future internet

MDPI

Article

A Survey on Intrusion Detection Systems for Fog and Cloud Computing

Victor Chang [1,*], Lewis Golightly [1], Paolo Modesti [1], Qianwen Ariel Xu [1], Le Minh Thao Doan [1], Karl Hall [1], Sreeja Boddu [1] and Anna Kobusińska [2]

[1] Cybersecurity, Information Systems and AI Research Group, School of Computing, Engineering and Digital Technologies, Teesside University, Middlesbrough TS1 3BX, UK; lewgol99@gmail.com (L.G.); p.modesti@tees.ac.uk (P.M.); qianwen.ariel.xu@gmail.com (Q.A.X.); minhthaodoanle@gmail.com (L.M.T.D.); drazarx3@gmail.com (K.H.); b.sreeja407@gmail.com (S.B.)

[2] Institute of Computing Science, Poznan University of Technology, 60-965 Poznan, Poland; anna.kobusinska@cs.put.poznan.pl

* Correspondence: victorchang.research@gmail.com

Abstract: The rapid advancement of internet technologies has dramatically increased the number of connected devices. This has created a huge attack surface that requires the deployment of effective and practical countermeasures to protect network infrastructures from the harm that cyber-attacks can cause. Hence, there is an absolute need to differentiate boundaries in personal information and cloud and fog computing globally and the adoption of specific information security policies and regulations. The goal of the security policy and framework for cloud and fog computing is to protect the end-users and their information, reduce task-based operations, aid in compliance, and create standards for expected user actions, all of which are based on the use of established rules for cloud computing. Moreover, intrusion detection systems are widely adopted solutions to monitor and analyze network traffic and detect anomalies that can help identify ongoing adversarial activities, trigger alerts, and automatically block traffic from hostile sources. This survey paper analyzes factors, including the application of technologies and techniques, which can enable the deployment of security policy on fog and cloud computing successfully. The paper focuses on a Software-as-a-Service (SaaS) and intrusion detection, which provides an effective and resilient system structure for users and organizations. Our survey aims to provide a framework for a cloud and fog computing security policy, while addressing the required security tools, policies, and services, particularly for cloud and fog environments for organizational adoption. While developing the essential linkage between requirements, legal aspects, analyzing techniques and systems to reduce intrusion detection, we recommend the strategies for cloud and fog computing security policies. The paper develops structured guidelines for ways in which organizations can adopt and audit the security of their systems as security is an essential component of their systems and presents an agile current state-of-the-art review of intrusion detection systems and their principles. Functionalities and techniques for developing these defense mechanisms are considered, along with concrete products utilized in operational systems. Finally, we discuss evaluation criteria and open-ended challenges in this area.

Keywords: cloud computing; intrusion detection and prevention; security; recommendations for cloud computing and security; recommendations for network security; defense techniques

Citation: Chang, V.; Golightly, L.; Modesti, P.; Xu, Q.A.; Doan, L.M.T.; Hall, K.; Boddu, S.; Kobusińska, A. A Survey on Intrusion Detection Systems for Fog and Cloud Computing. *Future Internet* **2022**, *14*, 89. https://doi.org/10.3390/fi14030089

Academic Editor: Carlos Filipe Da Silva Portela

Received: 19 February 2022
Accepted: 11 March 2022
Published: 13 March 2022

1. Introduction

The modern world has caused an absolute need for fast and efficient data. Many organizations see the need to integrate data efficiently and safely, apart from storing business data and datasets in database systems. The stored information and data require security measures to protect them from unauthorized personnel. The most crucial factors which

categorize an organization's data space are the performance of data backups, accessibility, and trustworthiness. Cloud computing as a specialist area refers to the performance of offering computing resources to safeguard and protect data accessibility from unauthorized personnel. The increasing organizational need for cloud computing brought unprecedented challenges for information security [1]. Intrusion detection and prevention are two broad terms referring to application safety performances measures used to mitigate attacks and respond to threats in real-time. The first term focuses on identifying and mitigating ongoing attacks, and the second one indicates a security measure used to prevent attacks on the target system. An intrusion detection system (IDS) is a software or device which continuously monitors the network to ensure that activity that may potentially signal that an attack is properly identified. Infrastructure, platform, and software are three different service models comprised of cloud computing that aid data protection. The computing services offered, including networking, servers, databases, software, and analytics intelligence, have been highlighted by the above service models' assistance. They offer more economies of scale, flexible resources, and rapid innovation in data encryption procedures. Heretofore, cloud security has been a major concern for many scientists as they claim that cloud computing has been an extended progression that hints at the past when computing systems were rare and not easily showcased. The mentioned software service models provide solutions that cloud computing technologies have been secured. The significant feature and the successful cloud computing have been identified by the accessibility of computer resources and services with many conveniences. Several types of intrusion detection systems and tools available on the market have been designed to protect personal information or vital organizations from being leaked because of unauthorized access. In intrusion detection, software and appliances should consider what sorts of offensive techniques can be used to apply countermeasures for effective prevention. Network intrusion techniques include flooding or overloading the network, exploiting vulnerabilities, injecting code, pivoting to attack other systems on the networks once the first host is compromised. With that in mind, it is imperative to maintain detection tools active at all stages to prevent an attack from escalating from the system periphery to the inner systems where usually the most valuable digital assets are stored. Intrusion detection systems can be considered as an extra layer of protection, implemented in either hardware or software or both, which integrates with all other measures enforced to protect an information system. IDS security works in combination with endorsement access power and substantiation, which used a twofold line of resistance against intrusion as its measurement. In essence, there are quite a few fundamental mechanisms related to intrusion detection preparation. Knowledge of potential intrusions, prevention of latent intrusions, awareness of previous intrusions, and actions in response to an intrusion will be required. In general, the fundamental action in defining efficient detection techniques that can improve future detection and prevent future attacks is understanding what kind of intrusions have taken place or have been attempted in the past. Moreover, awareness of the degree of the intrusion of an attack is extremely useful to shape measures such as appropriate policies or inform stakeholders. This paper presents various detection methodologies employed by intrusion detection and prevention approaches, considering their advantages and existing challenges.

1.1. Scope of the Study

This survey focuses on the various methodologies applied in intrusion detection and prevention systems, provides a survey on fog and cloud computing technologies, and recommends how organizations can adopt them. The detailed evaluations of techniques and the advantages and disadvantages of each technology are studied. Moreover, there is an examination of the many network topologies used alongside potential cyber threats. The study provides an overview of the possibilities of these systems and the essential qualities needed for the efficient and effective technological solutions and functions of fog and cloud computing and intrusion detection and prevention for both.

1.2. Background Information

One of the most crucial and high-value resources in cloud computing adoption for an organization or individual is data. It is of great importance that the management of the organization and individual in task allocation requires the assurance of integrity. The invention and innovation of database systems have improved data storage and management and eventually increased their usefulness for organizations and individuals needing to use this technology.

Cloud computing is a computing innovation technology that provides convenience and on-demand network access to computing resources based on strategies in a shared pool, and it can be easily and quickly released and supplied. There is little effort needed to manage and interact with the service provider when using this service. Novel models of cloud computing allow to incorporate applications, platforms, and infrastructure that have previously been used to provide information technology solutions. These technological solutions are composed of all categories based on availability on the internet. Cloud-based applications incorporate online file storage, webmail, online business applications, and social networking sites. Cloud computing technology is a very well-established solution due to the accessibility and influence of technology advancement. The mitigations that enable a business to have low costs in computing infrastructure and operations have resulted in moving critical resources to the cloud environment resulting in significant computing growth. It has been assessed and analyzed that it can work more effectively than the other solutions that can be offered [1,2]. However, security issues are presented to be a critical matter when businesses start to outsource data and applications to cloud computing providers.

1.3. Cloud Computing Security

The concept of cybersecurity is the assurance of safety from the activity of multiple entities (human and not), both internal and external, physically and in the cyberspace domain. Cybersecurity is classically characterized by the CIA triad:

1. Confidentiality: This is the assurance that user information is kept private from unauthorized agents to access.
2. Integrity: This is the assurance of data remaining accurate and unmodified from the original state.
3. Availability: This assurance of data reliability is readily accessible to the authorized personnel upon request.

To securely implement cloud computing technology, cybersecurity must be considered and applied to protect the information of the involved users. Keeping cybersecurity at the forefront of cloud-based environments aids in reducing the cyber threat risks and the assurance of compliance with rules and regulations set to ensure information security. A significant amount of Information Technology professionals is aware of cloud computing as a domain. Therefore, they should spend a significant amount of time understanding the security characteristics portrayed in cloud computing and related vulnerabilities. The increasing demands and adoption of computing can lead to improvements in the quality of services and user requirements. Web development has resulted in countless challenges, which can notably include the availability of massive data on the Internet—this has created an increase of servers with substantial storage capacity, enabling huge cloud storage capacity over vast geographical areas throughout the world.

According to NIST, cloud computing is defined as a model that realizes the on-demand network accessibility, convenience, and ubiquity of computing resource configuration, including networks, storage, services, servers, and applications. They are provided and released quickly and do not require significant management or service provider interaction.

The technology embedded in cloud computing covers five critical features: broad network access, a measured service, on-demand self-service, resource pooling, as well as the ability to have rapid elasticity. Service delivery models have different implementations, which make it complex to develop a standard security model that can be implemented

by end-users of cloud computing. The service models include Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS).

There are four deployment models for cloud computing, classified as three basic and widely used deployment models: public, private, and hybrid clouds, and a less commonly employed model known as the community cloud.

1. A private cloud is deployed and managed within a single organization.
2. A public cloud is deployed and managed in a third-party organization.
3. A hybrid cloud consists of private and public cloud technologies.
4. A community cloud consists of sharing computing resources within multiple organizations and has the management operations completed by an in-house IT department or third party.

There have been questions in the scientific community related to the significance of cloud computing. The management of these models can be extremely complicated, especially around meeting the cybersecurity needs around conflict and mitigation at the cloud level. The technology can require significant costs, including associated licenses with security solutions and resources, which are critical elements in achieving the standard and level of security needed—this can be a complex problem. Cloud providers need to pay close attention to the interests and requirements of end-users and seek suitable new security solutions to address users' concerns.

The paper in [2] uses an approach that focuses on a method for Software-as-a-Service (SaaS) threat model relating to the cloud service providers. According to this study, the SaaS methodology is a dominant and widely used cloud model as it minimizes the investment and acquisition cost of the consumer and simplifies deployment. The methodology consists of numerous critical characteristics, such as excellent compatibility over different devices and the automated system that will easily automate updates, allowing it to easily adjust products to meet the client's needs and be accessible over a wide area covering many locations. In recent times, the SaaS model has succeeded due to the benefits it showcases and, therefore, is secured. This paper's main highlight is providing a solution to the security problem related to the SaaS to a cloud computing environment model. The proposed model also supports performing professional security audits. Therefore, this model will save money and time with a preferred level of security being desired in the cloud environment.

