Sensors* **2021**, *21*, 3715. [CrossRef]
10. Holzinger, A.; Weippl, E.; Tjoa, A.M.; Kieseberg, P. Digital transformation for sustainable development goals (sdgs)-a security, safety and privacy perspective on ai. In *International Cross-Domain Conference for Machine Learning and Knowledge Extraction*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–20.
11. Liu, Y.; Wei, X.; Xiao, J.; Liu, Z.; Xu, Y.; Tian, Y. Energy consumption and emission mitigation prediction based on data center traffic and PUE for global data centers. *Glob. Energy Interconnect.* **2020**, *3*, 272–282. [CrossRef]
12. Leyden, J. Water treatment plant hacked, chemical mix changed for tap supplies. *Register* **2016**. Available online: https://www.theregister.com/2016/03/24/water_utility_hacked/ (accessed on 2 February 2022).
13. Brand, R.; Timme, S.; Nosrat, S. When pandemic hits: Exercise frequency and subjective well-being during COVID-19 pandemic. *Front. Psychol.* **2020**, *11*, 2391. [CrossRef]
14. Puat, H.A.M.; Abd Rahman, N.A. IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. *J. Phys. Conf. Ser.* **2020**, *1712*, 012009. [CrossRef]
15. Aazam, M.; Zeadally, S.; Harras, K.A. Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4674–4682. [CrossRef]
16. Li, D.; Deng, L.; Cai, Z.; Souri, A. Blockchain as a service models in the Internet of Things management: Systematic review. *Transactions on Emerging Telecommunications Technologies;* Wiley: Hoboken, NJ, USA, 2020; p. e4139.
17. Rizvi, S.; Orr, R.; Cox, A.; Ashokkumar, P.; Rizvi, M.R. Identifying the attack surface for IoT network. *Internet Things* **2020**, *9*, 100162. [CrossRef]
18. Khormali, A.; Park, J.; Alasmary, H.; Anwar, A.; Saad, M.; Mohaisen, D. Domain name system security and privacy: A contemporary survey. *Comput. Netw.* **2021**, *185*, 107699. [CrossRef]
19. Shim, J.P.; Sharda, R.; French, A.M.; Syler, R.A.; Patten, K.P. The Internet of Things: Multi-faceted research perspectives. *Commun. Assoc. Inf. Syst.* **2020**, *46*, 21. [CrossRef]
20. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. *Comput. Sci. Rev.* **2020**, *38*, 100312. [CrossRef]
21. Tahsien, S.M.; Karimipour, H.; Spachos, P. Machine learning based solutions for security of Internet of Things (IoT): A survey. *J. Netw. Comput. Appl.* **2020**, *161*, 102630. [CrossRef]
22. Azad, T. *Securing Citrix XenApp Server in the Enterprise*; Syngress: Waltham, MA, USA, 2008.
23. Schubert, E.; Sander, J.; Ester, M.; Kriegel, H.P.; Xu, X. DBSCAN revisited, revisited: Why and how you should (still) use DBSCAN. *ACM Trans. Database Syst. (TODS)* **2017**, *42*, 1–21. [CrossRef]
24. Hamerly, G.; Elkan, C. Learning the k in k-means. *Adv. Neural Inf. Process. Syst.* **2004**, *16*, 281–288.
25. Chen, Y.; Zheng, W.; Li, W.; Huang, Y. Large group activity security risk assessment and risk early warning based on random forest algorithm. *Pattern Recognit. Lett.* **2021**, *144*, 1–5. [CrossRef]
26. Uddin, M.P.; Mamun, M.A.; Hossain, M.A. PCA-based feature reduction for hyperspectral remote sensing image classification. *IETE Tech. Rev.* **2021**, *38*, 377–396. [CrossRef]
27. Zhang, H.; Jiang, L.; Yu, L. Attribute and instance weighted naive Bayes. *Pattern Recognit.* **2021**, *111*, 107674. [CrossRef]
28. Chen, W.; Wang, L.; Ren, W.; Zhao, J.; Wang, Z.; Quan, Y.; Zhuang, J. Effect of BaZrO3 amounts on the domain structure and electrical properties of lead-free piezoelectric KNN-based films. *Mater. Sci. Eng. B* **2022**, *276*, 115552. [CrossRef]
29. Chen, Y.; Huang, W.; Nguyen, L.; Weng, T.W. On the Equivalence between Neural Network and Support Vector Machine. *Adv. Neural Inf. Process. Syst.* **2021**, *34*. Available online: https://arxiv.org/abs/2111.06063 (accessed on 2 February 2022).
