electronics

MDPI

Article

Sensitivity Analysis for Vulnerability Mitigation in Hybrid Networks

Attiq Ur-Rehman [1,*], Iqbal Gondal [2], Joarder Kamruzzaman [3] and Alireza Jolfaei [4]

[1] Internet Commerce Security Laboratory (ICSL), Federation University Australia, Mount Helen 3350, Australia
[2] Cloud, Systems and Security Discipline, STEM College, School of Computing Technologies, RMIT University, Melbourne 3000, Australia; Iqbal.Gondal@rmit.edu.au
[3] School of Engineering, IT & Physical Sciences, Federation University Australia, Mount Helen 3350, Australia; joarder.kamruzzaman@federation.edu.au
[4] Department of Computing, Macquarie University, Sydney 2109, Australia; alireza.jolfaei@mq.edu.au
* Correspondence: attiqur-rehman@students.federation.edu.au

Abstract: The development of cyber-assured systems is a challenging task, particularly due to the cost and complexities associated with the modern hybrid networks architectures, as well as the recent advancements in cloud computing. For this reason, the early detection of vulnerabilities and threat strategies are vital for minimising the risks for enterprise networks configured with a variety of node types, which are called hybrid networks. Existing vulnerability assessment techniques are unable to exhaustively analyse all vulnerabilities in modern dynamic IT networks, which utilise a wide range of IoT and industrial control devices (ICS). This could lead to having a less optimal risk evaluation. In this paper, we present a novel framework to analyse the mitigation strategies for a variety of nodes, including traditional IT systems and their dependability on IoT devices, as well as industrial control systems. The framework adopts avoid, reduce, and manage as its core principles in characterising mitigation strategies. Our results confirmed the effectiveness of our mitigation strategy framework, which took node types, their criticality, and the network topology into account. Our results showed that our proposed framework was highly effective at reducing the risks in dynamic and resource constraint environments, in contrast to the existing techniques in the literature.

Keywords: IoT; ICS; hybrid networks; CVSS; $CVSS_{IoT\text{-}ICS}$; sensitivity analysis; mitigation; attack tree

Citation: Ur-Rehman, A.; Gondal, I.; Kamruzzaman, J.; Jolfaei, A. Sensitivity Analysis for Vulnerability Mitigation in Hybrid Networks. *Electronics* **2022**, *11*, 238. https://doi.org/10.3390/electronics11020238

Academic Editors: Xiaohong Jiang, Yulong Shen, Yuanyu Zhang and Tarik Taleb

Received: 6 December 2021
Accepted: 8 January 2022
Published: 12 January 2022

1. Introduction

The outbreak of COVID-19 has transformed working environments [1]. The lockdown restrictions have pushed organisations to digitise their interactions with their workforces and further facilitate remote working. As this outbreak has spread so rapidly, organisations have been forced to hurriedly buy cloud-based solutions for remote connectivity rather than building solutions for their specific needs [2]. These cloud-based solutions have helped organisations to keep operating to achieve their organisational goals. However, at the same time, these solutions have also exposed organisations' core networks to the Internet. Additionally, organisations are outsourcing the operational controls of their processes by relying on third parties to maintain the infrastructure in the cloud. In other words, with such quick transformations, an additional risk of cyber intrusion is being introduced. Existing IT security policies may not suit well due to the rapidly changing workflow of information. Sensitive data may also exist in the cloud and previous security risk assessments may be outdated, which can attract cyber adversaries to steal organisations' secrets [3], reduce their competitive edge, and put their reputation and goals at risk.

Cloud solutions are built using traditional IT data centres and servers. Their digital security policies and IT strategies are mainly designed to secure computer and database servers [4], while today's modern enterprise digital networks are fitted with IoT and industrial control systems (ICS), along with traditional IT devices. The IT devices are