The ability to pay for cloud-based systems and resources is an option and allows users to use the resources only at the required time. It is a good strategy to purchase and employ the most up-to-date technique. Elements that are vital to on-demand Infrastructure as a Service (IaaS) consist of customer isolation, multi-tenancy, and self-sustainability. However, cloud computing providers may adopt a level of control over users to create applications on top of the platform and security at the application level such as host, and intrusion prevention remains within the scope of providers. The service providers should offer appropriate assurances on the data's continued accessibility within apps. Three fundamental concepts are privacy, confidentiality, and obligations. These three are fundamental elements that contribute to privacy and confidentiality.

Multitenancy is about sharing resources, where several users can share identical resources at various levels of the cloud domain, including the host level, the network level, and the application level. The services within cloud computing have different aspects that consist of the technology, including electronic health record websites, video sites, and data storage availability. There are two different application storage methods, namely, single cloud providers and many cloud providers. For example, a user's contents can be stored using a single cloud provider or many different cloud providers. Multitenancy implies the performance of sharing computational resources and storage as well as services and applications for different users.

In the work in [3], it has been observed that multitenancy can be a leading cause of cybersecurity issues in fog and cloud-based environments. Multitenancy methods do not provide local privacy and require the location of the data to be controlled by users in the cloud-based environment. The multitenancy feature is designed to ensure sufficient

resources are utilized and services and costs are available. This can result in the data of different users residing in the same location. The multitenancy in cloud service concentrates on a variety of requirements that can result in network security issues. These market elements include billing models, information governance, policy-driven enforcement, service levels, isolation for different user divisions.

Elasticity is the property of adding and subtracting computing resources on-demand and releasing them when other resources are not in use. This can allow users the option to use the resources allocated previously, but it can represent a confidentiality threat in the cloud computing domain.

1.4. Research Methodology

Various tactics and strategies were employed to achieve the survey's objectives. We chose the exploration approach to address the research questions and goals of the survey. Specifically, the applied research methodology includes a systematic approach in which the research problems are identified, managed, and practical solutions are proposed. Consequently, the analysis to develop new ideas and transparent information about the issues was carried out by applying this approach, similarly to [4].

The research methodology used in this paper involves two review strategies.

The first strategy is a systematic literature review applied to identify, evaluate, and interpret the available influential studies in the specific area of interest. A systematic literature review was mainly performed to summarize existing recent and relevant academic literature and evaluate the currently available work opportunities. This helped us identify the results of research in the published work relating to the research study being undertaken.

The second strategy was to use online resources and journals that include recent and relevant academic literature in computer science. We used relevant research databases such as the ACM digital library, Science Direct, IEEEXplore, as well as Google Scholar. Our focus was on exploring titles, abstracts, keywords, and articles that include the terms 'cloud computing', 'cloud security', 'intrusion detection', 'intrusion prevention', 'IDS', 'SDN', and 'cloud privacy'. We refine our work and present important points for fog and cloud, as well as for security and privacy for both.

1.5. Contributions and Goals

This paper provides a deep survey on fog and cloud computing and intrusion detection and prevention systems. As the paper aims to enhance the current cybersecurity strategies deployed in businesses, we focus on the organizational adoption of such solutions and present selected examples from health and education sectors in different countries: China, Poland, and the United Kingdom.

In detail, the main objective of this survey paper is to provide an in-depth summary and survey of intrusion detection and prevention and cloud computing technology that can be adopted in the development of cloud security initiatives and productive intrusion detection and prevention solutions. The review of past research enables the investigation of several comparative facets of security policies involved in the cloud computing environment. It has also been a requirement for cloud providers concerning data security and, therefore, it aids in contributing to a scientific group of cloud computing security and development of cloud security policy.

The paper also sets out to achieve the following goals:

1. Proposing a methodology to identify new rules that should be operated in addition to cloud security policies and can be employed to evaluate the threats against cloud-based environments;
2. Reviewing detailed studies addressing fog computing and intrusion detection security issues;

3. Reviewing the available threats which can affect fog computing environments and intrusion detection technology, with a specific focus on the ones that cannot be employed in conventional systems;
4. Identifying security regulations and policies, particularly the most preferred recommendations for Software-as-a-Service security guidelines.

2. Security Overview

2.1. Service-Oriented Systems, Applications, and Security

According to IBM, service-oriented systems are 'described as an approach that enables software components to be interoperable and reusable through service interfaces'. This technology works by integrating services into applications using general interface standards and architectural patterns [5,6]. These systems are used primarily for web services and demonstrate significant importance, focusing on the many benefits it provides, including reliability, location independence, scalability, platform independence, reusability, agility, and easy maintenance. Recent academic literature [7] shows the deployment of service-oriented systems and their scale in the real world for software, AI, big data, and Internet of Things as services. The paper introduces service-oriented computing, as well as the essentials in service-oriented software development. Throughout the literature, the authors then move on to discussing the dependability of service-oriented software, including quality of service and reliability properties, security issues for SOA software, and reputation management systems.

In further literature, we can evaluate the security of service-oriented systems [8]. The paper focuses on multiple factors for devising countermeasures for SOA vulnerabilities. The factors include protocols, network paths, vulnerabilities, automotive attacks, and comparison to IT security. The countermeasures that can be deployed include firewalls, intrusion detection systems and identity and access management. Finally, throughout relevant work, this paper conveys the further opportunities currently available for this technology [9]. We can see the future landscape for service-oriented systems and the horizon for this technology. The authors discuss future directions for research in this domain, including businesses and society, services in organizations, services for software-defined networks, services for the Internet of Things (IoT), services in the cloud or on the edge, services and data, and service engineering and management.

Service orientation is a methodology for developing software systems that emphasizes standardization, well-defined interfaces, platform independence, as well as tool support (that even facilitates the integration of legacy systems). In [10], the authors investigate the use of service-oriented architecture for 5G systems. By adopting service aggregation and caching (SAaC) schemes, the network traffic congestion can be reduced, and network administration can be simplified. The Network model consists of multiple layers of architecture—these layers include the data acquisition layer, network routing layer, data center, and application layer. To conclude, service-oriented systems provide a successful measure to reduce the data transmission volume.

In other recent literature [11], the authors explore the cyber threat landscape when using a service-oriented architecture focusing on the threat modeling phase of attacking and defending a system. The research proposes that the users take some responsibility for thinking about the attack vectors and threat actors, which is usually formally a task of the internet service provider (ISP). The cloud services are described as having four generic properties: data storage, data processing, data transfer, and authentication. The usual method of cyber threat analysis is to take all four properties as the basis for analyzing a select number of threats that apply to cloud services. However, the authors state that while this approach is useful, it falls short of comprehensively analyzing the full computing environment.

In a study, the researchers examined the current process for intrusion detection and prevention in service-oriented vehicular networks [12]. They began by looking at common attacks associated with service-oriented networks: Sybil attacks, DoS attacks, and False alerts generation attacks. They then evaluated the volume of intrusion detection agents by

proposing a detection method that works by using an IDS agent for each vehicle, filtering its neighbors, using promiscuous patterns, and applying inspection protocols to each attack. This method works by using a greedy forwarding protocol that works by the furthest vehicle from the collaborating vehicle forwarding the transmitted packets. As a result, in the case where vehicle 2 is a forwarding node, it is expected to be mainly positioned at the edge of vehicle 1's radio range. To mitigate against these common attacks, they propose a rule-based intrusion detection technique that can be used to defend against common attacks such as Sybil and DoS attacks. The authors also provide a table that compares Alerts to expected behavior—this can be particularly helpful. For example, an 'Alert' may be 'Emergency Electronic Brake Lights' and the 'Expected behavior' would be 'Vehicle Must Slow Down'.

Finally, in another study, we can see how we measure and mitigate cybersecurity risks and vulnerability in service-oriented architectures [13]. The authors outline the most dangerous security vulnerabilities linked to this type of computing, including software weaknesses in the development that can escalate to software vulnerabilities—unless this is noticed. Mitigation methods have been successfully deployed, which can present a disastrous threat landscape. These threats include the following cyber-attacks: channel and path errors, common special element manipulations, structure and validity problems, format strings, buffer overflows, user interface errors, and many more. To mitigate attacks, the authors convey several methods, including business continuity management, incident management procedures, operations management, security of systems and facilities, human resources security, information governance and risk management, monitoring, auditing, and testing. The research highlights that the risks will vary between service providers and are dependent on features such as the provider type and service type.

2.2. Review of Cloud Security

Cloud security is an extremely significant deployment, maintenance, and continuity phase for the business running the infrastructure. According to [14], the most important practices for ensuring cloud security are due diligence, access management, data protection, as well as surveillance and defense. Furthermore, they identified key risk examples, including unsecured storage services, email compromise, data loss, systems and data destruction, data breaches, ransomware attacks, and supply chain attacks. Despite the cloud security measures we may deploy and the mitigations we take, there are prominent issues in cloud security. The authors investigate cloud-based web applications countermeasures for various common attacks, which include Cross-Site Scripting (XSS) and SQL injection for different cloud service models such as IaaS, PaaS, and SaaS by using the form of penetration testing to provide successful mitigation. The paper makes use of a table to provide a concise comparison between vulnerability scanning tools (used in the formative stages of a penetration test framework). With comparisons between WebScarab, OWASP ZAP, Uniscan, Nikto, and W3af, ZAP is the most effective in testing cloud environments for finding the mainstream attack vectors.

In the work of [15], the authors discuss advances in cloud security by developing SaaS by deploying a reliable cloud service architecture that can perform policy customization. They produce an overview of the proposed architecture throughout the work, ensuring its trustworthiness, availability, and consistency with the customer's security policies. The solution offers cloud subscribers the ability to do three things, including customizing and executing a security policy for the cloud environment, verifying that the ongoing migration operations of the computing environment comply with their customized security policy, and finally, auditing the security of present and historical requests throughout the VM's lifecycle through a non-reputation logger in the blockchain.

Six entities are involved in the process: customers, cloud managers, registry, attribute authorities, blockchain auditor, and server cluster. There are three stages of the deployment: Stage 1 (Initial Stage), Stage 2 (Attribute Authorization), and Stage 3 (VM Deployment).

Finally, we look at the study to implement machine learning for cloud security. In the research undertaken by [16], they review the ability to secure cloud environments by implementing machine learning—the study focuses on the machine learning techniques used to solve, detect, or prevent issues and vulnerabilities. The first finding is the vulnerabilities typically found, which are not limited to phishing attacks, zombie attacks, denial-of-service, and man-in-the-middle attacks. Thirty machine learning techniques were used either as hybrid or standalone across all papers reviewed. The study concluded that there had been very few surveys on machine learning techniques in a cloud security form.