30. Guo, H.; Nguyen, H.; Bui, X.N.; Armaghani, D.J. A new technique to predict fly-rock in bench blasting based on an ensemble of support vector regression and GLMNET. *Eng. Comput.* **2021**, *37*, 421–435. [CrossRef]
31. Haruna, S.; Malami, S.I.; Adamu, M.; Usman, A.; Farouk, A.; Ali, S.I.A.; Abba, S. Compressive Strength of Self-Compacting Concrete Modified with Rice Husk Ash and Calcium Carbide Waste Modeling: A Feasibility of Emerging Emotional Intelligent Model (EANN) Versus Traditional FFNN. *Arab. J. Sci. Eng.* **2021**, *46*, 11207–11222. [CrossRef]
32. Castillo, I.; Ročková, V. Uncertainty quantification for Bayesian CART. *Ann. Stat.* **2021**, *49*, 3482–3509. [CrossRef]
33. Montgomery, D.C.; Peck, E.A.; Vining, G.G. *Introduction to Linear Regression Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2021.
34. Hubona, G.S.; Schuberth, F.; Henseler, J. A clarification of confirmatory composite analysis (CCA). *Int. J. Inf. Manag.* **2021**, *61*, 102399. [CrossRef]
35. Yousefi, S.; Derakhshan, F.; Karimipour, H. Applications of big data analytics and machine learning in the internet of things. In *Handbook of Big Data Privacy*; Springer: Cham, Switzerland, 2020; pp. 77–108.

36. Agrawal, P.; Trivedi, B. Machine learning classifiers for Android malware detection. In *Data Management, Analytics and Innovation*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 311–322.
37. Nakhodchi, S.; Upadhyay, A.; Dehghantanha, A. A comparison between different machine learning models for iot malware detection. In *Security of Cyber-Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 195–202.
38. Saharkhizan, M.; Azmoodeh, A.; HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G. *A Hybrid Deep Generative Local Metric Learning Method for Intrusion Detection*; l2020. Available online: https://doi.org/10.1007/978-3-030-38557-6_16 (accessed on 2 February 2022).
39. Ramalingam, A. Child and Women's Safety with Wearable Devices: Wearable devices for security. *SPAST Abstr.* **2021**, *1*. Available online: https://spast.org/techrep/article/view/1985 (accessed on 2 February 2022).
40. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A machine learning security framework for iot systems. *IEEE Access* **2020**, *8*, 114066–114077. [CrossRef]
41. Łaskawiec, S.; Choraś, M.; Kozik, R.; Varadarajan, V. Intelligent operator: Machine learning based decision support and explainer for human operators and service providers in the fog, cloud and edge networks. *J. Inf. Secur. Appl.* **2021**, *56*, 102685.
42. Zhang, C. Design and application of fog computing and Internet of Things service platform for smart city. *Future Gener. Comput. Syst.* **2020**, *112*, 630–640. [CrossRef]
43. Rauf, A.; Shaikh, R.A.; Shah, A. Security and privacy for IoT and fog computing paradigm. In Proceedings of the 2018 15th Learning and Technology Conference (L&T), Jeddah, Saudi Arabia, 25–26 February 2018; pp. 96–101.
44. Wang, T.; Zhang, G.; Bhuiyan, M.Z.A.; Liu, A.; Jia, W.; Xie, M. A novel trust mechanism based on fog computing in sensor–cloud system. *Future Gener. Comput. Syst.* **2020**, *109*, 573–582. [CrossRef]
45. Rahman, F.H.; Au, T.W.; Newaz, S.S.; Suhaili, W.S.; Lee, G.M. Find my trustworthy fogs: A fuzzy-based trust evaluation framework. *Future Gener. Comput. Syst.* **2020**, *109*, 562–572. [CrossRef]
46. Soleymani, S.A.; Abdullah, A.H.; Zareei, M.; Anisi, M.H.; Vargas-Rosales, C.; Khan, M.K.; Goudarzi, S. A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access* **2017**, *5*, 15619–15629. [CrossRef]
47. Yuan, J.; Li, X. A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion. *IEEE Access* **2018**, *6*, 23626–23638. [CrossRef]
48. Dang, T.D.; Hoang, D. A data protection model for fog computing. In Proceedings of the 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), Valencia, Spain, 8–11 May 2017; pp. 32–38.
49. Wang, H.; Wang, Z.; Domingo-Ferrer, J. Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 712–719. [CrossRef]
50. Yang, R.; Xu, Q.; Au, M.H.; Yu, Z.; Wang, H.; Zhou, L. Position based cryptography with location privacy: A step for fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 799–806. [CrossRef]
51. Kumar, P.; Zaidi, N.; Choudhury, T. Fog computing: Common security issues and proposed countermeasures. In Proceedings of the 2016 International Conference System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 25–27 November 2016; pp. 311–315.
52. Liu, J.; Li, J.; Zhang, L.; Dai, F.; Zhang, Y.; Meng, X.; Shen, J. Secure intelligent traffic light control using fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 817–824. [CrossRef]
53. Qin, Z.; Yi, S.; Li, Q.; Zamkov, D. Preserving secondary users' privacy in cognitive radio networks. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 772–780.
54. Ibrahim, M.H. OCTOPUS: An edge-fog mutual authentication scheme. *Int. J. Netw. Secur.* **2016**, *18*, 1089–1101.
55. Yu, Z.; Au, M.H.; Xu, Q.; Yang, R.; Han, J. Towards leakage-resilient fine-grained access control in fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 763–777. [CrossRef]
56. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V. Design of secure key management and user authentication scheme for fog computing services. *Future Gener. Comput. Syst.* **2019**, *91*, 475–492. [CrossRef]
57. Dsouza, C.; Ahn, G.J.; Taguinod, M. Policy-driven security management for fog computing: Preliminary framework and a case study. In Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014), Redwood City, CA, USA, 13–15 August 2014; pp. 16–23.
