Northumbria Research Link

Northumbria
University
NEWCASTLE

algorithms

MDPI

Review

From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions

Shahid Anwar [1,*], Jasni Mohamad Zain [2], Mohamad Fadli Zolkipli [1], Zakira Inayat [3,4], Suleman Khan [4], Bokolo Anthony [1] and Victor Chang [5]

1 Faculty of Computer Systems & Software Engineering (FSKKP), Universiti Malaysia Pahang, Lebuhraya Tun Razak Gambang, 26300 Kuantan, Malaysia; fadli@ump.edu.my (M.F.Z.); bkanjr@gmail.com (B.A.)
2 Center for Computer Technology & Networking Studies, Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Malaysia; jasni@tmsk.uitm.edu.my
3 Department of Computer Science, University of Engineering and Technology Peshawar, Peshawar 2500, Pakistan; zakirainayat@uetpeshawar.edu.pk
4 Center for Mobile Cloud Computing Research (C4MCCR), University of Malaya, 50603 Kuala Lumpur, Malaysia; suleman@siswa.um.edu.my
5 International Business School Suzhou (IBSS), Xi'an Jiaotong-Liverpool University, 111 Ren'ai Road, Suzhou Dushu Lake Science and Education Innovation Industrial Park, Suzhou 215123, China; victorchang.research@gmail.com
* Correspondence: shahidanwar.safi@gmail.com; Tel.: +60-112-555-4858

Academic Editors: Sye Loong Keoh and Khin Mi Mi Aung
Received: 24 February 2017; Accepted: 24 March 2017; Published: 27 March 2017

Abstract: In the past few decades, the rise in attacks on communication devices in networks has resulted in a reduction of network functionality, throughput, and performance. To detect and mitigate these network attacks, researchers, academicians, and practitioners developed Intrusion Detection Systems (IDSs) with automatic response systems. The response system is considered an important component of IDS, since without a timely response IDSs may not function properly in countering various attacks, especially on a real-time basis. To respond appropriately, IDSs should select the optimal response option according to the type of network attack. This research study provides a complete survey of IDSs and Intrusion Response Systems (IRSs) on the basis of our in-depth understanding of the response option for different types of network attacks. Knowledge of the path from IDS to IRS can assist network administrators and network staffs in understanding how to tackle different attacks with state-of-the-art technologies.

Keywords: intrusion; attacks; information security; response option; intrusion detection

1. Introduction

As a result of the technological advances in recent years, we have become increasingly dependent on global networks when engaging in social, business, and educational activities. With the explosive use of computer networks, a number of security issues on the Internet and in computer systems have been raised. Hence, the security of Internet-connected devices from various threats has become considerably important to ensure system availability and integrity [1]. Based on the annual report of 2016 from Asia Pacific Computer Emergency Response Team (CERT) showed a tremendous increment in the amount of intrusions and cyber-attacks over the decade [2]. Similarly, according to a report from the Malaysia CERT published in 2016, 43% of 9986 malicious incidents involve intrusions during system operating hours [3]. An intrusion is a set of actions that violate security policies, including the integrity and confidentiality of data and the availability of services as well, by exploiting

the vulnerabilities in the security procedure and the implementation of the system monitored by an IDS [4,5]. By contrast, attacks can be said to be adversarial intrusions against IDS or simply a set of actions that violate the security policies associated with the IDS itself [5,6]. Despite the development of several defensive techniques such as cryptography, firewalls, and access control for secure communication, these anti-threat systems currently possess limitation in detecting intrusion attacks. Therefore, an IDS with appropriate countermeasures, such as an intrusion response system (IRS), is essential for detecting and responding to potential intrusions and attacks [7].

IDSs are the hardware or software systems that autonomously identify and response in-appropriate events (such as intrusion attacks) occur in computer systems [4]. Depending on IDS settings and configurations, IRSs can continuously monitor system health and apply suitable countermeasures to identify and respond to potential incidents and inappropriate activities effectively and hence ensures optimal security in any computing environment [8]. IDS is categorized into three types, namely intrusion tolerance, intrusion prevention system (IPS), and IRS [6,7]. The term "intrusion tolerance" is defined by [6], the capability of a personal computer system to maintain its integrity, confidentiality, and availability even when some of its components are being infected. An intrusion-prevention-system (IPS) is an IDS that generates a proactive response to stop attacks before they occur [8]. In contrast, IRS is always activated after the detection of attacks by IDS and is always generates reactive response. However, existing IDSs only provide a limited response approach and are inadequate to provide optimum response in detected intrusions. Therefore, a response option should be deployed according to the nature of attacks and IDS confidence should be improved in attaining suitable response.

Although IRSs have always been used with IDSs, they have been few research studies conducted on IRSs by academicians and researchers. Firewalls prevent external attacks only and mostly fail to detect internal attacks. To mitigate internal attacks, an intrusion detection and response system that detects and responds to threats in real time is needed. Therefore, security-related problems need to be correctly identified to ensure that suitable response options are selected for detected possible attacks. However, not all incidents are malicious in nature; for instance, a person may mistakenly obtain access to a different system by typing the address of a computer without authorization. In a different instance the same action might be performed by a cybercriminal and such an action is regarded as malicious because cybercriminals are highly skilled programmers with the intent to exploit vulnerabilities in computer systems. Thus, there is need for an IRS to distinguish malicious activity (cyber-criminal) from non-malicious activity (a person mistakenly obtaining access) and select an appropriate response option accordingly.

Furthermore, the response options should be selected according to the attacker's activity. For example, when an attacker has already logged out, terminating the session of the attacker will not be appropriate and will have no effect. Similarly, the attackers try to launch denial of service (DOS) or distributed denial of service (DDoS) attacks to make the resources unavailable to authorized users. A response option that increases service availability and performance is imperative. In spoof attacks, internal attacks, distributed attacks, and password-based attacks, attackers attempts to get access to personal data that is stored on a personal computer. Once the attacker gets access to the confidential information, the attacker can easily modify the stored data; in such cases, the response should be to enforce data integrity and confidentiality. In probing, phishing, and eavesdropping, attackers mostly attempt to collect credentials from the worldwide network and information about susceptibility as well. Thus, these types of attacks require a response option that improves data confidentiality and service availability.

This study aims to categorize network attacks and review the general attacks that may occur in computer systems. In addition, this study proposes response options according to intrusion and attack statistics. The rest of the paper is organized as follows. A description of different attacks detected by IDSs and a comparison of attacks according to affected parameters are presented in Section 2. Section 3 explains the common solution to intrusions. Section 4 describes the comparison of attacks

according to the affected parameters and various threats. Section 5 illustrates the responses to possible attacks. Sections 6 and 7 present the current challenges faced by IRSs and future directions. Finally, the conclusions of the study are presented in Section 8. Table 1 briefly outlines a list of acronyms used in this research paper.

Table 1. List of acronyms.

Symbol	Description
IDS	Intrusion Detection System
IRS	Intrusion Response System
IPS	Intrusion Prevention System
IDRS	Intrusion Detection and Response System
DIDS	Distributed Intrusion Detection System
CIA	Confidentiality, Integrity, Availability
DOS	Denial of Service
DDOS	Distributed Denial of Service
NIDS	Network-Based Intrusion Detection System
HIDS	Host-Based Intrusion Detection System
AD	Anomaly Detection
SD	Signature Based Detection
AIRS	Automatic Intrusion Response System
AAIRS	Adaptive Automatic Intrusion Response System
CSM	Cooperating Security Managers
MANET	Mobile Ad hoc Network
GIDP	Generalized Intrusion Detection System
IDAR	Intrusion-Detection and-Adaptive Response-Mechanism
AudES	Audit Expert System

2. Types of Intrusion

At the moment the majority of networks are basically unsecured, which creates opportunities for cybercriminals to access secure data. Attackers are interested in stealing information and also attempt to make digital resources unavailable to users. Numerous defensive techniques such as access control, cryptography, and firewalls can function as the front line of defense against external and internal attacks [6]. Firewalls mainly secure the front access points of a network connected node from a number of threats and attacks [7]. Cryptography allows for secure communication, whereas access control is deployed for authentication purposes. However, these anti-threat applications can only provide external security and are thus inadequate in detecting internal attacks or providing internal security to any computer system and network. IDSs address this problem by monitoring and detecting both internal and external attacks.

IDSs are hardware or software systems that automatically identify and respond to attacks on computer systems. Depending on IDS alerts, IRSs continuously monitor system health to effectively identify and address potential incidents or inappropriate activities [4]. IRSs apply suitable countermeasures to ensure security in a computing environment. Consequently, a proper mechanism for checking the optimum response of these systems is to implement alert procedures. In addition, techniques for statistically detecting attacks and categorizing attacks in terms of how they affect data integrity, availability, and confidentiality are necessary. For instance, if an attack affects the integrity of an enterprise database system, there is a need for an appropriate response to secure data integrity. However, if the attack is against the network the response should improve resource availability and network performance.

Responses cannot be evaluated without considering the proceeding incidents, as seen in Figure 1. Thus, in this instance, the main objectives of incident classification are to examine possible incidents, determine actual attacks and respective targets, and choose appropriate response options to counter such attacks. Thus, an incident may refer to any unexpected event that occurs during a program

execution in a network [8]. Specifically, an-incident occurs when an attack (natural or man-made) exploits information resources [9]. Most of the security attacks are categorized based on Figure 1.