3. Security in Fog Computing

The fast-growth and numerous big data and IoT applications have generated massive amounts of data required to process and analyze far beyond the traditional computing model. The rationale of fog computing (FC) technology is to tackle the issues of IoT applications in traditional cloud computing models such as ultra-high latency, high bandwidth, and geographic dispersion [17]. FC can be defined, according to the OpenFog Consortium, as a system-level horizontal architecture that distributes computing services, storage, networking functions, and controls to the proximity of data devices [18]. FC acts as an intermediary between the cloud and end-devices, bringing connected devices closer to the networking, storage, and processing services. It is an approach to provide computational and storage services closer to working in real time and closer to the connected devices in the network. FC can be treated as an extension of cloud computing to adapt to IoT data. It supports the computation offloading process and relevant services close to the users, enhancing the computational speed and reducing the burden of traditional cloud computing data centers. This novel computing model provides intelligent services to meet data optimization, privacy, security, and real-time processing requirements, by collaborating with cloud computing and mobile edge network infrastructure.

In the FC system, resources located at both core and edge can be employed for computing. It works based on the concept of decentralized computing to boost computational speed. In most FC models, the computational power is focused on the LAN resources further away from the network's core and closer to the data sources, consequently mitigating the latency related to the data transfer to the core, as observed in edge computing [19]. Therefore, FG supports the network load as the advancement of multitier offloading services matters to the network's core. App developers and content providers can utilize the FC systems providing users with services closer to them. Its applications have a significant position in various areas such as transportation, healthcare, energy grid, smart cities, video analytics, and climate change monitoring.

FC is employed to handle the high-latency challenge in the apps and services not adequately managed within the cloud computing system. FC platforms support different entities to synthesize their storage, network, and other core functions, which extremely offload the network core computing and communicating burden. At the same time, processing data near the data source delivers a better service quality and structural reinforcement for user data privacy and security. Although many aspects are similar to cloud computing, FC still possesses several differentiating features: mobility support, dense geographical distribution, heterogeneity, proximity, numerous node support, and low latency. These promising features support FC to have scalability, a wide geographic distribution, greater business agility, the predominant position of wireless access, and robust capability for time-sensitive data analysis and streaming applications [20].

Security Challenges in Fog Computing

Due to the above unique benefits and characteristics, the traditional data privacy and security approaches in cloud computing are no longer appropriate to protect huge data in FC. Rezapour et al. [21] identified security matters as the crucial concerns in the fog environment within a comprehensive survey on the benefits and challenges of FC. By analyzing recent implements of fog computing and accessing their quality of security

services, FC was found to be weak against security. The findings of this study point out some promising solutions and trends, including the desire for security protocols and new methods to detect and mitigate security risks in fog networks

Tamrakar et al. [22] described security challenges in FC and proposed solutions with blockchain technology. Some security problems related to FC that need to be managed are authorization systems for the entire FC's node, authentication, data integrity, access control, DOS attacks, and attack detection, because it impacts the fog layer's working efficiency. The blockchain technique, a decentralized computation and information-providing medium, is applied to solve each security challenge. For example, the smart contract can strengthen authentication by creating a five-main-element scheme, including admins, fog nodes, smart contracts, cloud server providers, and end-users. In this case, a decentralized technique to manage access controls and authentication is followed. All the lodged fog nodes to connected devices are mapped by smart contracts, and users have to connect the respective fog node for authentication and obtain access.

Zhang et al. [23] highlighted the significant security challenges in fog computing, including protecting computational data, access control, authentication, data storage, and privacy assurance problems. Services can be disrupted by any devices manipulated by an adversary as they are injected with false information or intrude with malicious actions. For example, even a tiny portion of compromised devices could potentially harm the entire ecosystem as these devices played as involved parties in the distributed fog environment at various layers. In order to address these issues raised in [24], privacy and security should be managed in the design process of FC.

4. Intrusion Detection and Prevention Systems

4.1. Review of Intrusion Detection and Prevention

Aldwairi et al. [25] explore how the expansion of the internet has developed into a world of interconnectivity. This expansion has led to malicious attacks against networked systems being more commonplace. These attacks typically begin with an offensive actor using sensors to scan the network, searching for a vulnerable host, then escalating to further breaches on the target network. As the attack progresses, more sophisticated techniques are usually applied. Butun et al. [26] describe advanced techniques for attackers utilizing distributed attack bases and obfuscating their network identifications. Therefore, countermeasures, IDS included, require increasingly sophisticated approaches. For example, Handa et al. [27] consider a machine-learning approach to develop an intrusion detection and prevention system used for wireless sensor networks on the Internet of Things (IoT). While many machine-learning solutions are computationally expensive, they propose an anomalous intrusion detective protocol (AIDP) utilizing a small attack and fault detection system. The protocol works in three stages: learning, trading, and refreshing. The experience values change depending on the cautions (TAFDS) in the learning stage. Every hub sends its experience estimates to its neighbors in the trading stage. Finally, in the refreshing stage, the standing is refreshed depending on the expertise estimates and trust is refreshed according to the new standing. Further work has been produced by H. Gupta and S. Sharma [28], where they investigated the security challenges in adopting IoT for smart networks. These authors highlight different attack methods using a layered approach: the first layer is the 'Perception Layer', which includes physical damage, jamming, and malicious code injection. The 'Network Layer' includes traffic analysis, flooding, spoofing, and router attacks. The 'Application Layer' includes malware attacks, code injection, and social engineering, and finally, the 'Multi-Layer Attacks' include cryptanalytic attacks, spyware, and distributed denial-of-service (DDoS) attacks. In further work [29], Khraisat et al. present a software-defined intrusion detection system assisted via networking. The intrusion detection system they ran was Snort, and multiple concurrent Snort processes ran on the same infrastructure. It works by forwarding the malicious data into the SDN controller, which moves data to specific points of an SDN in order to inspect it. This SDN device

runs through a docker container on the GNS3 virtual machine, handling the connection of different hosts within the SDN.

Huang et al. [15] investigate the current state of the art and future challenges with the protocols used for intrusion detection and prevention systems in networks using wireless sensors and their integration into the Internet of Things deployment. Their research examines the many security requirements of wireless sensor networks and IoT, focusing on key security properties, including authentication, integrity, confidentiality, non-repudiation, authorization, freshness, availability, forward secrecy, and backwards secrecy. Moreover, they consider common security attacks in wireless sensor networks and IoT-based communication. They use a layered approach for defining attacks and the study investigates the requirements of deploying an intrusion detection system to mitigate threats in this environment, including successful, careful, and strategic deployment. The overall system should be reliable, producing fewer false negatives and false positives. Hence, the system should not cause harm and expose other vectors of attack. It should also have an economical deployment, not using more network and system resources.

Cîrnu et al. [13] examine the current intrusion detection and prevention processes in service-oriented vehicular networks. They start by considering common attacks associated with service-oriented networks: Sybil attacks, DoS attacks, and false alerts generation attacks. They evaluate various intrusion detection agents and propose a monitoring scheme whereby vehicles can activate an intrusion detection agent to monitor their neighbors. To mitigate against common attacks, they propose a rule-based intrusion detection technique that can be used to defend against common attacks such as Sybil and DoS attacks.

4.2. Purposes of Intrusion Detection and Prevention Systems

A common feature of IDPS technologies is that they are not able to be in a place to provide completely perfect recognition. False positives can take place when an IDPS misidentifies friendly traffic as being harmful. On the other hand, when malicious activity is mistaken for friendly traffic, this is known as a false negative. It is not possible to eliminate all false positives and negatives. Therefore, the best outcome to hope for is to reduce them as much as is reasonably possible. In order to develop effective and efficient intrusion detection and prevention, there is a requirement that the base level also consists of a middle level with the establishment of real-time automated functions.

4.3. Intrusion Detection System Functionalities

Intrusion detection and prevention systems are widely used to monitor and investigate events related to cyberattacks. While their specific techniques may be different, intrusion detection and prevention systems (IDPS) there are some common functionalities:

1. Ensuring records of information are correlated to actual events. Information can be stored and made available also to disconnected systems;
2. It is essential that security administrators be notified of important events. The system can send notifications (alerts) by using different channels: messages on the system console, emails, text messages (SMS), trigger user-defined scripts, etc. The content of the message has mainly the purpose of notification. Full details are stored on the IDS;
3. Report generation. Such outputs summarize detected events or provide relevant details about them;
4. An IDS should be able to trigger defensive measures when a new threat is detected. For example, banning specific IP addresses or IP ranges associated with the origin of the anomalous activities. It may also protect the access to specific resources that need to be protected or are in danger by reconfiguring network devices such as routers and firewalls to prevent access to those resources;
5. An IDS may alter the traffic to block malicious content (for example, mail attachments containing malware) and forward the part deemed safe;

6. IDS technologies are not 100% accurate. Therefore, harmless activities may be classified as malicious (a false positive) or vice versa (a false negative). While detection rates can improve, errors cannot be totally eradicated.

4.4. Host-Based vs. Network-Based Intrusion Detection and Prevention Systems

There are two main types of intrusion detection and prevention systems (IDPS): host-based (HIDS) and network-based (NIDS). It is also possible to build hybrid solutions combining the strengths of both technologies to create a more efficient and effective solution.

The HIDS system operates by using functions to protect an endpoint. The technology can monitor the network traffic that moves towards the inside and sends off the device, progressions in succession on the system, and adjustments to files.

The NIDS technology operates by monitoring the traffic on the network. It consists of a packet sniffer to collate the packets from the network or sniff wireless traffic. This traffic is then assessed for any sign of malicious activity, which can signify the common types of attacks (namely, scanning and DDoS attacks).

4.5. Signature-Based Intrusion Detection Systems (SIDS)

According to the academic study in [30], signature intrusion detection systems (SIDS) work by giving high true-positive rates for label patterns. The detected patterns are also known as the signatures—they are stored in the database and compare current user activity with a stored pattern to identify authorized or unauthorized users. This system is lightweight and easy to implement [12].

Figure 1 represents the model of the SIDS approach. The primary concept is to aggregate intrusion signatures' records, compare the current actions with existing signatures, and generate an alarm if they are matching. In the work in [7], we can see that SIDS habitually achieves excellent performance in precision rate for predicting known intrusions. The SIDS approach is employed in many common tools to categorize attacks involving a considerable number of network packets. The IDS is required to analyze the content of previous packets; thus, it is essential to extract the information of signature over various packets as the current malware is extra challenging to detect. Nevertheless, SIDS is less effective in detecting zero-day attacks because no matching labeled signature can be found in the database to predict the new signature that will be generated and stored in the system. The growing sophistication of zero-day attacks has caused the SIDS process to become less successful as there are no previous signature records for such attacks. Moreover, polymorphic variations of malware can degrade the detection rate to a level which can be unsatisfactory. Therefore, alternatives must be considered, such as the anomaly-based IDS presented in the next session.