usually embedded in protected core networks and interact with client machines using proxy devices. The IT nodes are rich in processing power and memory capacities. These nodes are capable of performing various functions and can be reprogrammed as per changing requirements. IoT devices are usually in the outer layers of the network and are designed for dedicated functions with limited processing power and memory capabilities. Similarly, ICS nodes are considered the most sensitive nodes for an organisation. These nodes are most restricted and well protected. Due to the sensitive nature of ICS nodes, isolated networks and well-protected digital terminals are used to interact with these nodes to avoid any production impacts. The ICS nodes are considered complex to patch or reprogram [5]. For these reasons, the digital strategies developed for IT nodes may not work well for IoT and ICS nodes. The dependencies between the various node types are the key factor for protecting the critical infrastructure. A partial node failure may appear harmless, but eventually, it can cascade to multiple critical nodes and even to the connected cloud. With the rapid shift towards cloud-based solutions, the existing threat-modelling techniques and mitigation strategies, which were mainly developed for on-premises nodes and infrastructure, are likely to be ineffectual for IoT and ICS nodes. These strategies may not provide the best protection for cyber intrusion [6].

As discussed above, the mitigation strategies for managing risks should reflect the dynamic characteristics of diverse nodes, their location, distinct functions and interdependencies. In our previous work [7], we presented attack tree-based modelling for the vulnerability assessment of various node types. As attack tree graph models are considered the best for representing the node interdependences [8], assessment has not only highlighted the critical nodes of a hybrid network but has also evaluated the path dependencies based on node vulnerability weights. In this work, building on attack tree modelling, we recommend methods to evaluate the proposed mitigation strategies. This evaluation factored in the nodes' distinct characteristics and their locality and criticality, along with their operational control restrictions, such as resource, financial and performance limitations. The overall effectiveness of the mitigation strategy was also accessed by calculating the gain in the chain of critical nodes and their neighbouring nodes with cascading improvements.

The remainder of this paper is as follows: first, we analyse and compare the existing literature and highlight the possible gaps in Section 2. Section 3 defines our methodology to address these gaps and to develop mitigation strategies. The results from various case studies are analysed in Section 4 and then conclusions are presented.

2. Related Works

Cyber threats and their mitigation strategies have been a focal research point in recent cyber security research. Due to the economic and financial impacts linked to cyber disruptions, governments and organisations are heavily investing in the cyber security space. The security policies and threat mitigation strategies for traditional computer networks and data centres are well established [9]. The typical threat mitigation cycle involves identifying the possible assets, protecting the assets, detecting and responding to the attacks, and the possible recovery of the services or data [10].

The USA National Security Agency (NSA) and European Union have also published mitigation guidelines to protect digital solutions [11,12]. These guidelines have been regularly updated and suggest common practices, such as secure coding; patching applications; hardening networks with firewalls; detecting intrusions; analysing email contents; URL filtering; Internet control; server hardening; keeping antivirus software up to date; controlling removable storage media, such as USB drives; education; encryption; multifactor authentication; controlling privileged access; network segmenting; incident management; backups; and disaster recovery plans. Although the above strategies are essential, they mainly address the cybersecurity of IT-related nodes in modern networks. Due to the distinct nature and limited capabilities of IoT and ICS nodes, the existing IT base mitigation strategies and guidelines should be extended to cover IoT and ICS devices.

In recent years, several cloud-based cyber security solutions have been proposed for hybrid networks. In 2018, Vinit et al., conducted a detailed study on information processing in cloud computing [13]. This study revealed that though moving services to cloud infrastructure is fast and scalable, organisations lose their control of the infrastructure and data. The authors suggested the use of a dedicated network and a geo-restriction to secure their services in the cloud space. Noraden et al. [14] presented a novel approach to mitigate the vulnerability of enterprise nodes by controlling network traffic to that node. Their model recommends the best mitigation strategy from a set of policies based on a predefined budget and return on investment (ROI) values. In this model, the global risk to the enterprise network is measured and a cost-effective mitigation plan is suggested that may address the host vulnerability by adjusting the network parameters instead of patching the host.

In 2018, Vincenzo et al. [15] published a cyber-threat-modelling technique for detecting threat propagation. In this approach, the possible proliferation of attack is predicted based on Kendall's birth–death–immigration (BDI) mathematical model. Ashutosh in 2019 [16] defined a cyber-attack detection algorithm, where each node monitors the performance parameters of its neighbouring nodes. When an event occurs at a node and crosses the defined threshold, then alerts are raised, and predefined mitigation strategies are adopted to isolate the affected node. The compromised node is then isolated to stop the propagation of the attack.