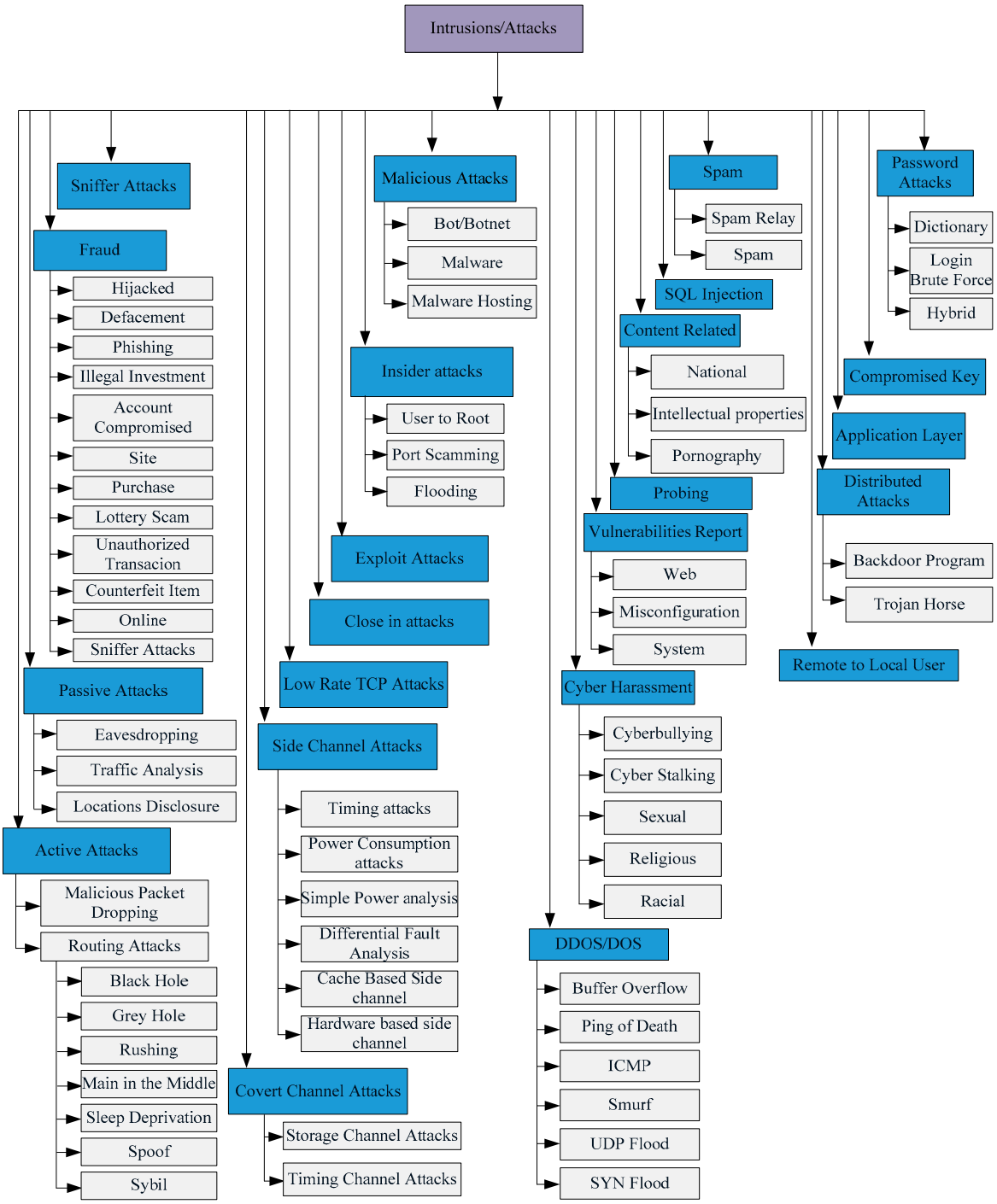

Figure 1. Types of intrusions/attacks.

However, in passive attacks, attackers only eavesdrop but do not modify any information in the system, whereas in active attacks, attackers attempt to gain unauthorized access and change information in the system with intent to destroy the entire network. Systems must be capable of rapidly recovering from such attacks. An IDS with an IRS enables a computer system to mitigate the damage and recover rapidly from incidents. These incidents are broadly divided into two sub-classes: network-based incidents and host-based incidents [10]. The application layer includes

host-based attacks such as spamming, race condition attacks, buffer overflow attacks, mail forgery, and man-in-the-middle attacks. Host-based attacks are mostly attacks against system availability, operating systems performance, and web service operations [11]. Network-based incidents include attacks on networks aimed at affecting network availability and performance. Unlike in wired networks, in which attackers target victim networks through firewalls and gateways, attackers of wireless ad hoc networks usually gain access from several access point and target any open node.

Figure 1 presents a diagram of a computer network and also presents general attacks that may be targeted at an organization [10,12]. These attacks are categorized as insider, outsider, active, passive, distributed, sniffing, spoofing, and DDoS/DoS attacks. These attacks can have some effects on system security policies such as confidentiality, integrity, and the availability of computing resources (CIA).

Table 2 describes general attacks and network-based attacks. A detailed description of each attack is given in the following table. The main categorization of these attacks is presented based on Table 2, which highlights active attacks, passive attacks, insider attacks, outsider attacks, DoS, DDoS, covert channel attacks, and side channel attacks. The attack classification aims to support the selection of a suitable response option on the basis of the specific attack behavior.

Table 2. Types of intrusions/attacks.

Types of Attacks	Ref.	Attack Name		Description
Active Attacks	[7]	Routing Attacks	Black Hole	Refers to dropped traffic in networks.
			Gray Hole	Behaves like a malicious node to drop malicious packets, but later switches back to normal.
			Rushing	A malicious node raising the speed of the routing process.
			Man in the Middle	Attacker secretly relays and intercepts messages between two parties.
			Sleep Deprivation	It targets the sensor of nodes to maximize power consumption.
			Spoof	When an attacker imitates someone else's device or a user in order to initiate attacks against network hosts, bypass access controls, steal data, or spread malware.
			Sybil	It is an attack wherein a reputation system is subverted by foreign identities in P2P networks.
		Malicious Packet Dropping		It is a type of DDoS attack similar to black hole attacks.
Passive Attacks	[5]	Eavesdropping		Network layer attacks that intercept private communication.
		Traffic Analysis		An attack that examines the communication patterns between entities in a system.
		Location Disclosure		Can expose anything about the network structure or the nodes' locations.

Table 2. *Cont.*

Types of Attacks	Ref.	Attack Name	Description
Fraud	[9]	Hijacked	The attackers take control of communication between nodes and networks, alias man-in-the-middle attacks.
		Defacement	It changes the physical appearance of a website or page.
		Phishing	It is an e-mail fraud scam that tries to obtain credentials such as credit card details, usernames, and passwords.
		Illegal Investment	Investment through others' accounts in an illegal way.
		Account Compromised	-
		Site	This fraud occurs when a user opens an infected website.
		Purchase	Using fake or stolen credit card for a transaction. The most common fraud is credit cards.
		Lottery Scam	An advanced type of Internet fraud where you get an unexpected e-mail explaining that you won a huge amount to attract victims.
		Unauthorized Transaction	Using stolen information from someone's credit card to perform a transaction.
		Counterfeit Item	Making a fake or copy of original items.
		Online	Criminal activities performed online: attackers may get someone's personal information, credit card data, or anything else private in an illegal way.
Sniffer Attacks	[10]	-	Capturing network packets and interrupting network protocol analyzing activities.
Covert Channel Attacks	[11]	Storage Channel Attacks	A covert channel allows transfer of information by an unauthorized process. A storage channel communicates by modifying a storage location. A timing channel performs operations that affect the response time observed by the receiver.
		Timing Channel Attacks	
Side-Channel-Attacks	[12]	Timing-driven attacks	This is a common threat to multi-level system such as databases, operating systems, and networks in which attackers extract information about the sensor of data that is used in the devices.
		Access-driven attacks	
		Trace-driven attacks	
Low rate TCP Attacks	[13]		It sends a burst of settled-timed packets, conceiving packet loss and incrementing the retransmission timeout for certain TCP flows. It has a severe impact on the Border Gateway Protocol (BGP).
Close-in Attacks	[5]	-	Social engineering is the main type of this attack. Getting closer to the network devices to get more information about them is known as a close-in attack.
Exploit Attacks	[7]	-	Using illegal means to utilize something to one's advantage.
Insider Attacks	[7]	User to Root (U2R)	An attacker accesses the account of normal users on a system and exploits some vulnerability.
		Port Scanning	Scan the free and less secure port for attempting attacks.
		Flooding	Sending requests to a server at the same time to shut it down by keeping the system busy.
Malicious Attacks	[14]	Bot/ Botnet	A network of infected devices connected to the Internet performs criminal activities in a group.
		Malware	This is software specially designed to damage or destroy a system or database.
		Malware Hosting	The place where malware resides can be mobile or a Personal Computer (PC).

Table 2. *Cont.*

Types of Attacks	Ref.	Attack Name	Description
DDOS/DOS	[10]	Buffer Overflow	When a program overruns the buffer boundary and overwrites the adjacent memory location.
		Ping of Death	It is a request that destroys the target device by putting an invalid packet size value in the packet header.
		ICMP	It is a kind of DDoS attack sending a huge flood of ICMP packets to the victim machine in order to crash it.
		Smurf	Sending a large number of ICMP packets to perform DDoS attack.
		UDP Flood	Sending a large number of UDP packets to random ports.
		SYN Flood	Consume enough server resources to make the system unresponsive to legitimate traffic.
Cyber Harassment	[15]	Cyberbullying	A type of bullying using the Internet. This attack can be performed using mobile devices or websites.
		Cyber Stalking	Using electronic media such as e-mail messages to harass a victim.
		Sexual	The Internet is the main source for the sexual harassment, harassment using Internet-based technologies such as email and social media platform.
		Religious	Includes forced religion conversion using electronic media and social media.
		Racial	Refers to harassment suffered by individuals or groups because of their color or race.
Vulnerabilities Report	[16]	Web	An interlinked documents type of hypertext that is accessed through the Internet.
		Misconfiguration	Configuration mistakes that result in unintended application behavior that includes misuse of default passwords, privileges, and excessive debugging information disclosure.
		System	-
Probing	[17]	-	Combining several different familiar dodging techniques for network attacks.
Content-Related		National	-
		Intellectual Properties	After research and work, finding something new or inventing something as the result of creativity is called IP.
		Pornography	Magazines, pictures, or movies that show naked people or sex in an open way.
SQL Injection	[18]	-	SQL injection is a code injection technique performed to attack data-driven applications to inject SQL statements for malicious intent.
Spam	[19]	Spam Relay	Sending e-mails to a huge number of victims by hiding the source address of e-mails.
		Spam	Sending the same messages to a large number of Internet users. These inappropriate or irrelevant e-mails are sent on the Internet to a huge number of victims.
Remote to Local User	[20]	-	Man-in-the-middle attacks can take place here.
Distributed Attacks	[19]	Backdoor Program	-
		Trojan Horse	A computer application or software that sends malicious emails or spam, or performs DDoS attacks.