58. Alharbi, S.; Rodriguez, P.; Maharaja, R.; Iyer, P.; Subaschandrabose, N.; Ye, Z. Secure the internet of things with challenge response authentication in fog computing. In Proceedings of the 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, 10–12 December 2017; pp. 1–2.
59. Amor, A.B.; Abid, M.; Meddeb, A. A privacy-preserving authentication scheme in an edge-fog environment. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; pp. 1225–1231.
60. Hu, P.; Ning, H.; Qiu, T.; Song, H.; Wang, Y.; Yao, X. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet Things J.* **2017**, *4*, 1143–1155. [CrossRef]
61. Ha, D.A.; Nguyen, K.T.; Zao, J.K. Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol. In Proceedings of the Seventh Symposium on Information and Communication Technology, Ho Chi Minh, Vietnam, 8–9 December 2016; pp. 173–179.
62. Fan, K.; Wang, J.; Wang, X.; Li, H.; Yang, Y. A secure and verifiable outsourced access control scheme in fog-cloud computing. *Sensors* **2017**, *17*, 1695. [CrossRef]

63. Lu, R.; Heung, K.; Lashkari, A.H.; Ghorbani, A.A. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* **2017**, *5*, 3302–3312. [CrossRef]
64. Zhang, P.; Chen, Z.; Liu, J.K.; Liang, K.; Liu, H. An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 753–762. [CrossRef]
65. Vohra, K.; Dave, M. Multi-authority attribute based data access control in fog computing. *Procedia Comput. Sci.* **2018**, *132*, 1449–1457. [CrossRef]
66. Popa, L.; Yu, M.; Ko, S.Y.; Ratnasamy, S.; Stoica, I. CloudPolice: Taking access control out of the network. In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Monterey, CA, USA, 20–21 October 2010; pp. 1–6.
67. Gope, P.; Sikdar, B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet Things J.* **2018**, *6*, 580–589. [CrossRef]
68. Xiao, M.; Zhou, J.; Liu, X.; Jiang, M. A hybrid scheme for fine-grained search and access authorization in fog computing environment. *Sensors* **2017**, *17*, 1423. [CrossRef]
69. Zaghdoudi, B.; Kaffel-Ben Ayed, H.; Harizi, W. Generic access control system for ad hoc MCC and fog computing. In *International Conference on Cryptology and Network Security*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 400–415.
70. Yavuz, F.Y. Deep Learning in Cyber Security for Internet of Things. Master's Thesis, Fen Bilimleri Enstitüsü, Istanbul, Turkey, 2018.
71. Torres, P.; Catania, C.; Garcia, S.; Garino, C.G. An analysis of recurrent neural networks for botnet detection behavior. In Proceedings of the 2016 IEEE Biennial Congress of Argentina (ARGENCON), Buenos Aires, Argentina, 15–17 June 2016; pp. 1–6.
72. Canedo, J.; Skjellum, A. Using machine learning to secure IoT systems. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 219–222.
73. Wang, N.; Jiang, T.; Lv, S.; Xiao, L. Physical-layer authentication based on extreme learning machine. *IEEE Commun. Lett.* **2017**, *21*, 1557–1560. [CrossRef]
74. Yousefi-Azar, M.; Varadharajan, V.; Hamey, L.; Tupakula, U. Autoencoder-based feature learning for cyber security applications. In Proceedings of the 2017 International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, USA, 14–19 May 2017; pp. 3854–3861.
75. Li, L.; Xiaoguang, H.; Ke, C.; Ketai, H. The applications of wifi-based wireless sensor network in internet of things and smart grid. In Proceedings of the 2011 6th IEEE Conference on Industrial Electronics and Applications, Beijing, China, 21–23 June 2011; pp. 789–793.
76. Aminanto, M.E.; Kim, K. Improving detection of Wi-Fi impersonation by fully unsupervised deep learning. In *International Workshop on Information Security Applications*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 212–223.
77. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]
78. Abeshu, A.; Chilamkurti, N. Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Commun. Mag.* **2018**, *56*, 169–175. [CrossRef]
79. Saied, A.; Overill, R.E.; Radzik, T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing* **2016**, *172*, 385–393. [CrossRef]
80. Chen, Y.; Zhang, Y.; Maharjan, S. Deep learning for secure mobile edge computing. *arXiv* **2017**, arXiv:1709.08025.
81. Shi, C.; Liu, J.; Liu, H.; Chen, Y. Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. In Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Chennai, India, 10–14 July 2017; pp. 1–10.
82. Alzaylaee, M.K.; Yerima, S.Y.; Sezer, S. DL-Droid: Deep learning based android malware detection using real devices. *Comput. Secur.* **2020**, *89*, 101663. [CrossRef]