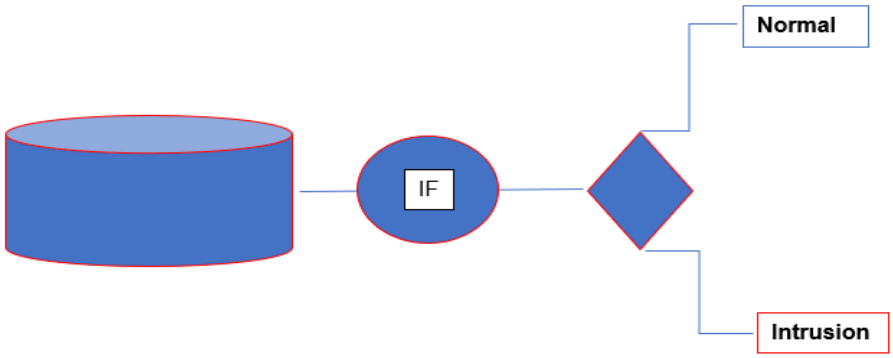

Figure 1. SIDS Model.

4.6. An Anomaly-Based Intrusion Detection System (AIDS)

Recent research [31] has considered an anomaly-based intrusion detection system (AIDS), which is an approach to detect intentional attacks into network systems. This technique is used in intrusion detection problems—it can recognize unknown and known

attacks, making detection more efficient, and representing an improvement over the limitations of signature-based intrusion detection systems (SIDS). The idea behind AIDS is that it is used to protect the network by finding anomalous behaviors, i.e., actions related to deviations from standard user behavior are classified as intrusions. Based on the training method, this system can be separated into three groups: statistical, knowledge, and machine learning models. The most important improvement of AIDS is the capability to recognize the zero-day attacks as their peculiar network behavior distinguishes them from the signature database. An AIDS activates a warning signal when the scanned traffic diverges significantly from the common behavior. An additional benefit is that they can detect internal malicious actions, and if an intruder attempts to penetrate the system, an alarm is raised, and it informs the system manager to take action.

4.7. Statistics-Based Techniques

Statistics-based intrusion detection (SBID), presented in [32], is a method that applies pattern-matching techniques to identify known attacks. It considers the standard patterns in network traffic and flags them when they deviate from the standard statistical parameters (e.g., average, norm, mode, and standard deviation). Statistics-based intrusion detection systems calculate a statistical distribution for the normal behavior profile and identifies low-probability events as potential threats. SBIDSs can operate according to different methodologies: univariate and multivariate. A normal statistical profile is considered for each variable in the univariate, and each metric is considered individually for anomaly detection. The multivariate can consider multiple variables and their correlation and generally achieve a better detection rate.

4.8. Knowledge-Based Techniques

Knowledge-based techniques [30] for intrusion detection are expert systems whose knowledge base models reasonable traffic profiles. This takes into consideration not only data, but also a set of rules that can characterize the expected shape of normal traffic. As a rule, the need to encode manually requires expertise and can be time-consuming. One major drawback is that these rules should be adapted if the traffic shapes change because of technology and internet services evolution. If the set of rules is well-calibrated, the false positives can be maintained at a low level.

4.9. Machine-Learning-Based Techniques

Machine learning (ML) algorithms have been successfully applied to AIDS to improve their effectiveness and efficiency [33]. The ability to process large datasets makes machine learning a suitable technique for analyzing network traffic. Several algorithms have been successfully applied for intrusion detection, including decision trees, neural networks [34,35], nearest neighbors [35], and genetic ones [36]. Although deep learning has made considerable progress in the application of IDS, there is a potential problem of slow detection due to a large amount of traffic and the increased dimensionality of the data. Injadat et al. [37] studied the impact of training sample size, feature selection techniques, and hyper-parameter optimization techniques on detection performance.

ML solutions can generally be classified into supervised learning or unsupervised learning. Supervised algorithms operate with labeled, classified data and can identify the relationship between different variables within the data. Supervised learning typically involves a training phase and a testing phase.

Supervised learning-based intrusion detection system methods detect intrusions utilizing labeled training data. In supervised learning, data are organized in pairs, mapping a host data source or a network and a connected output's value (i.e., label) that should be in normal modes, intrusion, or precise. Functional features are fitted to the model in the training stage, which discovers the data relationship. Then, the supervised learning algorithms utilize the selected features in training data and find the inherent relationships between the input data and the labeled outcome. These learning algorithms are referred to

as classifiers, and they perform the classification task in the detection system. With supervised learning, the labeled outcomes are prearranged and utilized to teach the algorithm how to achieve the necessary outcomes for unobserved data types. In contrast, labels are not specified in unsupervised learning models. Unsupervised learning outlines machine learning techniques that aim to obtain attractive information from input data lacking output labels. The positions of the input data points are processed as an accidental feature set, and a combined density model is then fitted to the dataset. In unsupervised learning models, the data are clustered into a range of output types through procedural learning. In IDS, the unsupervised learning method employs machinery to detect intrusions by applying unlabeled data to train the model. See Figure 2 for cluster classification: intrusion and normal clusters.

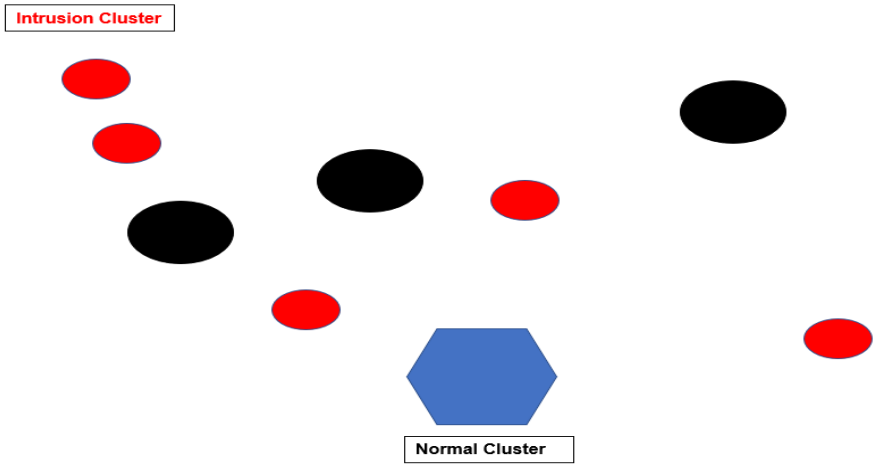

Figure 2. Cluster classification: intrusion and normal clusters.

4.10. Clustering Techniques for the Intrusion Detection System

Recent academic literature [24,38] has explored multiple clustering of intrusion detection systems. There are many different techniques we can use in this domain. The hierarchical clustering (HC) algorithm is one of the most popular approaches. A clustering algorithm in IDS intends to generate a cluster hierarchy. Hierarchical clustering can be classified into two categories: divisive and agglomerative approaches. First, the divisive approach is a top-down HC algorithm. The cluster with the significant amount of relative feature breathing space distance is selected and assorted using binary subclustering techniques. In other words, it starts in one cluster for all observations, and the divisions are recursively performed while moving down the hierarchical structure. Next, the agglomerative approach is a bottom-up HC algorithm where clusters are further broken down into sub-clusters, which are then broken down again into sub-clusters, and pairs of clusters are joined at one level above in the hierarchical structure. In fact, several bodies of work have been conducted applying unsupervised learning algorithms in the vicinity of the cyber-physical control system with malicious attack detection and mitigation. For example, a redundancy-based flexibility methodology was projected in [24], where a dyed-in-the-wool network sub-layer that can grip the circumstance was anticipated through data mining methods. This sub-layer regularly carries information from the nodes of a driver controlled in the network by itself and identifies differences in observations.

5. Intrusion Detection in Fog, Edge, and Cloud Computing

5.1. Fog Computing

By definition, fog computing is the decentralization of IT infrastructure—this can include the processing, storage, and intelligence control to the proximity of the data devices. When utilizing this technology, there is an opportunity to reduce the distances throughout the network environment and improve efficiency as well as the data volume required

to transport to the cloud for processing, analysis, and storage. Thanks to the flexibility presented in fog computing, this can extend cloud computing services to the edge of the network. See Figure 3.

Figure 3 presents three different levels: (1) The Cloud Layer sends the data to the Fog servers, (2) The Fog Layer only stores the recently used data, and in the (3) Edge Layer the user receives the data through the nearest Fog device which are connected through the internet. In the architecture of the topology there is a greater distance between the Cloud Layer (Level 1) and the Fog Layer (Level 2) than the Edge Layer (level 3) and the Fog Layer (Level 2).

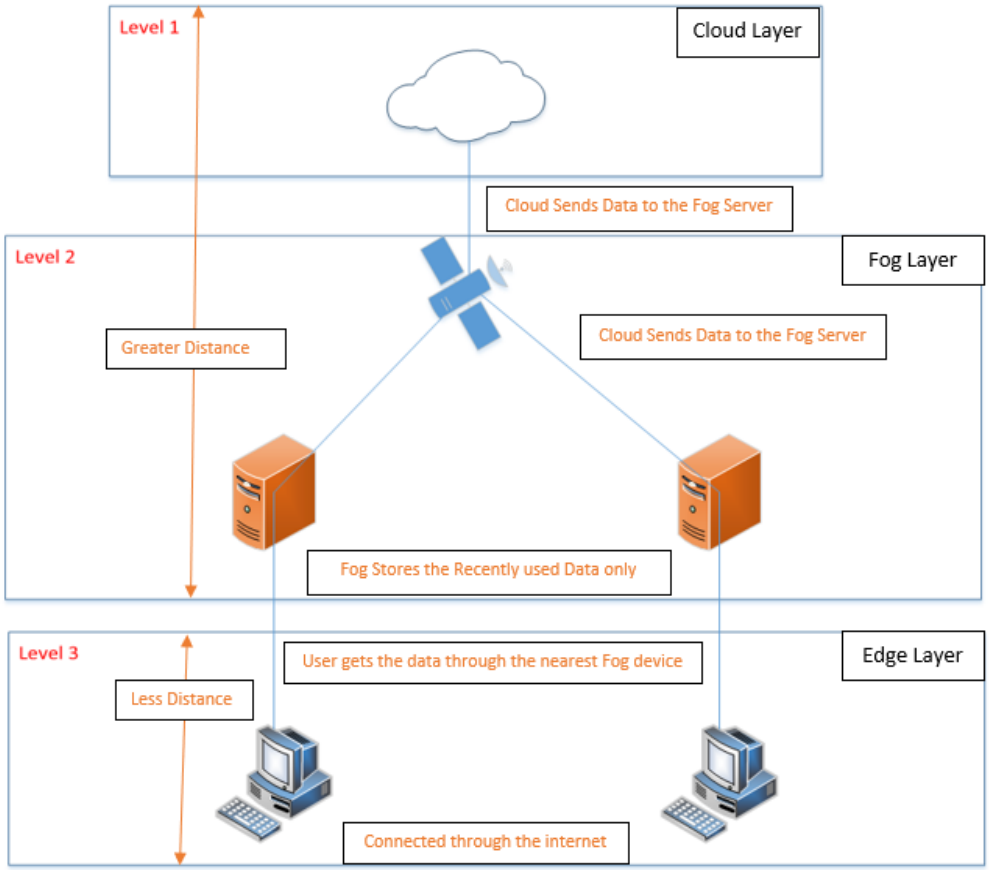

Figure 3. Fog Computing Architecture.