Table 2. *Cont.*

Types of Attacks	Ref.	Attack Name	Description
Application Layer	[21]	-	It is very hard to defend, and vulnerabilities are always encountered here for complex user input.
Compromised Key	[22]	-	Attacker uses stolen key to gain access to the secure system or transmission, which allows the user to decrypt the encrypted data being sent by someone or a system.
Password Attacks	[23]	Dictionary	Dictionary attacks are used for decrypting the encrypted message.
		Login Brute Force	Mainly aims to get access to a website by applying the simplest method. It always involves trying several usernames and passwords again and again.
		Hybrid	It is a combination of dictionary and brute force attacks.
Adversarial Attacks against IDS	[5]	Evasion	Attacker tries to change the intrusion pattern in order to deceive the IDRS.
		Overstimulation	Intruders try to feed the IDRS with a huge number of attacks pattern to enforce to generate many false alarms.
		Poisoning	Attacker tries to inject a well-crafted pattern into the data, aiming to alter the data that are used to train and construct the detection algorithm.
		Reverse Engineering	Adversary tries to access the internal processing of IDRS and stimulates the IDRS with a familiar attack signature.

3. Common Solutions to Intrusions

Presently firewalls, access control, and cryptography are the main defensive mechanisms deployed against intrusions. As mentioned previously, these mechanisms function as the first line of defense of any network-connected, computer-based system. Cryptography is employed to ensure secure communication, whereas access control is used for user authentication. Both anti-threat applications assist to secure the overall system, but only provide external security. Thus they are inadequate in providing internal security to computer systems. A firewall is either a software or hardware system used to control incoming and outgoing traffic according to predefined rules. A basic firewall is installed at the entry points of servers to divert or allow Internet Protocols (IPs) and IP addresses. A firewall permit the arriving traffic from the worldwide through internet to access open available services such as hypertext transfer protocols and domain name servers. A number of operating systems feature built-in firewalls [24]. These firewalls mainly protect digital devices and contents but traditional ones cannot detect and block viruses, worms, and Trojan horses.

Although both IDSs and firewalls are used for network security, they have different functions: firewalls search for external intrusions, whereas IDSs protect against intrusions that originate within systems [25,26]. D. Sequeira [27] discussed in their research different types of firewalls. Traditional firewalls cannot detect internal attacks such as flooding attacks, user-to-root attacks, and port scanning because they only sniff out network packets at the network boundaries. These traditional firewalls cannot detect a complex attack such as DoS and DDoS. Moreover, traditional firewalls cannot differentiate between ordinary traffic and DoS attack traffic, as mentioned by [28,29]. Access control, which serves as the frontline of defense against intrusions, supports both confidentiality and integrity parameters.

Table 3 summarizes the defensive mechanisms according to the intrusion type and attacks. A few of the defensive mechanisms such as cryptography, firewall, and access control that are used for detecting internal attacks are shown in Table 3. However, IDS, IPS, and IRS are used for detecting internal as well as external attacks.

Table 3. Solutions to intrusions.

Intrusion Solution	Intrusion Types	Description	Attack Examples
Firewall	External	It is a system designed to stop unauthorized access.	IP spoofing, eavesdropping, DOS, port scan, and fragmentation attacks.
Access Control	External	These are systems that control or limit illegal access to a system.	Unauthorized access, password attacks, dictionary attacks, rainbow table attacks, and sniffer attacks.
Cryptography	External	To stop the coding or decoding of secret messages.	Meet-in-the-middle attacks, brute force attacks, and birthday attacks.
IDS	Internal + External	A system or device that controls and monitors a network or system.	DOS, DDOS, user to root (U2R), port scanning, and flooding.
IPS	Internal + External	Network security appliances that monitor network and/or system activities for malicious activity.	ICMP storms, ping to death, SSL evasion, and SMTP mass mailing attacks.
IDPS	Internal + External	Also known as IPS	DOS and DDOS.
IRS	Internal + External		DOS, user to root, remote to local, and prob.

3.1. Intrusion Detection System

Different phases that can be deployed as defensive mechanisms are shown in Figure 2. These phases include preventing, detecting, and responding to intrusions [30]. In the prevention phase, attacks are prevented before they happen. In the detection phase, analysis tools are developed to monitor network and host information and also identify intrusions. Response tools are used to mitigate possible intrusions detected by IDS. As stated by [4], an intrusion is a set of actions that violate security policies. Any defensive mechanism that prevents attacks before they occur is called an IPS. IPSs are IDSs that possess the same features of IDS along with the capability of preventing detected attacks. However, in the prevailing distributed environment, early prevention of attacks is impractical. An IDS is usually a hardware or software set that monitors events occurring in a computer system and identifies intrusions. Based on IDS alerts, a security countermeasure (IRS) is used to thwart detected intrusions.

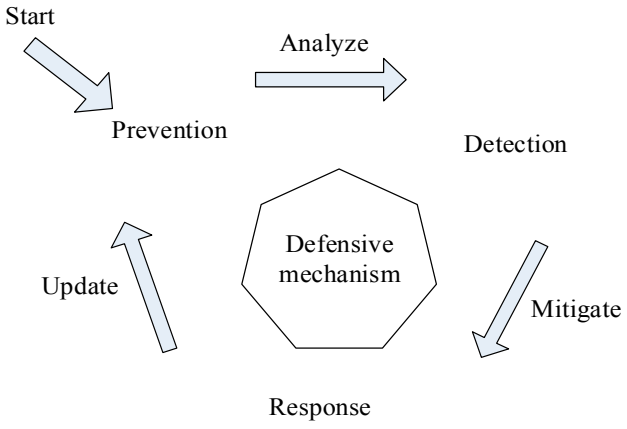

Figure 2. Defensive life cycle.

As presented in Table 4, IDSs are classified based on the monitoring environment into two sub-classes, namely network-based IDSs and host-based IDSs, that is, whether they monitor network traffic or a host system log file. IDSs are also divided into distributed-based IDSs and hybrid-based IDSs depending on the data source. According to the detection approach, IDSs are categorized into three subcategories: anomaly-detection, misuse-detection, and hybrid-detection. IDSs for anomaly detection

monitor systems for abnormality and are used for unknown attacks. ADEPTS is an anomaly-based approach that simulates an intrusion based on an attack graph used in identifying and locating possible attack paths and interdependencies between resources services [31,32]. In misuse detection, the signature of an attack is matched with the signatures of attacks stored in a database; signature-based IDSs are used only for known attacks. The IRS developed by Stakhanova [33] is a signature-based IDS that introduces a response goodness parameter to group a response as either a success or a failure. USTAT [34] is also a signature-based IDS that uses a state transition diagram for the detection of attacks; in this IDS, known attacks are represented by the state of the diagram. The hybrid approach is used for detecting firstly known and then unknown attacks. The mobile visualization hybrid IDS [4] is an adaptive hybrid IDS that uses an artificial neural network for intrusion detection. A generalized intrusion detection and prevention (GIDP) mechanism for mobile ad hoc-networks [35] combines anomaly detection, signature-based approaches and responds to intrusions in a predetermined static manner by isolating intrusive nodes. An intrusion detection and adaptive response mechanism [36] uses a hybrid approach, responds to intrusions in a flexible adaptive manner. That is, it selects a response on the basis of IDS confidence and attack severity, and conducts network performance degradation. Figure 3 presents the basic architecture of intrusion detection system.

Table 4. Intrusion detection system types.

Types of IDS	Description	Pros	Cons
Host-Based	Host-based IDSs are installed on a specific machine such as a server and mobile devices that monitor the operating system's audit information for any sign of intrusion. In addition, they detect which programs are accessing which part of the system or resources.	• At the transport layer, it monitors network traffic. • Does not require additional hardware. • Can deal with switched and encrypted environments. • Can help with the detection of a Trojan horse.	• Formation at a host may cause severe limitation-of-the network. • Any other attacks can involve software integrity breaches.
Network-Based	Network-based IDSs monitor network traffic and application protocol activity between any two computers for any type of intrusion.	• Cost-effective. • NIDS can detect attacks that are skipped by HIDS. • Allows for quick response. • It is easy to deploy as it does not affect existing infrastructures.	• It is far from the individual host. • Unable to monitor and analyze encrypted packets. • Requires full-time monitoring.
Hybrid	This is combination of both HIDS and NIDS components using mobile agents and a combination of anomaly- and misuse-based approaches. A system log file checker is performed by the mobile agent traveling to each host, while the overall network can be checked by a central agent for the existence of anomalies.	• Provides in-depth defense. • Gives administrators the ability to quantify attacks. • Provides an additional layer of protection. • Provides protection for the entire network.	• Generates false positives and false negatives. • Reacts to attacks rather than prevents them. • Generates an enormous amount of data to be analyzed. • It is most expensive.
Distributed	Various IDS (HIDS and NIDS) are combined by working as faraway sensors and constructing a report about intrusions. Later submits report to a centralized control, called distributed IDS. Uses remote sensors that can be host-based, network-based or even a combination of host- and network-based.	• It utilizes traffic information from various sources. • Monitoring is controlled by a central server. • Detection and response are also monitored from a central point. • Facilitates advanced network monitoring, incident analysis, and instant attack data.	• The flow of data may generate huge network movement overheads. • The system uses data packets that may be obtained from a network. • A program can be edited or interrupted by an intruder.