In 2019, Svilicic et al. [17] designed a framework to mitigate the security risks for a ship's digital networks, including the ICS controllers. In this framework, first, a comprehensive study is conducted to determine the vulnerabilities, and then safeguards are put in place for all digital devices. Penetration testing is conducted and a safety score is assigned to the ship's digital network. Abhik presented the assessment criteria for secure and trustworthy IoT devices [18]. In 2019, Arunabha published a cyber risk assessment and mitigation model based on the probability of the occurrence of an attack on a computer network, and mitigation strategies were proposed for these types of attacks by matching the dynamics characteristics from the database at the run time and calculating the possible financial loss based on historical data [19].

In 2019, Hunor et al. [20] suggested a comprehensive solution for both IT and ICS nodes of a power network. This solution uses the run-time reconfigurable network switches to monitor the traffic, detects the ambiguities, and dynamically changes the configuration of all connected switches to limit the impact. They analysed this new model with a real-life case study to evaluate its performance.

In 2020, Poudel et al. [21] recommended an attack detection and mitigation framework for ICS controllers of a microgrid. Their scheme detects the voltage variances based on historical data and auto-adjusts the voltage of connected nodes to mitigate any malicious activity. Based on a similar technique of measuring the voltage variances, Ciaran et al. [22] proposed a tool to predict future attacks on a node by comparing its performance statistics. In this model, the selected node uses deep reinforcement learning and its parameters are stored. This is then used to compare with the runtime performance. The anomalies are treated as an attack or failure.

Zhou et al. [23] published a threat mitigation technique based on a multi-agent system. In this framework, the diagnostic agents are installed at multiple nodes of cyber-physical systems to detect an attack and generate coordinated responses by adjusting the node parameters at runtime. Similarly, in 2021, Kholidy et al. [24] proposed an automated response for an attack on cyber-physical systems relying on the criticality of a node. This framework is built on a hierarchical risk correlation tree model with capabilities to measure the financial risk of an attack. In this model, the voltage variation of an attack is monitored, and then mitigation strategies are suggested based on a comparison with stored behaviours. The financial impact is also forecasted based on historical data for that node.

2.1. Gap Statements

After analysing the recent works, it is obvious that the security and mitigation modelling for IT nodes has matured and is well established. The focus in the IT nodes space is to auto-detect and mitigate the unknown threats and vulnerabilities. Traditional IT networks are evolving to hybrid networks as IoT and ICS nodes are increasingly being integrated. However, the IT security solutions developed for IT nodes cannot be applied due to the limited capabilities and heterogeneous nature of these nodes. Although Vinit's proposal [13] of using dedicated networks and geolocation to ensure security and reliability may address specific issues, overall, this may not resolve the variety of vulnerabilities, resourcing, and performance-related issues, especially for IoT and ICS nodes, since the majority of IoT devices are portable and hard to bind with dedicated networks.

Likewise, Noraden's model [14] of controlling network traffic to vulnerable nodes does address resourcing and cost constraints but may not address the actual node vulnerability based on its criticality. Limiting the traffic to central noes may result in decreasing the system performance. Vincenzo's [15] and Ashutosh's [16] frameworks are performance friendly but these may not detect the hidden vulnerability as these models are based on a reactive approach rather than a proactive approach; where early detection of vulnerabilities is essential for securing the system. Likewise, in [20–22], IoT- and ICS-related threat detection and mitigation solutions were proposed to address specific network topologies. These solutions may not be extended to all types of nodes in hybrid networks. Along with rapid transformation, the enterprise part of the hybrid network is moving into the cloud space where IT admin has limited administration capabilities. Due to rapid transformation and heterogeneous nodes, organisations are looking for a smarter way to address the risks and threats with smarter mitigation strategies. Some recent works [14,17,23] presented models to analyse the operational cost of applying mitigation. However, their work is limited to the IoT and cyber-physical systems only. Instead of looking at the segments of the network, all nodes of a network should be secured as suggested by government studies and guidelines [10–12] because attackers may make their way from weak nodes to the critical node if only one segment is protected. This needs to be addressed in the context of moving the location of IT-based nodes into cloud space. Along with securing the networks, organisations are looking for a smarter way to gain a better return on investment (ROI) on cyber mitigation policies.