5.1.1. Fog Computing Applications

Many strategies of fog computing devices are focused on analyzing the device status and other time-critical data, such as false alerts, alarm status, and others. It can minimize latency and improve efficiency, whilst preventing major damage from taking place. Successes of the fog computing technology can be noticed primarily in critical Internet of Things (IoT) applications that are particularly time-sensitive or have a requirement for real-time responses, which can be the following: data acquisition and pre-processing, short-term data storage needs, condition monitoring, and rule-based decision making.

5.1.2. Advantages of Fog Computing

Deploying Fog Computing as a measure for strategic system innovation can be seen to have an array of advantages for a business. Some of the most significant advantages can be observed as:

- Data storage in fog computing will be able to minimize any delays in the transmission of data;

- Allowing to efficiently process and analyze the data for many applications (Industrial IoT Smart Cities);
- Providing interactions that are essential between the end-devices and cloud computing servers;
- Deploying a distributed network on a global scale that aids in reducing network downtime;
- Supporting service in real time and providing a reduced state of network latency.

5.2. Open-Successes for Fog Computing in the IoT Environment

Throughout the research of F. A. Kraemer, et al. [39] many succession points for fog computing as technology are described and highlighted. Some of the most noteworthy ones are presented below.

5.2.1. Latency Constraints

Fog computing meets the standard of latency constraints from IoT applications by performing all-time sensitive actions near the end-users.

5.2.2. Network Bandwidth Constraints

Fog computing technology has the ability to provide a reduction to the amount of data needed to be deployed to the cloud by enabling data processing around the following: 'Application demands', 'Available networking', and 'Computing resources'—this contributes to saving network bandwidth.

5.2.3. Uninterrupted Services

The ability of fog computing to run independently can ensure the interruption of services even under conditions of fluctuating network connectivity to the cloud.

5.2.4. IoT Security Challenges

The technology behaves as a proxy for devices that are particularly resource-constrained, making it possible to update the software or security credentials on devices. In addition, it is possible to perform monitoring of the nearby devices and their security status.

5.3. Applications of Fog Computing in IoT

IoT applications—one which store data in terabytes (TB) or higher, that have fast or a significant quantity of essential data processing requirements, and that must send data to the cloud back and forth—become successful candidates for the deployment and implementation of fog computing. With a vast number of IoT applications, there is a large opportunity for fog computing to play a critical role.

5.3.1. Smart Home

The innovation of Smart Homes utilizes an array of devices with censored connections. However, they use an array of devices which all have different platforms, making integration complex. The technology can provide an interface that is unified, integrating many devices (that are independent) and benefiting applications for the Smart Home with resources (that are flexible), enabling storage, real-time processing, and low latency. In the work of Stojkoska and Trivodaliev [40], the authors present a framework for hierarchical IoT. The three tiers of the framework are 'Smart Home', 'Nanogrid', 'Microgrid'. The work aims to prove that fog computing is a suitable solution for reducing traffic on the network. The research addresses the use in the Smart Home environment—the framework proposes to expand the Smart Home to a microgrid level by integrating many renewable energy sources from the microgrid and achieving a greater energy optimization. In the research, the authors used a simulation of a real dataset and highlighted that Fog Computing based on predictive filters could mitigate the quantity of transmissions and lower Smart Home network energy consumption.

5.3.2. Healthcare Activity Tracking

Fog computing has the ability to provide processing and event responses (in real-time), being imperative for technological use in the healthcare industry—the technology also focuses on issues around the essential network connectivity and traffic needed to use storage remotely for processing and medical record retrieval in the cloud. The following work [41] highlights where fog computing can be noticed in the healthcare domain, where the researchers propose fog computing as the potential gateway for augmenting health monitoring systems. They used services embedded in fog computing, which include interoperability, distributed databases, a real-time notification mechanism, location awareness, and GUI containing access management. In addition, they introduce a flexible, lightweight template for an ECG feature (examples include heart rate, P wave, and T wave) extraction. When researching, they performed demonstrations and obtained results highlighting the success of using the smart gateway.

6. Intrusion Detection Overview

6.1. Providing Strong Intrusion Detection in Fog Computing

Fog computing (also known as fog networking and fogging) is a specific type of architecture that makes use of edge devices (a device providing an entry point into enterprise or service provider core networks) to hold a significant volume of computer storage and digital communication locally, as well as being routed over the internet.

In the recent work of [42], a game model was developed to provide intrusion detection technology into the cloud–fog-based IoT networks, using game theory. Game theory is used as a way of modeling to design a situation based on the predefined rules of the game to understand what will happen in a specific situation. The main elements of the game theory include players, actions, profits, and information, which are considered as the rules of the game. The model has been designed to detect attacks attempting to intrude into the network. Applied mathematical formulation and algorithms are used to demonstrate how the technology works in the environment. The model produces an evaluation comparing the results against other similar models, see [43] and [36]. When evaluated against the other models, the proposed model in the research was compared in five different areas: (1) Coverage of security threats—where it is seen to be a non-cooperative game; (2) Emphasized detection methods—combined; (3) Type of game model—focuses on common attacks in IoT networks and wireless sensors; (4) Complexity of protocol and architecture—which is low; and, finally, (5) Scalability—where the model is seen to be scalable in comparison.

Additionally, in the work in [44], where the authors present a novel IDS system that can be used in a fog computing environment—the system consists of three steps: (1) Data preprocess; (2) Data normalization; and (3) Decision Tree detection method. The paper presents three contributions to the field of cybersecurity through the implementation of IDS, including proving that the IDS system is suitable for a big data environment, completing detection for four different attacks addressing the denial of service (disturbing or denying services to clients), probing (monitoring and other detection activities), R2L (Accessing systems or resources illegally for remote systems), and U2R (performing unauthorized access of normal users, as well as privileges of administrators). The study implements further the detection for twenty-two different attacks, providing a calculation time to compare each method which aids in the accuracy of detection, which is acceptable and can be used in the big data environment, as well as providing sections on experimental evaluation, related work, and research conclusion.

Moreover, in recent work [45], the authors have addressed IDS in fog computing and IoT-based logistics systems using a smart data approach. The main aim of the paper is to expand on previous research conducted by the authors—moving into a three-layered structure of IoT systems which include cloud, fog, and edge layers. Using smart data can be a significant step forward for a framework to enable lightweight, effective, and efficient intrusion detection—this is due to the framework providing a path for the detection of silent attacks (these can typically include botnet attacks). The authors provide a diagram of

the structure for the smart data and a prototype of the proposed IDS architecture, as seen in [27]. Throughout the research, there has also been a new approach presented for the clustering of primary network connections, which proves to be a more effective method than previous attempts. The authors explore future work and innovation opportunities in this area by focusing more in depth on detecting botnet attacks using smart data technology.

6.2. Providing Strong Intrusion Detection in Edge Computing

Edge computing is a distributed computing model that delivers computational tasks and data storage closer to data sources. The reason for this innovation in computer science is to improve response times and save bandwidth, making this method of computing highly efficient.

In recent academic literature [46], intrusion detection technologies have been observed in edge computing, where the authors propose an intelligent anomaly-based intrusion detection technology for edge computing, known as Passband. The technology aims to be both hosted and executed on a typically used edge device (including an IoT gateway). The authors created a testing environment that consisted of two different scenarios to understand how the technology would behave differently and perform experiments using an IoT environment that simulates a Smart Home automation environment (typically used). After the experiments were performed in the first scenario, Passband was validated to protect all the IoT devices connected to it. In the second scenario, Passband was observed to have the ability to monitor both the incoming and outgoing traffic of all the IoT devices connected to the network. The aim is to investigate potential malicious patterns noticed in the network traffic, as Passband has been executed on the IoT gateway (A Raspberry Pi 3 Model B). Passband has also been tested against four common cyber-attacks, including Port Scanning, HTTP Brute Force, SSH Brute Force, and SYN Flood attack, which highlighted to be that the IDS can achieve scores of higher than 0.9 on some of the attacks, 0.99 in the best case and 0.79 in the worst case.

Moreover, in the work of [47], an intrusion detection solution has been discussed, proposing a GAN-based intrusion detection system to provide mitigations in the CEC-based slot. This solution works by extracting network data features and using the proposed intrusion detection method to see various incoming attacks on the system and the network. The authors propose three key phases: feature extraction, an IDS model that focuses on a single attack, and an IDS model that focuses on multiple attacks using various discriminators. The proposed method begins enhancing security by preprocessing the flow and feature extraction. They then design an IDS algorithm focusing on a single attack by GAN—with the combination of multiple IDS models focusing on one attack. They also design an IDS algorithm to counter many attacks based on GAN. The researchers have evaluated their project by implementing it over two particular data sets (CSE-CIC-IDS-2018 and CIC-DDoS-2019). When addressing the results from the simulation, the overall method demonstrates the improvement and accuracy of IDS. The main contributions of the work to the field of IDS are the novel IDS method deployed in GAN, the design of an algorithm to provide high accuracy that can be used to capture different variations of attacks, and the ability to detect new attacks by training and learning of attack types. The researchers look at future research directions into the method—improving the accuracy more in the combination of neural networks and the GAN method to extract more features (spatiotemporal) of network data.

The research in [48] conveyed a proposal for an IDS model for edge computing deployment and highlighted the demand for resource allocation. The paper aims to understand the method of achieving fair resource allocation in the IDS technology by covering three crucial topics, such as a virtual security network model for the edge that is made with consideration of the specific network characteristics of edge computing. The proposed model provides a division of edge networks into six layers—(1) User equipment layer; (2) Network layer; (3) Data-processing layer; (4) Detection layer; (5) Analysis layer; and (6) Management layer. Each has its own individual unique functions. The second

topic is a proposition of an SDMMF allocation that adapts the characteristics of resource-constrained nodes at the edges. Finally, a scheme that allows for multi-layer resource allocation is known as MDMMF, where a resource demand is given for each edge node. The paper discusses how the architecture of the model can defend against four prominent cyber-attacks, including probing attack, distributed denial of service, R2L attack and U2R attack, and provides a diagram of how the resource is allocated in the IDS using the model.

6.3. Providing Strong Intrusion Detection in Cloud Computing

Due to the increasing volume and complexity of cyber-attacks happening in the cloud computing domain, there is a need for enhanced security measures to counter unwanted malicious activity from criminals intending to cause harm. Therefore, a proposed method is the adaptation of an already successful cybersecurity technology with a demonstrated history to be implemented into cloud computing architecture.