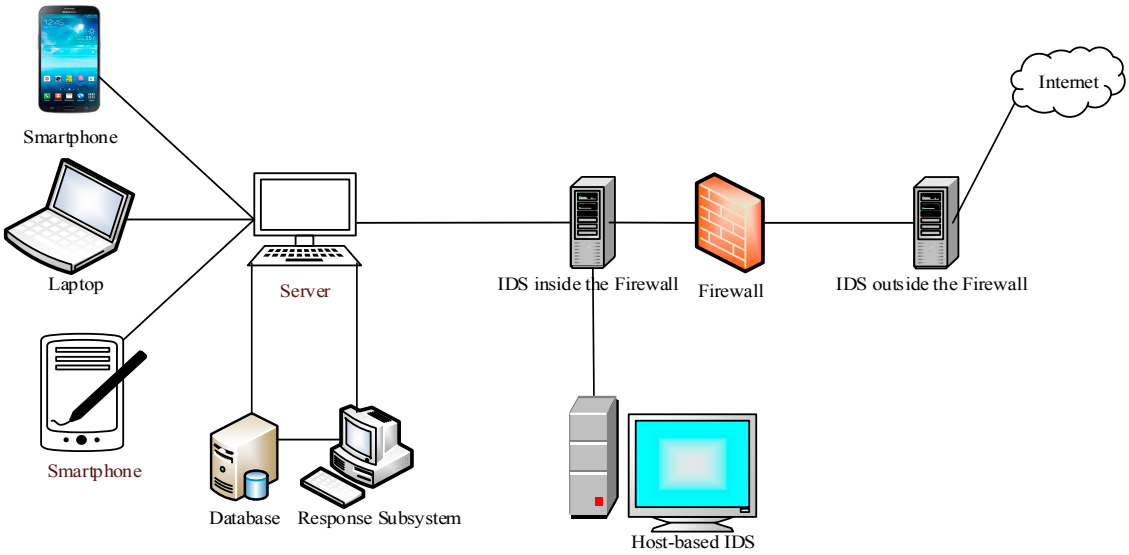

Figure 3. Intrusion detection system architecture [37].

3.2. Intrusion Response System

An IDS basically generates an alert in the form of a report and notification upon the detection of an intrusion. Without an appropriate security countermeasure, IDS is useless. A response system should be integrated with IDS to assist and find the source of an attack [38]. An IDS is classified as either passive or active depending on the response system. Passive response is further divided into notification and manual response, whereas active response is considered automatic. Similarly, an IRS has three main types: notification, manual, and automatic [39]. In a notification system, a response in the form of an alert and a report is generated and sent through e-mail or notification. By contrast, in a manual response system a predefined set of response options exists and is triggered by a security controller with the detection of an intrusion. In these two systems, the time duration within the detection and response activation opens an opportunity for attackers. The Audit Expert System [30] is a host-based misuse detection system that employs an expert system to detect intrusions. However, it simply forwards e-mails, notifications, and reports to system administrators and occasionally generates and sends urgent notifications to mobile phones.

In contrast to a manual response system, an automatic response system does not involve a human interface between the detection and response systems. Automatic IRS is further categorized into adaptive, expert, and association-based. In an adaptive system a feedback loop is used to evaluate the previous response. Expert system rules are usually applied-as-a-series-of if-then statements. Furthermore, an expert system uses the signature and anomaly-based approach to detect intrusions. The distinguishing feature of an expert system-based IRS is the separation of control reasoning from the formulated solution to the problem. The expert system has a drawback: it requires excessive initial training and extraordinary care during the lifetime, while in associative-based IRS when an attack occurs a specific predefined response associated to that specific attack is activated [40]. This approach is highly static and the basic type is based on an automated response system that initiates a static automated response upon detection of an attack. These systems are more vulnerable to attackers as the response option is static and the attackers can easily adapt the signature of the stored response strategy [41]. Network IRS [42] and USTAT [34] are associative-based response systems. Decision table and rule-based are the two approaches for automatic systems. The majority of IRSs based on a decision table are implemented where a specific response is associated with each initially known intrusion. A number of the existing IRSs [42,43] are implemented as automatic response mechanisms by using a rule-based approach for determining how to react to possible detected intrusions.

Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD) [44] is an automatic IRS that provides interoperability, high scalability, and applicability to large network infrastructures [44]. It is a distributed IDS for large-scale heterogeneous computing environments. EMERALD overcomes previous IDS limitations and is capable of detecting distributed, coordinated attacks. Furthermore, it is suitable for detecting attacks in large global networks. A signature engine, profiler engine, resolver, and resource object are the four main components of EMERALD. The resolver component is an expert system responsible for analyzing response plans to invoke various response handlers for global response selection. However, an automatic response system has a problem with the generation of inappropriate responses, which has a negative effect on response cost and network performance. Response cost refers to the effect of a generated response option on a system. Therefore, in an automatic response system a response option strategy is necessary in selecting appropriate response. From the response options, the optimum response is selected according to the attack statistics.

IRS in networks ensures security is one of the main issues in any computer networks due to heterogeneous devices that can be easily accessed and utilized. Unsecured communication in a network allows potential attackers to access the private data of users. Meanwhile, different communication networks are available, such as Wi-Fi, LTE 3G/4G, and wireless networks, which connect end users to network resource [45]. The process of transferring data from a PC (source) to the server (destination) goes through various network communication devices such as routers and switches, from which possible attackers can capture useful information. However, firewall, encryption, and access controls are common solutions offered to protect different communication networks from unauthorized access. These defensive mechanisms are unable to secure the network from malicious traffic and insider attacks [46,47]. Therefore, the installation of an IRS on the network is necessary to protect the network from malicious traffic and network-based attacks. Attacks on the network exploit physical, network, data link, and transport communication protocols.

Moreover, the open nature of the network and the lack of centralized monitoring control make wireless ad hoc networks more vulnerable to attacks such as DoS, DDoS, sniffer, port scan, and spoofing attacks [36,48,49]. Common attacks on the network comprise active and passive attacks [35]. Active attacks disrupt the operation of the attacked network and causes serious damage to the network. In passive attacks the attackers collect valuable information from the communication link to attack the functioning element in the network. Jamming, flooding, DoS, hole attacks (wormhole, blackhole, sinkhole, etc.), and Sybil types are the most common examples of active attacks. Node malfunctioning, eavesdropping, and node tampering/destruction are examples of passive attacks. Both passive and active attacks degrade the performance and operation of the entire network. Designing a single security system or IDS for a large enterprise heterogeneous network is often not practical. This is due to several challenges associated with existing IDS due to the centralized paradigm architecture that need to be overcome. Some of these challenges could be addressed by using a distributed architecture and considering network performance in the design of this architecture.

Therefore, to resolve the aforementioned security issues in the computer network, an IRS must have automatic countermeasures to continuously monitor network traffic for various types of malicious activities. The IRS can be divided into two types: autonomous and cooperative [50]. Autonomous IRSs handle intrusion independently at the time of detection, while cooperative IRSs have the ability to autonomously configure response systems in finding intrusions in the network. Most of the IRSs in the network are built based on a cooperative approach. The network-based IRS is deployed in the transport layer to monitor network traffic for various types of intrusions.

A layered security system can reduce the possibilities of being hacked as it provides multiple ways of integrating security [51]. In addition, the IRS terminates network connections when any network traffic matches the stored signature of malicious behavior in its database [52]. CSM, ADEPT, and network-based IRS are designed for the network environment in detecting any malicious behavior in the network and also provide useful countermeasure responses [31,42,53]. IDAR [36] is a flexible and adaptive approach that takes the benefits of both knowledge-based and anomaly-based techniques

to secure MANET from a variety of attacks. The selection response is based on the confidence level of the detected intrusions, the attack severity, and the network performance degradation. Furthermore, some of the IRS in networks are given in Table 5 with underlying detection techniques and description.

Table 5. IRSs in networks.

Domain	Ref	IRS	Underlying Detection Techniques	Description
IRS in Networks	[54]	NetSTAT	Misuse	To propose IRS, in which stream of audit data is matched with a stored signature of attacks descriptions for the evidence of the occurring attacks.
	[55]	A-NIDS	Anomaly	To detect intrusion events that are previously unobserved, but for which the false alarm rate is high.
	[56]	AIDP	Anomaly	To propose AIDP in MANET for the detection and mitigation of DDoS attacks.
	[36]	IDAR	Hybrid	To provide a flexible response to attacks instead of a static response without isolating the effected node.
	[57]	A-NIDS using Fuzzy	Anomaly	To propose intelligent techniques with the help of machine learning such as fuzzy logic to prevent and classify network attacks.
	[35]	GIDP	Hybrid	To propose a fixed response approach to intrusions by isolating the intruding node.
		Network IRS	N/A	To compare intrusion severity and response cost, an assessment algorithm is proposed.