2.2. Contribution

To address this gap, this study made the following contributions:

- Classification and analysis of common mitigation techniques for heterogeneous nodes for multiple network topologies, including cloud base nodes.
- Development of attack tree-based modelling for the analysis to proactively inspect the impact on all nodes of a hybrid system.
- Recommendation of efficient mitigation methods based on the node type by incorporating their distinct nature, severity assessment, operational control over the nodes, and considering the resources and cost limitation in a wider context.
- Sensitivity analysis for the accurate selection of mitigation strategies to predict the performance and financial impact.

3. Vulnerability Mitigation Framework for Hybrid Networks

Attack trees are structural diagrams that are used to represent the interdependencies between the connected nodes of a system. In cyber security space, attack trees are used to represent all paths that an attacker may use to target a particular node. This helps to identify the weak and critical nodes and all possible path combinations. Due to its strong dependency on nodes and paths, any misinterpretation of the nodes' connectivity paths may result in weakness in designing the mitigation strategies for the defence of a target node [25].

An attack tree model includes a target node, intermediate nodes, and leaf nodes. The leaf nodes are the entry points in a system. Intermediate nodes are all the possible nodes starting from leaf nodes that an attacker can use to reach a target node. The success of mitigation strategies is demonstrated by stopping an attack as close as possible to the leaf nodes. The cost to provide defence for a target node depends on the number of paths available to reach the target node, as well as the relationship between a child to its parent node. This relationship can be one of the two types: "AND" and "OR." In an "AND" type relationship, the attackers have to attack all child nodes to reach the parent node, but in an "OR" relation, it only requires compromising a single child node. Similarly, to provide defence in an "OR" relationship, all children nodes need to be protected and the cost would be the sum of providing protection to all children nodes. However, in an "AND" type relation, the propagation of an attack can be prevented just by protecting a single node; therefore, the cost would be to defend a single node.

Although there are several types of mitigation strategies depending on the node type, vulnerability, and the criticality of a node, when accessed based on the protection level, strategies can be broadly grouped into the following three categories [26–29].

3.1. Avoid

In the avoid-type mitigation strategies, the protection of a vulnerable node is provided by patching the node's weakness permanently, i.e., upgrading the operating system and using encryption and secure protocols. These types of strategies are commonly used for IT-based nodes in a hybrid network. For these types of nodes, redundant systems and equivalent sandbox environments are available. Patches are typically evaluated in non-production environments to assess for possible impacts before applying them in the production system.

3.2. Reduce

In the reduce-type mitigation strategies, the protection to a vulnerable node is provided by stopping the attack at the leaf nodes and, thereby, preventing it from propagating further in the tree. Examples include privileges restriction, blocking the IP at the network to only allow legitimate traffic to the vulnerable node. The reduce-type strategies are considered safe for IoT nodes because of the limited processing power and remote location. Due to heterogeneous technologies and varieties of operating systems, the patches are not released for IoT nodes as quickly as compared to the IT devices, leaving the reduce strategy a viable option.

3.3. Manage

In the manage-type mitigation strategies, the protection of a vulnerable node is provided by accepting its risk and applying an acceptable workaround to the node, i.e., configuring the access control to the vulnerable nodes or accepting the risk on non-encrypted traffic to the node, allowing only valid locations to communicate with the node. These types of strategies are considered safe when it comes to providing temporary protection for industrial control systems, where nodes are designed to perform dedicated functionality. Unnecessary patches are usually avoided on these nodes to prevent any unnecessary interruption in a production line. ICS nodes are also built using heterogeneous technologies and with a variety of operating systems; hence, the fixes are not released in time [30]. These nodes usually do not have direct network connectivity and are secured in demilitarised zones (DMZ).