Throughout literature [49], intrusion detection technology can be observed in the cloud computing environment. The authors integrate a network IDS into a cloud-based environment (open-source) in the paper. The solution works by designing and developing the IDS to be compatible in a cloud system that provides services according to the Platform-as-a-Service (PaaS) model and it is structured as an added service option of the clouds infrastructure. The research demonstrates the practical implementation of the different strategies of implementation. Many advantages of this solution have been highlighted throughout the research, including the ability to monitor all traffic flowing to and away from the cloud infrastructure when placing the IDS close to the cluster controller. By placing the IDS close to the physical machines, each one can focus on a smaller area of network traffic, meaning that there is a smaller likelihood of the solution being overloaded. However, it has also been highlighted in the research that the IDS has been overloaded in a given scenario, and this has left the network open to coordinated attacks that can ruin the IDS technological functionality by using specifically designed traffic before commencing the real cyber-attack.

In addition, IDS can be noticed in the work in [50], where the authors address the current challenges and opportunities present in using IDS technology in a cloud-based environment which can be used to create successful security deployment measures. The paper highlights multiple intrusions that can affect the confidentiality, integrity, and availability of the cloud system. The authors then explore various IDS technologies deployed in a cloud environment, including network-based IDS, host-based IDS, VMM/Hypervisor-based IDS, distributed IDS. The researchers then discuss the detection techniques used, such as signature-based IDS, anomaly-based IDS, and finally, hybrid detection. They also discuss the key limitations of using IDS technology, highlighted in the lack of features, scalability, and autonomic self-adaption. IDS technology is also not deterministic, which ultimately makes them unsuitable for cloud-based environments, demonstrating a significant challenge in attempting to use the technology as a valid cybersecurity measure in the environment.

6.4. Intrusion Detection in SDN for Fog and Cloud Computing

Software-defined networking manages networks that aim to provide dynamic, programmability, and efficient network configuration to enhance network performance and monitoring. In other work [51], the authors explore how the use of SDN technology can be utilized to improve intrusion detection technology through the concept of detection as a service (DaaS) in the SDN environment. The research focuses on how the combination of the programmability features in SDN can be combined with intrusion detection systems to make a redundant, reliable, and scalable anomaly detection system that can be used for mobile network operators. The paper focuses on multiple approaches for the implementation of the DaaS technology. The first approach considers where the traffic originates from a subscriber and aims towards the internet—it uses DaaS units to analyze the traffic and differentiate between anomalies and maliciousness in traffic. The second approach

mentioned uses a clustering algorithm combined with the SDN application and controller to forward incoming to the respective DaaS node—the cluster information is sent to the SDN application to formulate forwarding rules (also known as flows) for different DaaS nodes and for load balancing. The platform consists of an application layer, a management layer, and a data layer. The architecture is evaluated throughout the research in that it protects SDN environments from being destroyed in cyber-attacks, focusing on resource overload and destructive attacks.

6.5. Intrusion Detection and Prevention System Functionality

As previously seen, there are two different main types of intrusion detection technology, including anomaly-based and signature-based. There are also other techniques such as statistic-based, knowledge-based, and machine-learning techniques. Hybrid systems have been observed to be the most effective. Moreover, in an application, the technology should provide a suitable notice to the security personnel (for example, a Security Analyst) to make them aware of the intrusive situation—typically by sending an alert on the interface of the machine. Next, reports should be generated which provide a summary of the events that have been highlighted during the detection process. Furthermore, many of these technologies can adapt their security characteristics when a new threat is posed. Using intrusion detection technology—they have the ability to simulate an attack automatically. They can also block access to the host, services, and other relevant network resources. Lastly, they can perform changes to the security background, disturbing an incoming cyber-attack. This can include a reconfiguration for network devices such as routers, switches, and firewalls which can defend against a cyber-attack.

7. Opportunities for Organizational Adoption of the Research

We recommend the following direction for the organizational adoption of intrusion detection technology into businesses. Firstly, there is a need to recognize and understand the specific type of technological choice, including anomaly-based, signature-based, knowledge-based, statistics-based, or machine learning. Additionally, there must be understanding around the current infrastructure and systems currently operating within the company (considering the possibility of change in the near future), including the opportunity to change closely in the future), including enhancing or deploying cloud or fog computing environments and providing a future proof cybersecurity and operational security measure. Finally, we recommend that the businesses decide on the IDS vendor they want to choose based on the current state-of-the-art research and developments.

7.1. Methods of Defending Organizational Systems—Business Recommendations

We have discussed many approaches for providing efficient and effective intrusion detection and prevention throughout the paper. In this section, we will be discussing which implementations of IDPS technology should be used in real-world business scenarios. We recommend businesses to follow a strategic organizational adoption based on relevant research studies, similar to those presented in the previous sections and the lessons learned from case studies presented in Section 8. Moreover, the technical recommendation may consider solutions highlighted in the rest of this section.

7.1.1. NIDS or HIDS for a Business Strategy

A network-based intrusion detection system gives the organization significantly more monitoring capability than the host-based intrusion detection system, as seen in Section 3—this will aid in the business noticing cyber-attacks (in real-time), providing a higher level of cyber threat intelligence. Moreover, the HIDS technology can only understand a cyber threat once a setting or file has already been altered, meaning that it can only mitigate the problem once the problem has happened, causing a HIDS to be a problematic solution in comparison. The recommendation for businesses is to deploy a NIDS as the priority

and, if possible, use both technologies as a hybrid solution but avoid using a HIDS as a standalone IDS.

7.1.2. Signature-Based or Anomaly-Based IDS for a Business Strategy

Signature-based technology is highlighted to have a greater speed than anomaly-based technology, which is the most noticeable difference in capability comparison. However, despite this, a complete IDS system must offer both signature and anomaly-based operations. This is because there are advantages and constraints to using either technology as a security measure for the enterprise cybersecurity strategy, and these are highly compensated with the combination of the technologies. Therefore, we recommend that businesses deploy a hybrid solution utilizing both technologies to get the most out of their IDS system and are not constrained by the weaknesses in either technology [52].

Three key criteria used for deciding on the most effective software to deploy in a real-world business setting have been assessed using three main criteria, which include: (1) identifying false positives, (2) staffing needs, and (3) the identification of genuine risks.

8. Case Studies

8.1. Adopting Content for Teaching and Learning in Higher Education

8.1.1. Teesside University

Teesside University is a higher education institution in the North-East of England. According to the British education system, Teesside University provides many programs in computer science and sub-domains ranging from Level 4 to Level 8.

The undergraduate course entitled "Cybersecurity and Networks" aims at training professionals in protecting systems and networks from digital attacks. The degree provides a hands-on approach and places a strong emphasis on cybersecurity, including ethical hacking and network infrastructures, particularly, ways to create and manage secure systems and networks. Students explore a range of different cybersecurity and networking techniques applied to different networks, hardware, and software platforms during their course.

Examples of these techniques include:

- How to effectively perform an effective, ethical hacking and security analysis;
- How to design and implement different network architectures used in industry, e.g., virtualized, mobile, and cloud-based systems;
- How to deliver excellent server administration and enterprise server management;
- How to secure computers and networks and implement intrusion detection/prevention systems;
- How to perform risk assessment, data governance, and compliance.

In the context of networks security, students explore different approaches and solutions. In some modules, they experiment with fundamental theories and basic applications. In other words, they apply their knowledge to a near-real-world scenario. In particular, in a module called "CIS CYBER", students work in small teams to plan, design, and build a secure network. Each team is required to design, implement, and document a secure network, including the installation of virtualized servers running a variety of operating systems. The module requires a professional approach to plan a successful development project, informed by current industry practice.

In this context, as part of the network design, the student must identify and deploy solutions for the implementation of infrastructural services, such as routing, firewalling, intrusion detection/prevention, and others. Therefore, they use tools such as pfSense to implement routing services, network address translation, and Snort for intrusion detection and prevention. As part of their project, teams must conduct a security assessment of their system and perform a pen testing activity on another team's system. Thus, they can compare their findings with the one from the team who pen-tested them. This approach helps the student to develop critical thinking and understand real-world scenarios of system attacking and defending in the cyber landscape.

8.1.2. Middlesbrough College

Middlesbrough College is a further and higher education institution in the North-East of England—they provide many courses in computer science, ranging from Level 1 to Level 6, including undergraduate degree programs. When teaching cybersecurity and networks, they teach the fundamentals through a more conceptual approach, allowing the students to create, design, and develop network diagrams focusing on building intrusion detection and prevention systems into a given specification for a given scenario. This has been their method of teaching and learning for a significant amount of time. However, in recent months, they have been expanding their cyber education landscape by creating the new technology building MCdigital.

The college will invest in new technology and infrastructure to provide a higher standard of computer science education. This technology includes new hardware—investing in Cisco equipment, including their ASA technology in physical devices to allow the students to build a network and configure using the CLI physically. The higher education institution has also invested in using new computers and servers with a specification to allow software-defined networking. The college will make use of the industry-standard tool GNS3 to be installed on all student computers with the appropriate images paid for and installed, giving the students access to software-defined networking (SDN) using Cisco technology, Cumulus technology, Juniper technology, and, finally, pfSense. SDN software will be installed into GNS3 through a hypervisor to allow the students to undertake projects and assignments focused on intrusion detection and prevention systems. Students can install Snort, which means that they can get the critical education and understanding to prepare them for a cybersecurity role in the future, namely, a security analyst.

8.1.3. Xiang'an Campus of Xiamen University

Located in Xiamen, this campus was built in the 1950s and had over 20 low-rise buildings. It has its own independent financial and personnel systems and a range of student admissions, administration, and logistics services management systems, its own library and modern education center, and is a relatively independent branch campus. Relative to the size of other campus networks, the campus network is small, but there are distinctive features. First, the campus network has a large and dense user base. Students live in centralized accommodation and have regular working and resting hours; therefore, their internet access is relatively concentrated. The high broadband and large user base provide favorable conditions for the rapid spread of network security issues. Secondly, as the campus has many buildings, but fewer floors per building, the campus network of the college adopts a two-layer network topology, i.e., a core layer and access layer, with no convergence layer. However, the access is complex and there is no single outlet. The coexistence of LAN, MAN, and WAN in the campus network makes it necessary for campus managers to face a complex network environment. Thirdly, the campus network is open and more relaxed. To facilitate access to the internet for students without computers, the college has a computer room with direct access to the campus network. This open network environment is also fraught with hidden dangers. Fourthly, user identities are complex and mobile, and pirated software, film, and TV resources, as well as all kinds of shareware, are prevalent in the campus network, providing opportunities for network viruses to invade. Fifth, many of the campus's network hardware devices are exposed to the public space of the campus and are vulnerable to natural disasters and human damage.