4. Comparison of Attacks According to Affected Parameters

Without considering actual attacks, the response options for attacks cannot be evaluated; therefore, Table 6 is used to illustrate the effects of some of the most popular attacks and their effects on CIA [29,48]. Intrusion attacks on PCs usually violate the security parameters, previously referred to as CIA [58]. Attackers try to breach the confidentiality by approaching a computer system or data storage without approval (either implicit or explicit). When cyber-attackers try to edit any information residing in or passing through a computer system or to change the-system-state, these attacks are tantamount to integrity contravention. An intrusion/attack is considered a violation of resources when cyber-attackers try to make resources unavailable to the target or users.

Some attacks affect the confidentially and integrity of data, whereas some affect service availability. For instance, flooding attacks (e.g., DoS and DDoS) make the resources of a system unavailable to its intended users, as shown in Table 6. Therefore, to mitigate these types of attacks IRS must be designed to improve performance and service availability. Similarly, network sensors are more vulnerable to availability and confidentiality attacks. The attackers try to overload the network sensor by generating more packets to flood it, so it fails to process the successive packets. This prevents the network sensors from getting unauthorized access to the web server and uses a database server to exploit valuable information. Hence, network-based IDS is implemented to reduce the effects of flooding (DoS or DDoS) attacks and increase the network bandwidth [59]. Attackers in spoofing attacks and distributed attacks try to access and modify stored data. Therefore, response options should be selected according to affected parameters that can improve data confidentiality, availability, and integrity, as shown in Table 6.

Table 6. Comparison of attacks according to affected parameters.

Attacks	Ref.	Example	Objectives	Affected Parameters		
				Confidentiality	*Integrity*	*Availability*
Insider	[60]	Flooding attacks, user to root, and port scanning.	The authorized user tries to harm the network.	√	x	√
Flooding Attacks	[61]	DOS, DDOS, Direct and Indirect DOS,	Attackers try to flood or block a machine or network by sending invalid information.	x	x	√
DOS	[61,62]	Ping of death, Buffer overflow, ICMP flood, Smurf, UDP flood, SYN flood.	Attackers try to make resources unavailable to the intended users.	x	x	√
Port Scanning	[63]	TCP scanning, UDP Scanning, SYN scanning, FIN scanning, ACK scanning, and Window scanning.	Attackers try to find the open port, closed ports, and filtered port in a list of open ports for attacking services running on these ports.	x	x	√
Application Layer Attacks or Host based attacks	[62]	Spamming, race condition attacks, buffer overflow attacks, and man-in-the-middle attacks.	These attacks target the application layer and cause faults in the application or in a server's operating system.	x	√	√
Passive attacks	[35,64]	Eavesdropping, traffic analysis, and location disclosure.	The intention of passive attackers is to disturb the performance and operation of the network and locate valuable information.	√	√	x
Active attacks	[35,64]	Routing attacks and malicious traffic dropping.	Active attacks interrupt the network operation by introducing malicious code, modifying information, and causing damage to the entire network, which results in network performance degradation.	√	√	√
Routing Attacks	[65]	Spoofing attacks (IP and URL spoofing), rushing, gray hole, black hole, Cybil, man-in-the-middle attacks, and sleep deprivation.	Routing attacks aim to modify the routing protocol in mobile ad hoc network (MANET).	√	√	√
Code Red Attacks	[66]		To exploit a known vulnerability in Microsoft IIS servers.	x	√	√
Side Channel Attack	[23]		To extract confidential information from systems by exploiting computational characteristics.	√	√	√
Covert Channel Attack	[67]		To extract secret information by using a covert channel.	√	√	√
Adversarial Attacks Against IDS	[59]		These attacks disable the IDRS and affect the detection accuracy of IDS by modifying their internal processing and disrupting the functionality of the detection algorithm.	x	x	√

Data Threats and Response Options

As a result of global networking, which promotes data outsourcing and open access, data leakage has become a major risk in the context of big data, targeting databases and threatening privacy. Furthermore, data integrity, availability, and confidentiality are major concerns in large-scale collaborations, involving big data that frequently change [68,69]. Computer attacks usually violate three major parameters denoted by CIA plus control [58]. As defined in Section 6, the components of CIA are the usual targets of attackers. As for attacks on control, a control violation occurs when an (unauthorized) attacker is granted privilege to violate the access control policy of a system [70].

All the above incidents, as explained in Section 3, affect the integrity, confidentiality, and availability of a computer system and network resources [61]. Specifically, in DDoS and DoS attacks an attacker slows down a computer system by sending a huge number of queries to a network and trying to make resources unavailable to authorized users. For such attacks, a response that increases performance (or service availability) is necessary. In spoof attacks, internal attacks, distributed attacks, and password-based attacks, a computer system is under the control of attackers who can play with personal credentials. In this case an efficient response is needed for improving data integrity and confidentiality. In probing, phishing, and eavesdropping attacks, cyber-attackers attempt to collect private data and possible vulnerabilities from worldwide networks. In such cases, the response mechanism should improve service availability and data confidentiality.

5. Responses to Attacks

We live in an era when information technology systems are always prone to risk and may be compromised. However, organizations are not always prepared to offer a proper response to security incidents. With the sustained increment in number of incidents, advanced and distinct response options for response execution process have become necessary. Although Internet users do not always intentionally probe, monitor, attack, or attempt to access the information of an organization without authorization, they can potentially do so. A PC in an organization may also be affected by viruses and potential attacks.

Moreover, digital devices and contents are unsecure because of the connectivity of external devices. Attacks have become considerably complex and automated existing antiviruses programs are no longer sufficient. Numerous technical issues including efficiency enhancement of antiviruses and system damage reduction have yet to be resolved. When IDSs receive threat information, they generate responses on the basis of the nature of the intrusion/attack. As mentioned in Section 5, IDSs are categorized as either active or passive according to their response options. Active responses are those that immediately respond to an intrusion to protect data assets without human participation. However, the pitfall of this approach is that the security configuration under a passive response is greater than under an active response [71]. Moreover, passive responses are not automatic response systems and do require human involvement, thus facilitating the movement of data by authorizing alarm events on information assets.

However, the disadvantage of this approach is that information assets are usually leaked to intrusions during security administrator investigation. It may unnecessarily slow up the network traffic since alarm events are blocked based on responses that generate alarms and report results. In this approach, some responses are automatic and activated without human involvement. By contrast, non-automatic response systems need human intervention [70]. The common active responses of IDSs for hindering possible attacks include suspending IP addresses, blocking IP addresses, blocking ports, injecting TCP resets to terminate connections, changing access control lists, reconfiguring routers, and firewalls. IDSs mostly generate alarms in the form of an onscreen alert or a popup window. The Simple Network Management Protocol traps and reports generate alarms to network management systems. Using a proper IRS in the form of an antivirus that supports the entire network infrastructure can help with responding to intrusions within a specific timeframe [72].

However, in adaptive IRS the response is always dynamic based on the response parameter and attack nature. During the selection of dynamic response options, the response manager is mostly concerned about the cost of the response. The requirement of the distributed environment is mainly to have a cost-sensitive and adaptive IRS. In cost-sensitive IRS, the main contribution is that the cost of any response should always be lower than the damage cost [50]. Figure 4 illustrates how a suitable response is selected if the response cost is less than the combined cost of damage and confidence level. The response process is activated when the pattern detection probability exceeds a predefined threshold, as shown in Figure 4. Damage cost and response costs (DC and RC respectively) are static input parameters utilized for optimum response selection. There are two steps that determine the applicable response. In the first step, the responses are selected based on the condition: DC $\times$ confidence level $\geq$ RC, where the confidence level is the pattern detection probability. In the second selection step the cost-sensitive response selection is based on the success-factor (SF) and response-factor (RF) of the triggered response. The percentage of successful responses in the past is denoted by SF, whereas the risk factor shows the impact the considered response will have on legal users. EV(Expected value) is the basis of the ideal response selection for response rS of a sequence where

$$\text{S: EV (rS)} = \text{Prsucc(S)} \times \text{SF} + (\text{Prrisk(S)} \times (-\text{RF})),$$

where Prsucc is the probability of the occurrence of sequence S. This study selects the optimum response only if the (EV (Rs)) value is high, whereas a higher EV indicates a better response.

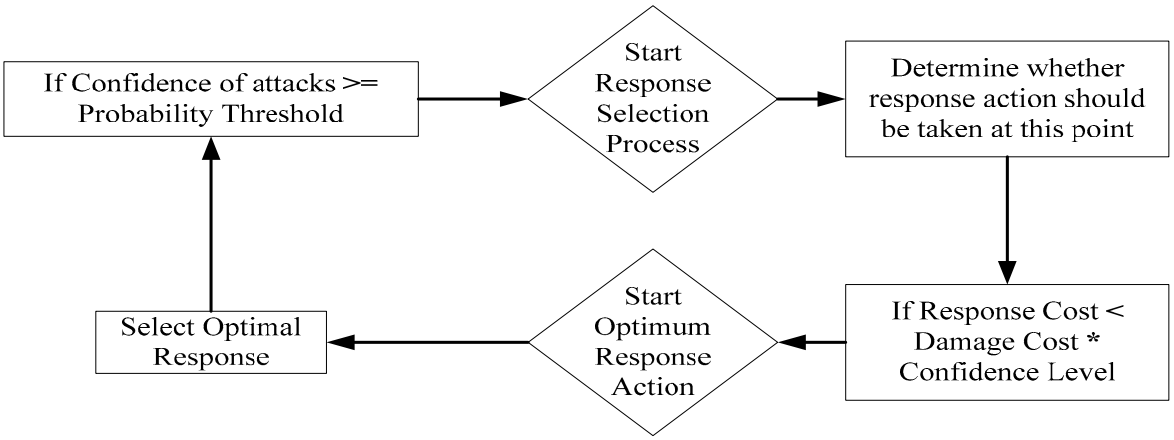

Figure 4. Response selection process.