In our study, we selected a realistic hybrid network with real-world vulnerabilities assigned to its nodes. To provide defence, we implemented the avoid-, reduce-, and manage-type mitigation strategies for these vulnerabilities. These strategies were evaluated based on the financial cost (FC) and performance cost (PC) for its implementation to our hybrid network. We analysed the effectiveness of each mitigation strategy on each type of node in our hybrid network. Figure 1 illustrates this concept using two nodes and

the associated costs. These mitigation strategies are defined by the system admins based on the node criticality, location, function, historical data, and many other local factors. Figure 1 represents the intended mitigation strategies to highlight the cost and performance constraints. It is assumed that system admins have three mitigation strategies, where for mitigation strategy 1, the financial cost must not exceed 60% of the allocated budget and performance should not reduce by more than 25% during mitigation implementation on nodes A and B. Similarly, mitigation strategies 2 and 3 were assumed on behalf of the system admin. Mitigation strategy 1 was mapped to avoid-type strategies, mitigation strategy 2 was linked with reduce-type strategies, and mitigation strategy 3 was associated with manage-type strategies.

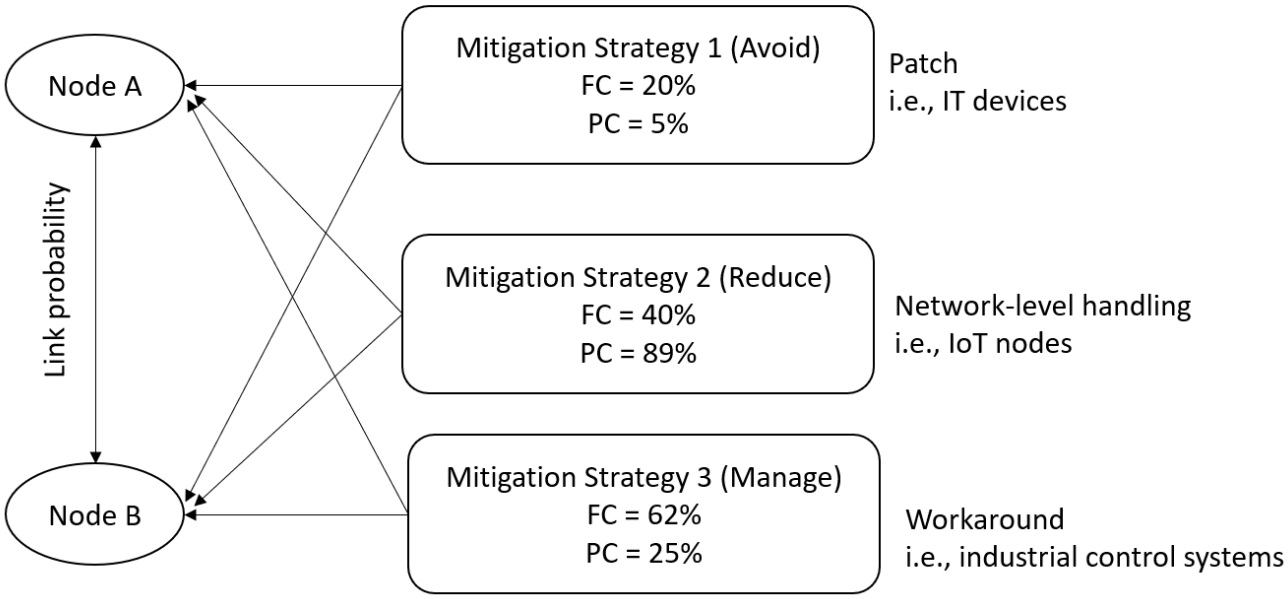

Figure 1. Mitigation categories.

The *FC* and *PC* depend on the relationship between the parent and child nodes. There is either AND or OR relation between the child and its parent node. In an AND-type relationship of child nodes with the parent, the financial cost of mitigation of a vulnerability would be equal to the *FC* factor of the child node with the lowest value. The same would be the case for the *PC* factor, as per Figure 2.

$$FC(P) = FC(C_i) \tag{1}$$

$$PC(P) = PC(C_i)$$

where *FC* represents the financial cost and *PC* represents the performance cost. The parent node is denoted by *P* and the child nodes *i* ($i = 1, 2, \ldots, n$) are denoted by C_i.