In order to combat the above issues, as a part of the security system of the campus network, this campus has deployed a firewall and intrusion detection system (IDS) from Tianrongxin at the central exit of the network. The intrusion detection system captures and monitors the transmission of data on the campus network in real time, deeply inspects all packets entering the campus network, detects whether DMZ servers and data center applications are under attack, audits malicious port scanning and probing behavior, and implements supervision of all activities on the network. As soon as a potential threat is detected, the system sends out an alert to notify the relevant management. It also

prevents some wrong actions, generates log files for analysis, detects intrusions against the network and servers in real time, and makes up for the lack of equipment such as routers, firewalls, and switches. Physical security avoids damage to network equipment from natural disasters and environmental incidents, ensuring that it is protected from dust, lightning, and static electricity, and especially from deliberate human damage. Xiamen is a typhoon-prone and humid city, and the campus's short buildings have a negative impact on the physical protection of network equipment. Therefore, the campus places servers and core switches on the third floor and builds network cabinets according to relevant standards. It also sets up dedicated equipment grounding cables and equips them with uninterruptible power supplies to ensure that equipment has a continuous and stable power supply and is not affected by external power supplies. The batteries are also regularly maintained following the requirements of the operating code. Moreover, air conditioning is installed to maintain a certain temperature and humidity [53].

8.1.4. Poznań University of Technology

The Poznań University of Technology is a technical university located in western Poland established over a hundred years ago. It is a leading Polish technical university, which is the third most popular university among all those operating in Poland. The university is also the leader of the European University for Customized Education (Eunice), in which it participates with other universities from the EU, including Germany, Spain, Italy, France, Finland, and Belgium. The Poznań University of Technology is ranked high in many rankings. It is seventh among Polish universities in the EECA ranking and is among the top 15% of Polish universities in the Best Global Universities Ranking. The university was also included in the prestigious list of the world's best universities—QS World University Ranking. The Computer Science Department at the Faculty of Computing and Telecommunications contributes significantly to the high position of Poznań University of Technology. The department offers bachelor's engineering, master's, and doctoral degree programs. In each degree, a strong emphasis is placed on subjects related to teaching elements of information systems security.

The objectives of the course entitled "Security of Computer Systems", taught during a bachelor's degree program, is to acquaint the students with the understating of basic security problems regarding the use, configuration, and administration of security mechanisms at the system and application level. Moreover, the students' skills in solving problems related to securing the computing system infrastructure are developed. During this course, the students develop the effective use of access control and network communication protection mechanisms, along with application-layer security tools. Those skills are acquired while solving practical exercises in laboratory classes, where students acquire security management skills, including design and implementation of security policies, security analysis tools and monitoring systems, IDP/IPS, honeypots and honeynets, and, finally, incident response procedures.

As part of the master's degree program, students interested in the topic of security in information systems can expand their knowledge by choosing the cybersecurity specialization. Students of this specialization become acquainted with the problems of widely understood information and communication security: design of cryptographic algorithms, protocols, analysis and evaluation of the security of systems, applications, information and communication networks, Internet of Things, analysis of malicious software or security aspects of data processing and storage in order to avoid cyber-attacks, such as ransomware, phishing, internet frauds, risks associated with removable media. In the course of teaching, special emphasis is placed on network security problems, including wireless security, software-defined networking security, application security development, testing and evaluation; Internet of Things IoT security; big data analytics security, and security breaches in clouds and data centers. Courses providing broad practical knowledge are conducted in specialized laboratories equipped with Cisco Systems, Huawei, and Juniper Networks equipment. Graduates will be prepared to conduct penetration tests, analyze malicious

software, manage IT systems, and take courses that prepare them for certification exams of such companies as Cisco and Huawei. The proposed specialization is implemented in cooperation with domestic and foreign partners (Intel, Global Cybersecurity Institute Rochester, Florida International University).

8.2. Adopting Content for Healthcare Service Providers

8.2.1. National Health Service, UK

The National Health Service (NHS) is the taxpayer-funded healthcare provider in the United Kingdom and one of the world's largest publicly funded healthcare systems, carrying out over 500 million appointments per year and providing most of the healthcare delivered in the UK. Given the combination of the UK's large reliance on the NHS as a service and its vast scale, it becomes cumbersome to roll out operating system updates and security patches across the service as a whole. As a result of these factors, it has often been a target of security breaches in recent times, such as patient data leaks and ransomware attacks. Indeed, in the previous two years, over 3000 data breaches were reported, with many more expected to have gone unreported. In 2017, the NHS fell victim to a large-scale attack propagated by the WannaCry ransomware, disrupting administration tools and the care of patients. Estimates of the financial damage caused by this attack are upwards of GBP 19 million, with an additional GBP 73 million in IT costs and 19,000 canceled appointments [54].

As a result of these attacks, the NHS has been forced to improve security and it adopted the Cyber Security Program in the wake of the WannaCry attacks, which act as a series of security measures. These include the completion of independent assessments, which are conducted upon ensuring that companies associated with NHS services register to cyber alert monitoring services and increase investment. Security services invested in include Virtual Perimeter Security (VPS), vulnerability scanning through the Vulnerability Monitoring Service (VMS), and the BlueFort intrusion detection systems, which are also widely used by other large companies with a large technology infrastructure. BlueFort automated intrusion detection systems combine network intrusion detection (NIDS) systems and host system intrusion detection systems (HIDS) in tandem to create a multilayer threat mitigation service. The NIDS monitors inbound packets at the network perimeter, sending alerts when potential breaches are identified based on a set of defined criteria or activity. The HIDS monitors the traffic within the network and host system and, similarly to the HIDS, sends alerts to the networking team.

8.2.2. Polish e-Health Center

Work on medical ICT systems is treated as a priority in Poland. The most developed system is the Internet Patient Account (IPA), whose aim is to facilitate patients' convenient use of digital services and organize medical information about the patient's health in one place. Every person with a personal ID number has a free IPA account.

The Internet Patient Account provides information about past, current, or planned treatment and allows to arrange a number of issues without the need to visit the clinic or hospital. The IPA system also provides information about issued and filled e-prescriptions, the dosage of the medicine prescribed by the doctor, history of visits to the doctor, vaccinations, and many others [55]. In addition, using the IPA system, a patient can consent to certain health services such as invasive surgeries, share e-prescriptions and e-referrals with a medical facility or a medical professional, or check the medical results. These are sensitive data that require special security.

Therefore, the e-Health Center, which is responsible in Poland for monitoring the development of e-Health and responsible for medical ICT systems created at the national and regional level, uses national cloud resources to implement medical systems [56]. The unlimited computing power available in the public cloud allows operating a scalable, flexible, and fully efficient system. Moreover, it provides advanced security mechanisms in the sphere of digital security, operating procedures, as well as physical security in data

processing centers. The applied security mechanisms are based on recognized norms and the highest standards: ISO 27001, ISO 22301, ISO 27017, ISO 27018, and CSA STAR.

For example, the e-Registration system integrated with the IPA system has so far enabled more than 32 million appointments for covid vaccination. In the days of the system's peak popularity, 880,000 visits per day and 122,000 in just one hour were registered with its help, and users conducted 350,000 searches for free appointments per hour and 950 searches per second. The solution has been integrated with many existing public IT systems (including the e-Health System (P1) and the Vaccine Distribution System (SDS)) and it was designed to allow for easy integration with other healthcare systems in the future and, through the security mechanisms used, allows for intrusion detection.

9. Conclusions

This paper presents a conceptual overview and summary of multiple technologies used throughout business and enterprise environments, focusing mainly on fog and cloud computing, and the related intrusion detection and prevention technologies. With the support of cloud computing, applications are also shifting from local to cloud environments, benefiting people's lives and work. In terms of the concept of cloud, this computing model is based on the use, interaction, and expansion of the internet.

Fog computing is a method with strong potential to grow in ways that have impacts on the availability of resources for online businesses. In comparison to public clouds, private clouds are believed to offer a higher degree of security as the security is managed by organizations [57].

A common problem for businesses in putting IDS into practice is that they sometimes lack an adequate incident response strategy. Successful incident response requires experienced security personnel who can quickly understand the threats and implement effective countermeasures without affecting day-to-day operations. There should be rapid communications between personnel processing the alerts and those in charge of implementing remediation measures. Before deploying an intrusion detection system, organizations should complete a comprehensive risk assessment to understand their environment better and identify key resources that require protection. In some instances, businesses have outsourced network monitoring to provide access to IDS logs and alerts externally and may offer prompt and specialized scrutiny on the concern system.

System availability and business continuity are other issues to consider because if the false positive rate is too high, it could trigger countermeasures that are not necessary and limit the availability of systems. This may paradoxically lead to offensive actions where the attacker can exploit known traffic patterns that trigger false positives to flood alerts to the target system administrators. This may then lead to two scenarios: one where the attacker may aim at undermining the availability of the system, the other where a real attack is performed but obfuscated among the flood of alerts. This can represent a challenge that IDS designers may need to consider.

Author Contributions: Conceptualization, V.C., P.M. and Q.A.X.; Formal analysis, V.C., P.M., Q.A.X., L.M.T.D., K.H. and A.K.; Funding acquisition, V.C.; Investigation, V.C., L.G., L.M.T.D. and S.B.; Methodology, V.C. and L.G.; Project administration, V.C.; Resources, V.C.; Supervision, V.C.; Validation, V.C.; Writing – original draft, V.C., L.G., P.M., Q.A.X., L.M.T.D. and S.B.; Writing – review & editing, V.C., L.G., P.M., Q.A.X., L.M.T.D., K.H., S.B. and A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by VC Research grant number VCR 0000162.

Data Availability Statement: Not Applicable, the study does not report any data.