Protecting network and computer systems against exploitation before such an exploitation occurs is impossible because vulnerabilities are not known in advance. Intrusions can occur in a PC without any connectivity to a network. With the development of a global network and information sharing, security problems have become more serious than ever. Modern network-based IDSs [73,74] and host-based IDSs [31,44] can initiate responses in addition to simple alarms or notifications. Analysis results recorded in a log file are used to generate a report based on the attack response type. Immediate responses trigger an alarm linked to the network manager console, after which a message is promptly displayed in the security manager's page and an e-mail is also sent to a system administrator. These are possible examples of response options [75]. This section presents some common response options for host- and network-based IDSs. These responses are summarized in the Table 7 as follows:

Table 7. Response option for host- and network-based IDSs.

Responses	Description
Report/Alarm generation	An alarm or report is generated with the detection of an intrusion attack.
Isolation	Completely and immediately isolates the affected node.
Relocation	Relocates the affected server by allotting a new different address.
No Punishment	In some cases, when the response causes a blip in the network performance, it ignores the attack.
Service Denial	Upon detection of an intrusion, the nodes stop providing services (not sending or receiving data).
User Account Locking	Once the user accounts are changed, the intruders should be locked out.
Remote Locking	In this response the affected server is blocked from remote areas.
IP Address Blocking	Once the intrusion is detected, the IP address of that network node should be blocked.
Network Disconnection	The affected node is disconnected from the network.
Attack Port Disabling	The port that may be the cause of an intrusion is disabled.
Backup Creation	If there is an attack detected, a backup of the infected device should be created.

In report/alarm generation, intrusive behavior is communicated through reports, e-mail messages, pager messages, or a console window that provides critical information to system administrators. Next the intruding node should be completely and immediately isolated from the network. Although the main disadvantage of this technique is attributed to the network performance degradation. A GIDP mechanism responder should be installed to detect incidents in all cases in a predetermined fixed mode by isolating the intrusive nodes that may cause a variety of attacks [35,76]. In some cases the direct isolation of critical attackers could cause the whole network to shut down; thus, in avoiding such a case, a relocation response is adopted for securing the network system [77].

Furthermore, in a no-punishment response an intrusion is simply ignored when the performance of the network is not affected by the intrusion. In addition, if the cost of the response is greater than the cost of damage from attack, the no-punishment response option is activated from pre-stored response options. In a service denial response a network node terminates the services offered by or provided to intruders. The locking of user accounts is a response in which the account of a user is locked and the session of the user is terminated to prevent future attacks. The purpose of an ICMP response is to ensure that the attacking host identifies the victim network or prevents a "requested service is unavailable" response [78].

However, differentiating true attackers from normal users is difficult, so enabling remote logging in to another system is the best method to collect additional information about attackers. Blocking the IP addresses of specific attackers is also an alternative. The shutdown response option is the most suitable mechanism for protecting a network or a computer system under active attack from being further compromised. Network disconnection is an appropriate solution against network-based attacks when shutting down the host or the network system is not an option. In a response involving the disabling of attacked ports, a specific port used as the basis for attack generation is disabled. These responses effectively stop attacks without affecting other system resources.

Symantec Security Response systems protect computer systems from Code Red attacks. Code Red [79] is an attack on the IIS (Microsoft Internet Information) web server. Symantec Security Response offers a tool for performing vulnerability assessment on a high number of infected IIS web servers to remove Code Red attacks. Creating an up-to-date system backup is one of the responses to prevent attacks against system integrity. Real-time backup is difficult because the degree of suspicion is increased when a network system is being attacked, thus the time gap should be decreased within backups to limit the loss of or maintain the integrity of data. Figure 5 categorizes the intrusion response options according to whether they generate an active response or passive response during the response selection process. An active response refers to a response that is used to counter an incident in order to minimize the impact on victims [80].

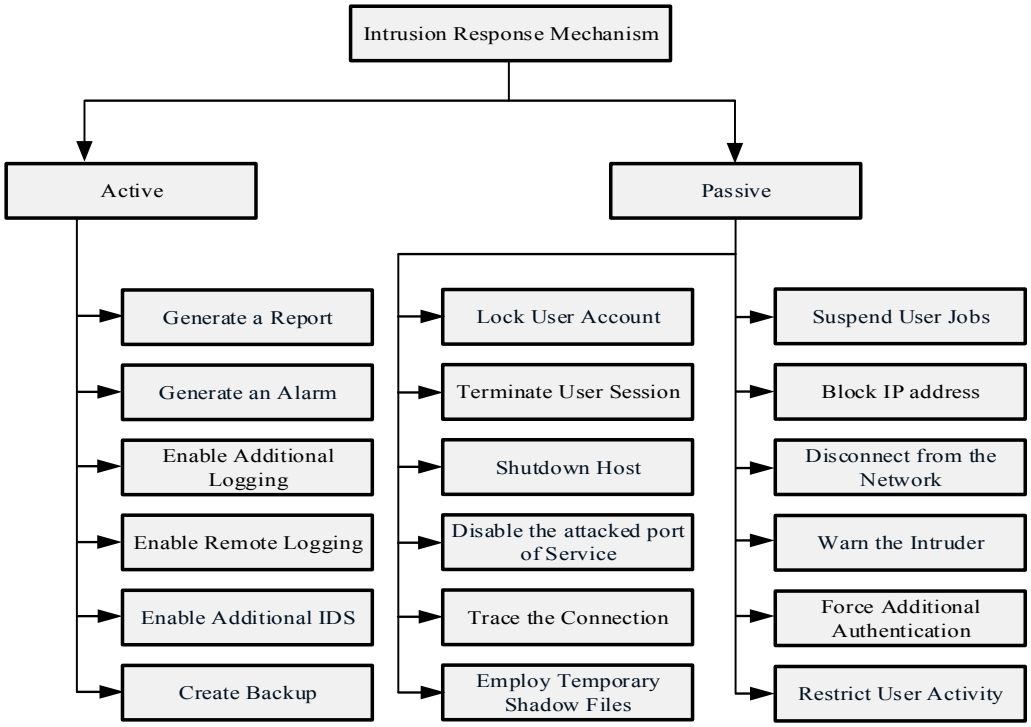

Figure 5. List of common intrusion response options.

6. Current Challenges to IRS

The following are the current challenges that affect the progress of IRSs. In addition to neglecting system requirements, the proposed IRS suffers from these challenges, which developers as well as network administrators must consider. Presently available IRSs are inappropriate for mitigating cyber-attacks and challenges as shown in Figure 6. The evolving limitations that IRS developers experience in developing IRS comprise the following:

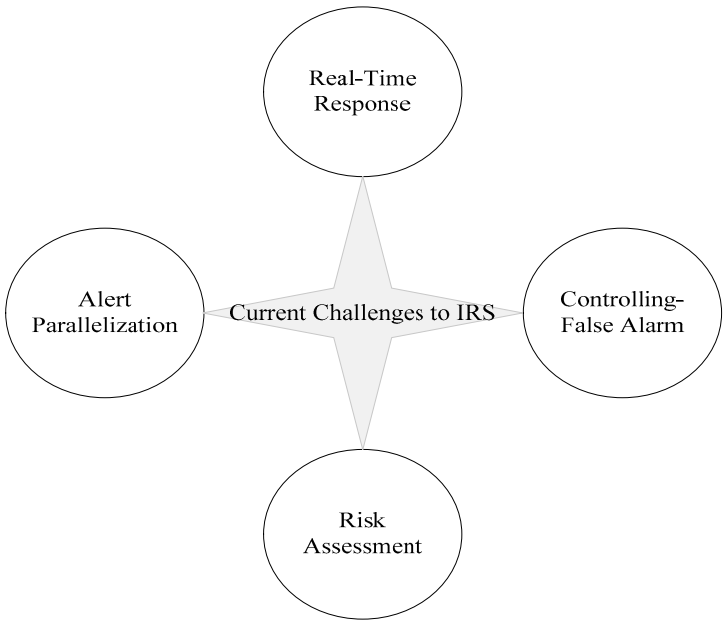

Figure 6. Current challenges to IRS.

6.1. Real-Time Response

In IRS the real-time response improves the security level by early warning security and intrusion violation threats. Thus the response system should be accurate, automatic, and active in distinguishing malicious from non-malicious activities. However, IDS products existing today are insufficient in accuracy and generate a huge false positive rate (FPR). In some cases these products are generating thousands of FPR in a single day. In this technological age it is imperative to have a proper mechanism for managing false alarms. Therefore, IRSs must be active and smart in distinguishing malicious activities from non-malicious activities. In addition, IDS and IRS have the capability to categorize responses according to the nature of the attacks and activate a response accordingly during the response selection process.

The time gap between a detected intrusion and a response creates a window of vulnerability for attackers. Another problem faced by all detection and response systems is the difficulty in analyzing packets in real-time traffic. This results in another problem that limits traffic access, thus making it very difficult for a network designer to concentrate on interpreting network performance rather than network visibility.

6.2. Alert Parallelization

In any distributed systems there are different types of IRSs that aim to monitor cyber-attacks. In each system a correlation component is inserted and should be installed on each and every host that cooperates with response and detection process. However, any intrusion correlation requires perceptive information from various systems to determine and observe the intrusions to be managed. An ontology-based intrusion alert system was presented in a study conducted by Kruegel et al. [81], but this method was insufficient for detecting zero-day attacks [81]. The alert parallelization can improve the quality of an IRS alert system by quickly identifying and monitoring intrusions. The parallelization management, alert aggregation, knowledge-based acquisition, and alerts evaluation are the most pressing challenges that should be solved.