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

References

1. Hussein, N.H.; Khalid, A. A survey of Cloud Computing Security challenges and solutions. *J. Comput. Sci. Inf. Secur.* **2016**, *14*, 52.
2. Ryan, M.D. Cloud computing security: The scientific challenge, and a survey of solutions. *J. Syst. Softw.* **2013**, *86*, 2263–2268. [CrossRef]
3. Kuyoro, S.O.; Ibikunle, F.; Awodele, O. Cloud Computing Security Issues and Challenges. *Int. J. Comput. Netw.* **2011**, *3*, 247–255. Available online: https://eprints.lmu.edu.ng/1390/ (accessed on 18 February 2022).
4. Tripathi, A.; Mishra, A. Cloud computing security considerations. In Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China, 14–16 September 2011; pp. 1–5. [CrossRef]
5. Soa. 2021. Available online: https://www.ibm.com/nl-en/cloud/learn/soa (accessed on 18 February 2022).
6. Chen, Y. *Service-Oriented Computing and System Integration: Software, IoT, Big Data, and AI as Services*, 6th ed.; Kendall Hunt Publishing: Dubuque, IA, USA, 2017.
7. Rumez, M.; Grimm, D.; Kriesten, R.; Sax, E. An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures. *IEEE Access* **2020**, *8*, 221852–221870. [CrossRef]
8. Grant, D.; Yeo, B. Enterprise integration using Service-Oriented Architecture. *Issues Inf. Syst.* **2021**, *22*, 164–177.
9. Yangui, S.; Goscinski, A.; Drira, K.; Tari, Z.; Benslimane, D. Future generation of service-oriented computing systems. *Future Gener. Comput. Syst.* **2021**, *118*, 252–256. [CrossRef]
10. Huang, M.; Liu, A.; Xiong, N.N.; Wang, T.; Vasilakos, A.V. An effective service-oriented networking management architecture for 5G-enabled internet of things. *Comput. Netw.* **2020**, *173*, 107208. [CrossRef]
11. Choo, K.-K.R. The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **2011**, *30*, 719–731. [CrossRef]
12. Sedjelmaci, H.; Senouci, S.M.; Abu-Rgheff, M.A. An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks. *IEEE Internet Things J.* **2014**, *1*, 570–577. [CrossRef]
13. Cîrnu, C.E.; Rotună, C.I.; Vevera, A.V.; Boncea, R. Measures to Mitigate Cybersecurity Risks and Vulnerabilities in Service-Oriented Architecture. *Stud. Inform. Control* **2018**, *27*, 359–368. [CrossRef]
14. Mishra, S.; Sharma, S.K.; Alowaidi, M.A. Analysis of security issues of cloud-based web applications. *J. Ambient Intell. Humaniz. Comput.* **2020**, *12*, 7051–7062. [CrossRef]
15. Huang, C.; Chen, W.; Yuan, L.; Ding, Y.; Jian, S.; Tan, Y.; Chen, H.; Chen, D. Toward security as a service: A trusted cloud service architecture with policy customization. *J. Parallel Distrib. Comput.* **2021**, *149*, 76–88. [CrossRef]
16. Nassif, A.B.; Abu Talib, M.; Nasir, Q.; Albadani, H.; Dakalbab, F.M. Machine Learning for Cloud Security: A Systematic Review. *IEEE Access* **2021**, *9*, 20717–20735. [CrossRef]
17. Singh, J.; Singh, P.; Gill, S.S. Fog Computing: A Taxonomy, Systematic Review, Current Trends and Research Challenges. *J. Parallel Distrib. Comput.* **2021**, *157*, 56–85. [CrossRef]
18. White Paper. Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Available online: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf (accessed on 28 January 2022).
19. Chalapathi, G.S.S.; Chamola, V.; Vaish, A.; Buyya, R. Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions. In *Fog/Edge Computing For Security, Privacy, and Applications*; Chang, W., Wu, J., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 293–325. [CrossRef]
20. Sabireen, H.; Neelanarayanan, V. A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges. *ICT Express* **2021**, *7*, 162–176. [CrossRef]
21. Rezapour, R.; Asghari, P.; Javadi, H.H.S.; Ghanbari, S. Security in fog computing: A systematic review on issues, challenges and solutions. *Comput. Sci. Rev.* **2021**, *41*, 100421. [CrossRef]
22. Tamrakar, M.; Jain, S.; Doriya, R. Security Issues in Fog Computing. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021; pp. 1853–1858. [CrossRef]
23. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; Hu, F. Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access* **2018**, *6*, 18209–18237. [CrossRef]
24. An, X.; Su, J.; Lü, X.; Lin, F. Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system. *EURASIP J. Wirel. Commun. Netw.* **2018**, *2018*, 249. [CrossRef]
25. Aldwairi, M.; Khamayseh, Y.; Al-Masri, M. Application of artificial bee colony for intrusion detection systems. *Secur. Commun. Networks* **2012**, *8*, 2730–2740. [CrossRef]
26. Butun, I.; Morgera, S.D.; Sankar, R. A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Commun. Surv. Tutorials* **2013**, *16*, 266–282. [CrossRef]
27. Handa, A.; Sharma, A.; Shukla, S.K. Machine learning in cybersecurity: A review. *WIREs Data Min. Knowl. Discov.* **2019**, *9*, e1306. [CrossRef]
28. Gupta, H.; Sharma, S. Security Challenges in Adopting Internet of Things for Smart Network. In Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 18–19 June 2021; pp. 761–765. [CrossRef]
29. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]
30. Sarnovsky, M.; Paralic, J. Hierarchical Intrusion Detection Using Machine Learning and Knowledge Model. *Symmetry* **2020**, *12*, 203. [CrossRef]

31. Thorarensen, C. A Performance Analysis of Intrusion Detection with Snort and Security Information Management. 2021. Available online: http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-177602 (accessed on 18 February 2022).
32. Teixeira, D.; Assunção, L.; Pereira, T.; Malta, S.; Pinto, P. OSSEC IDS Extension to Improve Log Analysis and Override False Positive or Negative Detections. *J. Sens. Actuator Netw.* **2019**, *8*, 46. [CrossRef]
33. Saranya, T.; Sridevi, S.; Deisy, C.; Chung, T.D.; Khan, M.A. Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. *Procedia Comput. Sci.* **2020**, *171*, 1251–1260. [CrossRef]
34. Di Mauro, M.; Galatro, G.; Liotta, A. Experimental Review of Neural-Based Approaches for Network Intrusion Management. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 2480–2495. [CrossRef]
35. Belgrana, F.Z.; Benamrane, N.; Hamaida, M.A.; Chaabani, A.M.; Taleb-Ahmed, A. Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing Features. In Proceedings of the 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), Bali, Indonesia, 27–28 January 2021; pp. 23–29. [CrossRef]
36. Carlin, S.; Curran, K. Cloud Computing Security. In *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments*; IGI Global: Hershey, PA, USA, 2013. Available online: https://www.igi-global.com/chapter/cloud-computing-security/www.igi-global.com/chapter/cloud-computing-security/68920 (accessed on 18 February 2022).
37. Injadat, M.N.; Moubayed, A.; Nassif, A.B.; Shami, A. Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 1803–1816. [CrossRef]
38. Wu, C.; Peng, Q.; Lee, J.; Leibnitz, K.; Xia, Y. Effective hierarchical clustering based on structural similarities in nearest neighbor graphs. *Knowledge-Based Syst.* **2021**, *228*, 107295. [CrossRef]
39. Kraemer, F.A.; Braten, A.E.; Tamkittikhun, N.; Palma, D. Fog Computing in Healthcare–A Review and Discussion. *IEEE Access* **2017**, *5*, 9206–9222. [CrossRef]
40. Stojkoska, B.R.; Trivodaliev, K. Enabling internet of things for smart homes through fog computing. In Proceedings of the 2017 25th Telecommunication Forum (TELFOR), Belgrade, Serbia, 21–22 November 2017; pp. 1–4. [CrossRef]
41. Gia, T.N.; Jiang, M.; Rahmani, A.-M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 26–28 October 2015; pp. 356–363. [CrossRef]
42. Pirozmand, P.; Ghafary, M.A.; Siadat, S.; Ren, J. Intrusion Detection into Cloud-Fog-Based IoT Networks Using Game Theory. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, e8819545. [CrossRef]
43. Sönmez, F.Ö.; Günel, B. Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation. In Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018; pp. 38–44. [CrossRef]
44. Peng, K.; Leung, V.C.M.; Zheng, L.; Wang, S.; Huang, C.; Lin, T. Intrusion Detection System Based on Decision Tree over Big Data in Fog Environment. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, e4680867. [CrossRef]
45. Hosseinpour, F.; Amoli, P.V.; Plosila, J.; Hämäläinen, T.; Tenhunen, H. An Intrusion Detection System for Fog Computing and IoT based Logistic Systems using a Smart Data Approach. *Int. J. Digit. Content Technol. Its Appl.* **2016**, *10*, 34–36. Available online: https://jyx.jyu.fi/handle/123456789/54088 (accessed on 18 February 2022).
46. Eskandari, M.; Janjua, Z.H.; Vecchio, M.; Antonelli, F. Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices. *IEEE Internet Things J.* **2020**, *7*, 6882–6897. [CrossRef]
47. Nie, L.; Wu, Y.; Wang, X.; Guo, L.; Wang, G.; Gao, X.; Li, S. Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach. *IEEE Trans. Comput. Soc. Syst.* **2021**, *9*, 134–145. [CrossRef]
48. Lin, F.; Zhou, Y.; An, X.; You, I.; Choo, K.-K.R. Fair Resource Allocation in an Intrusion-Detection System for Edge Computing: Ensuring the Security of Internet of Things Devices. *IEEE Consum. Electron. Mag.* **2018**, *7*, 45–50. [CrossRef]
49. Mazzariello, C.; Bifulco, R.; Canonico, R. Integrating a network IDS into an open source Cloud Computing environment. In Proceedings of the 2010 Sixth International Conference on Information Assurance and Security, Atlanta, GA, USA, 23–25 August 2010; pp. 265–270. [CrossRef]
50. Mehmood, Y.; Shibli, M.A.; Habiba, U.; Masood, R. Intrusion Detection System in Cloud Computing: Challenges and opportunities. In Proceedings of the 2013 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, 11–12 December 2013; pp. 59–66. [CrossRef]
51. Monshizadeh, M.; Khatri, V.; Kantola, R. Detection as a service: An SDN application. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 19–22 February 2017; pp. 285–290. [CrossRef]
52. El-Taj, H.; Najjar, F.; Alsenawi, H. Intrusion Detection and Prevention Response based on Signature-Based and Anomaly-Based: Investigation Study. *Int. J. Comput. Sci. Inf. Secur.* **2012**, *10*, 8.
53. Chen, H. *Research and Implementation of Information Security System of Campus Network in Branch Campus*; Xiamen University: Xiamen, China, 2016.
54. Ghafur, S.; Kristensen, S.; Honeyford, K.; Martin, G.; Darzi, A.; Aylin, P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digit. Med.* **2019**, *2*, 1–7. [CrossRef] [PubMed]

55. Dymyt, M.; Dymyt, T. E-HEALTH as a Tool for Strengthening the Role of a Patient in the Process of Providing Health Services. *Mod. Manag. Rev.* **2018**, *25*, 21–34. [CrossRef]
56. Furlepa, K.; Tenderenda, A.; Kozłowski, R.; Marczak, M.; Wierzba, W.; Śliwczyński, A. Recommendations for the Development of Telemedicine in Poland Based on the Analysis of Barriers and Selected Telemedicine Solutions. *Int. J. Environ. Res. Public Health* **2022**, *19*, 1221. [CrossRef]
57. Al-Shqeerat, K.H.A.; Al-Shrouf, F.M.A.; Hassan, M.R.; Fajraoui, H. Cloud Computing Security Challenges in Higher Educational Institutions—A Survey. *Int. J. Comput. Appl.* **2017**, *161*, 22–29. Available online: https://www.ijcaonline.org/archives/volume161/number6/27154-2017913217 (accessed on 18 February 2022).