6.3. Controlling-False Alarm

Uncertainties remain in the detection of intrusions despite the extensive research on IDSs. Moreover, the verification of whether an attack is an actual attack or a false alarm is beyond the scope of current IDSs. Therefore, a mechanism that allows IRSs to handle the false alarms generated by IDSs should be developed. IDS products' detection capabilities can be characterized in terms of accuracy and specificity. Inaccuracy in IDS in terms of generating false alarms is a huge challenge presently faced by automated response systems. Accuracy is often measured as the "true detection rate", sometimes referred to as the "false-negative rate" and the "false-positive rate". The true detection rate specifies how successful a system is in detecting attacks when they occur in real time.

6.4. Risk Assessment

The majority of existing studies consider individual topics in design issues. For instance, risk needs to be considered in designing IRSs to mitigate attacks. Selecting a good response option by IRS increases the security performance against an intruder. However, an optimum response decreases service availability.

7. Future Directions

False alarm handler, Dynamic Response Metrics, and Online Risk Assessment are important issues from an IRS design point of view. This survey shows that the currently available IRSs are unable to handle false alarms and also fail to implement an instant response, according to the attack statistics. These three parameters (False alarm handler, Dynamic Response Metrics, and Online Risk Assessment) must be included in the design of IRSs for the selection of appropriate response. There is still a need

for research on IRS to take these three parameters into consideration. Thus in future work an IRS with a false alarm handler should be included to handle the false alarms generated by IDSs. Most of the existing approaches are based on a static approach, where intrusions are mostly isolated during the response selection process. This may cause a reduction in system performance. Therefore, in future work IRSs will be integrated with a dynamic response approach to increase the network's system performance. Furthermore, with the use of online risk assessment future IRS design should be more effective at addressing this issue. However, lots of research needs to be carried out in the area of online risk assessment during the design of automated response systems.

8. Conclusions

This research study provides a comprehensive explanation of intrusions in terms of their detection and corresponding responses. A few decades back, emphasis was placed on the development of automatic IRSs to overcome the effects of different intrusions. However, IRSs still require extensive research, especially with regard to the selection of proper response options through an automatic response selection process based on intrusion types. Different response options must be activated and executed for each intrusion type to mitigate and overcome the effects of such intrusions. However, developing a perfect automatic IRS that completely detects and prevents different types of intrusions is still a challenge. Therefore, IRSs are considered a trending and growing research domain to be explored in terms of response option selection, response time, attack mitigation, alert generation, and adaptability. Comprehensive research must be conducted to achieve the goal of establishing an optimal automated IRS design and architectural framework.

Acknowledgments: The authors are grateful to the Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang for funding this research study under the Grant GRS140392.

Author Contributions: S.A. and Z.I. have studied the literature about the research in this paper. S.A. with the assistance of M.F.Z have analyzed the studied literature and found a research gap for writing a review. Then S.A under the continuous guidance of J.M.Z, M.F.Z., and S.K have written a review paper on the studied literature title as "From Intrusion Detection to an Intrusion Response System: Fundamental Requirements, and Future Direction". B.A. and V.C. contribute in the drafting and proofreading of this manuscript and finalize the paper with some future direction.

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

References

1. Ren, S.Q.; Tan, B.H.M.; Sundaram, S.; Wang, T.; Ng, Y.; Chang, V.; Aung, K.M.M. Secure searching on cloud storage enhanced by homomorphic indexing. *Future Gener. Comput. Syst.* **2016**, *65*, 102–110. [CrossRef]
2. Asia Pacific Computer Emergency Response Team. Available online: http://www.apcert.org/ (accessed on 20 September 2016).
3. Malaysia Computer Emergency Responce Team Incident Statistics. Available online: http://www.mycert.org.my/en/ (accessed on 20 September 2016).
4. Scarfone, K.; Mell, P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*; Report Number: 800-94; NIST Special Publication: Gaithersburg, MD, USA, 2007.
5. Inayat, Z.; Gani, A.; Anuar, N.B.; Anwar, S.; Khan, M.K. Cloud-Based Intrusion Detection and Response System: Open Research Issues, and Solutions. *Arab. J. Sci. Eng.* **2017**, *7*, 1–25. [CrossRef]
6. Fraga, J.; Powell, D. A fault-and intrusion-tolerant file system. In Proceedings of the 3rd International Conference on Computer Security, Dublin, Ireland, 12–15 August 1985; pp. 203–218.
7. Inayat, Z.; Gani, A.; Anuar, N.B.; Khan, M.K.; Anwar, S. Intrusion response systems: Foundations, design, and challenges. *J. Netw. Comput. Appl.* **2016**, *62*, 53–74. [CrossRef]
8. Anuar, N.B.; Papadaki, M.; Furnell, S.; Clarke, N. An investigation and survey of response options for Intrusion Response Systems (IRSs). In Proceedings of the Information Security for South Africa (ISSA), Johannesburg, South Arfica, 2–4 August 2010.

9. Hajian, S.; Domingo-Ferrer, J.; Martinez-Balleste, A. Discrimination prevention in data mining for intrusion and crime detection. In Proceedings of the 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, France, 11–15 April 2011; pp. 47–54.
10. Neela, K.; Kavitha, V. A survey on security Issues and vulnerabilities on cloud computing. *Int. J. Comput. Sci. Eng. Technol. (IJCSET)* **2013**, *4*, 855–860.
11. Wu, Z.; Xu, Z.; Wang, H. Whispers in the Hyper-space: High-speed Covert Channel Attacks in the Cloud. In Proceedings of the USENIX Security Symposium, Washington, DC, USA, 14–17 August 2012; pp. 159–173.
12. Yarom, Y.; Falkner, K. FLUSH+ RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. In Proceedings of the USENIX Security, San Diego, CA, USA, 20–22 August 2014; pp. 719–732.
13. Chang, C.-W.; Lee, S.; Lin, B.; Wang, J. The taming of the shrew: Mitigating low-rate TCP-targeted attack. *IEEE Trans. Netw. Serv. Manag.* **2010**, *7*. [CrossRef]
14. Anwar, S.; Zain, J.M.; Zolkipli, F.; Inayat, Z. A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing. In Proceedings of the ISCI 2014—IEEE Symposium on Computers & Informatics, Sabah, Malaysia, 28–29 September 2014; p. 5.
15. Workman, M. A behaviorist perspective on corporate harassment online: Validation of a theoretical model of psychological motives. *Comput. Secur.* **2010**, *29*, 831–839. [CrossRef]
16. Bernaschi, M.; Ferreri, F.; Valcamonici, L. Access points vulnerabilities to DoS attacks in 802.11 networks. *Wirel. Netw.* **2008**, *14*, 159–169. [CrossRef]
17. Duc, A.; Dziembowski, S.; Faust, S. Unifying Leakage Models: From Probing Attacks to Noisy Leakage. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014; pp. 423–440.
18. Halfond, W.G.; Viegas, J.; Orso, A. A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE International Symposium on Secure Software Engineering, Washington, DC, USA, 13–15 March 2006; pp. 13–15.
19. Naser, A.; Majid, M.A.; Zolkipli, M.F.; Anwar, S. Trusting cloud computing for personal files. In Proceedings of the 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, South Korea, 22–24 October 2014; pp. 488–489.
20. Hoque, M.S.; Mukit, M.; Bikas, M.; Naser, A. An implementation of intrusion detection system using genetic algorithm. *arXiv*, 2012; arXiv:1204.1336.
21. Ranjan, S.; Swaminathan, R.; Uysal, M.; Knightly, E.W. DDoS-Resilient Scheduling to Counter Application Layer Attacks Under Imperfect Detection. In Proceedings of the INFOCOM, Barcelona, Spain, 23–29 April 2006.
22. Yi, S.; Naldurg, P.; Kravets, R. Security-aware ad hoc routing for wireless networks. In Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, CA, USA, 4–5 October 2001; pp. 299–302.
23. Liu, F.; Yarom, Y.; Ge, Q.; Heiser, G.; Lee, R.B. Last-level cache side-channel attacks are practical. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 17–21 May 2015; pp. 605–622.
24. US-CERT. Available online: https://www.us-cert.gov/ncas/tips/ST04-004 (accessed on 12 September 2016).
25. Khan, S.; Shiraz, M.; Wahab, A.W.A.; Gani, A.; Han, Q.; Rahman, Z.B.A. A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing. *Sci. World J.* **2014**, *2014*, 27. [CrossRef] [PubMed]
26. Genge, B.; Siaterlis, C.; Karopoulos, G. Data fusion-base anomay detection in networked critical infrastructures. In Proceedings of the 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Budapest, Hungary, 24–27 June 2013; pp. 1–8.
27. Sequeira, D. Intrusion Prevention Systems Security's Silver Bullet? Available online: http://www.sans.org/reading-room/whitepapers/detection/intrusion-prevention-systems-securitys-silver-bullet-366?show=366.php&cat=detection (accessed on 9 September 2016).
28. Anwar, J.M.Z.S.; Zolkipli, M.F.; Inayat, Z.; Jabir, A.N.; Odili, J.B. Response Option for Attacks Detected by Intrusion Detection System. In Proceedings of the 4th International Conference on Software Engineering and Computer System, Kuantan, Malaysia, 19–21 August 2015; p. 7.
29. Asosheh, A.; Ramezani, N. A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. *WSEAS Trans. Comput.* **2008**, *7*, 281–290.

30. Shameli-Sendi, A.; Cheriet, M.; Hamou-Lhadj, A. Taxonomy of intrusion risk assessment and response system. *Comput. Secur.* **2014**, *45*, 1–16. [CrossRef]
31. Foo, B.; Wu, Y.-S.; Mao, Y.-C.; Bagchi, S.; Spafford, E. ADEPTS: Adaptive intrusion response using attack graphs in an e-commerce environment. In Proceedings of the International Conference on Dependable Systems and Networks, Yokohama, Japan, 28 June–1 July 2005; pp. 508–517.
32. Genge, B.; Haller, P. A hierarchical control plane for software-defined networks-based industrial control systems. In Proceedings of the IFIP Networking Conference (IFIP Networking) and Workshops, Vienna, Austria, 17–19 May 2016; pp. 73–81.
33. Stakhanova, N.; Basu, S.; Wong, J. A Cost-Sensitive Model for Preemptive Intrusion Response Systems. In Proceedings of the AINA, ON, Canada, 21–23 May 2007; pp. 428–435.
34. Ilgun, K. USTAT: A real-time intrusion detection system for UNIX. In Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy, Okland, CA, USA, 24–26 May 1993; pp. 16–28.
35. Nadeem, A.; Howarth, M. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. *Telecommun. Syst.* **2013**, *52*, 2047–2058. [CrossRef]
36. Nadeem, A.; Howarth, M.P. An intrusion detection & adaptive response mechanism for MANETs. *Ad Hoc Netw.* **2014**, *13*, 368–380.
37. Kizza, J.M. *A Guide to Computer Network Security*; Springer: London, UK, 2009.
38. Khan, S.; Gani, A.; Wahab, A.W.A.; Bagiwa, M.A. SIDNFF: Source identification network forensics framework for cloud computing. In Proceedings of the 2015 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Taipei, Tiwan, 6–8 June 2015; pp. 418–419.
39. Ragsdale, D.J.; Carver, C.A.; Humphries, J.W.; Pooch, U.W. Adaptation techniques for intrusion detection and intrusion response systems. In Proceedings of the 2000 IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN, United States, 8–11 October 2000; pp. 2344–2349.
40. Carver, A.C.J. Adaptive Agent-Based Intrusion Response. Ph.D. Thesis, Texas A&M University, College Station, TX, USA, May 2001.
41. Anwar, S.; Zain, J.M.; Inayat, Z.; Haq, R.U.; Karim, A.; Jabir, A.N. A Static Approach Towards Mobile Botnet Detection. In Proceedings of the 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 11–12 August 2016; pp. 563–567.
42. Toth, T.; Kruegel, C. Evaluating the impact of automated intrusion response mechanisms. In Proceedings of the 18th Annual Computer Security Applications Conference, Washington, DC, USA, 9–13 December 2002; pp. 301–310.
43. Jou, Y.; Gong, F.; Sargor, C.; Wu, X.; Wu, S.; Chang, H.; Wang, F. Design and implementation of a scalable intrusion detection system for the protection of network infrastructure. In Proceedings of the DARPA Information Survivability Conference and Exposition, DISCEX'00, Hilton Head, CA, USA, 25–27 January2000; pp. 69–83.
44. Porras, P.A.; Neumann, P.G. EMERALD: Event monitoring enabling response to anomalous live disturbances. In Proceedings of the 20th National Information Systems Security Conference, Baltimore, MD, USA, 7–10 October 1997; pp. 353–365.
45. Shiraz, M.; Gani, A.; Khokhar, R.H.; Buyya, R. A review on distributed application processing frameworks in smart mobile devices for mobile cloud computing. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1294–1313. [CrossRef]
46. Ying, L.; Yan, Z.; Ou, Y. The design and implementation of host-based intrusion detection system. In Proceedings of the 2010 Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI), Jian, China, 2–4 April 2010; pp. 595–598.
47. Intrusion Prevention for the Cisco ASA 5500-X, Series. Available online: http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78_459036.pdf (accessed on 15 August 2016).
48. Hansman, S.; Hunt, R. A taxonomy of network and computer attacks. *Comput. Secur.* **2005**, *24*, 31–43. [CrossRef]
49. Zhang, Y.; Lee, W. Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6–11 August 2000; pp. 275–283.

50. Stakhanova, N.; Basu, S.; Wong, J. A taxonomy of intrusion response systems. *Int. J. Inf. Comput. Secur.* **2007**, *1*, 169–184. [CrossRef]
51. Chang, V.; Kuo, Y.-H.; Ramachandran, M. Cloud computing adoption framework: A security framework for business clouds. *Future Gen. Comput. Syst.* **2016**, *57*, 24–41. [CrossRef]
52. Patel, A.; Taghavi, M.; Bakhtiyari, K.; JúNior, J.C. An intrusion detection and prevention system in cloud computing: A systematic review. *J. Netw. Comput. Appl.* **2013**, *36*, 25–41. [CrossRef]
53. White, G.B.; Fisch, E.A.; Pooch, U.W. Cooperating security managers: A peer-based intrusion detection system. *Netw. IEEE* **1996**, *10*, 20–23. [CrossRef]
54. Vigna, G.; Kemmerer, R.A. NetSTAT: A network-based intrusion detection system. *J. Comput. Secur.* **1999**, *7*, 37–71. [CrossRef]
55. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur.* **2009**, *28*, 18–28. [CrossRef]
56. Nadeem, A.; Howarth, M. Adaptive intrusion detection & prevention of denial of service attacks in MANETs. In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, Leipzig, Germany, 21–24 June 2009; pp. 926–930.
57. Shanmugavadivu, R.; Nagarajan, D.N. Network intrusion detection system using fuzzy logic. *Indian J. Comput. Sci. Eng. (IJCSE)* **2011**, *2*, 101–111.
58. Lindqvist, U.; Jonsson, E. How to systematically classify computer security intrusions. In Proceedings of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 4–7 May 1997; pp. 154–163.
59. Corona, I.; Giacinto, G.; Roli, F. Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues. *Inf. Sci.* **2013**, *239*, 201–225. [CrossRef]
60. Banerjee, U.; Arya, K. Experimental Study and Analysis of Security Threats in Compromised Networks. In *Emerging Trends in Computing and Communication*; Springer: Kolkata, India, 2014; pp. 53–60.
61. Rubinstein, I.S. Big Data: The End of Privacy or a New Beginning? *Int. Data Priv. Law* **2013**, *3*, 12–56. [CrossRef]
62. TechNet. Available online: http://technet.microsoft.com/en-us/library/cc959354.aspx (accessed on 28 September 2016).
63. Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M. A survey of intrusion detection techniques in cloud. *J. Netw. Comput. Appl.* **2013**, *36*, 42–57. [CrossRef]
64. Spam and Fraud Activity Trends. Available online: http://www.symantec.com/ (accessed on 7 September 2016).
65. Nadeem, A.; Howarth, M.P. A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 2027–2045.
66. Moore, D.; Shannon, C. Code-Red: A case study on the spread and victims of an Internet worm. In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment, Marseille, France, 6–8 November 2002; pp. 273–284.
67. Wang, Z.; Lee, R.B. Covert and side channels due to processor architecture. In Proceedings of the 22nd Annual Computer Security Applications Conference, ACSAC'06, Washington, DC, USA, 1–15 December 2006; pp. 473–482.
68. Khan, N.; Yaqoob, I.; Hashem, I.A.T.H.; Inayat, Z.; Ali, W.K.M.; Alam, M.; Shiraz, M.; Gani, A. Big Data: Survey, Technologies, Opportunities, and Challenges. *Sci. World J.* **2014**, *2014*. [CrossRef] [PubMed]
69. Xu, Q.; Liu, G. Configuring clark-wilson integrity model to enforce flexible protection. In Proceedings of the International Conference on Computational Intelligence and Security, CIS'09, San Jose, CA, USA, 11–14 December 2009; pp. 15–20.
70. Bace, R.; Mell, P. *NIST Special Publication on Intrusion Detection Systems*; DTIC Document 2001; Macmillan: McLean, VA, USA, 2001.
71. Yue, W.T.; Çakanyıldırım, M. A cost-based analysis of intrusion detection system configuration under active or passive response. *Decis. Support Syst.* **2010**, *50*, 21–31. [CrossRef]
72. Raju, P.N. State-of-the-Art Intrusion Detection: Technologies, Challenges, and Evaluation. Master Thesis, Linköping University, Linköping, Sweden, February 2005.
73. Cansian, A.M.; Moreira, E.; Carvalho, A.; Bonifacio, J. Network intrusion detection using neural networks. In Proceedings of the International Conference on Computational Intelligence and Multimedia Applications, Gold Coast, Australia, 10–12 February; pp. 276–280.

74. Bonifaco, J.; Moreira, E. An adaptive intrusion detection system using neural networks. In Proceedings of the International Federation for Information Processing (IFIP) Information Security & Privacy Conference, Poznan, Poland, 31 August–4 September 1998.
75. Bace, R.G. Intrusion Detection. Available online: http://books.google.com.my/books?isbn=1578701856 (accessed on 20 September 2016).
76. Hasswa, A.; Zulkernine, M.; Hassanein, H. Routeguard: An intrusion detection and response system for mobile ad hoc networks. In Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, (WiMob'2005), Big Island, HI, USA, 2005; pp. 336–343.
77. Wang, S.-H.; Tseng, C.H.; Levitt, K.; Bishop, M. Cost-sensitive intrusion responses for mobile ad hoc networks. In *Recent Advances in Intrusion Detection*; Springer: Berlin, Germany, 2007; pp. 127–145.
78. Hawrylkiw, D. SANS. Available online: http://www.sans.org/security-resources/idfaq/auto_res.php (accessed on 30 April 2014).
79. Symantec. February 2007. Available online: http://www.symantec.com/security_response/writeup.jsp?docid=2001-080421-3353-99 (accessed on 24 September 2016).
80. Anuar, N.B.; Furnell, S.; Papadaki, M.; Clarke, N. *Response Mechanisms for Intrusion Response Systems (IRSs)*; University of Plymouth: Plymouth, UK, 2009.
81. Kruegel, C.; Valeur, F.; Vigna, G. *Intrusion Detection and Correlation: Challenges and Solutions*; Springer: New York, NY, USA, 2004; Volume 14.