An attacker has multiple ways to be successful in an OR node. In an OR-type relationship, the *FC* of mitigating a vulnerability would be equal to the costs for all children nodes and the same is true for the *PC*.

$$FC(P) = \sum_{i}^{n} FC(C_i) \tag{2}$$

$$PC(P) = \sum_{i}^{n} PC(C_i) \tag{3}$$

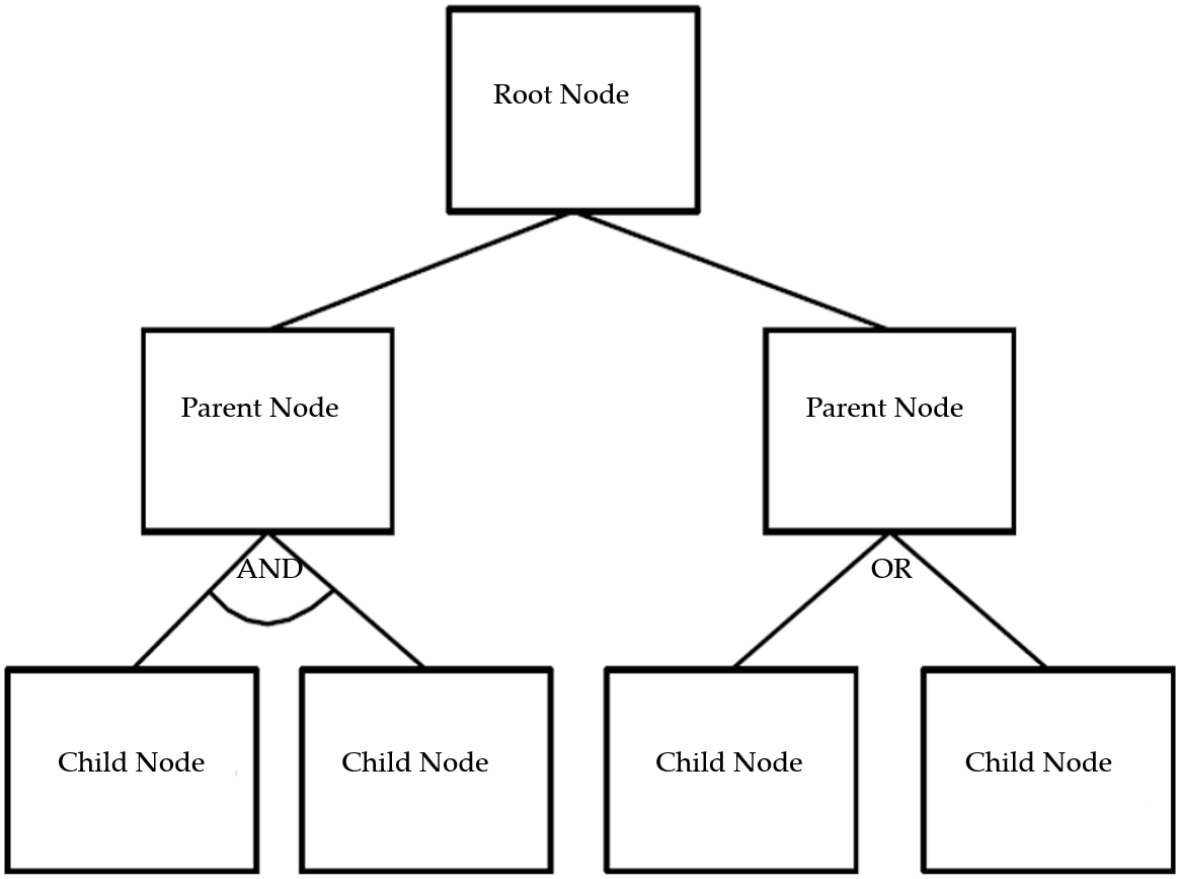

Figure 2. AND and OR relationships between nodes.

For this study, we only considered the OR-type relationship for all calculations for the following reasons:

1. This will consider the factors for all children nodes rather than one node;
2. It is more inclusive and covers all scenarios.

This work is a continuation of our previous work, where we published vulnerability modelling for networks containing IT, IoT, and industrial control system nodes, which are called hybrid networks [7]. Each node is assigned a real-world vulnerability from the national vulnerability database (NVD) [31]. The link probability for the path joining two nodes is calculated using the fitness factor method [32]. The overall system vulnerability score is determined by averaging all the link probabilities of joining nodes. Using the vulnerability security analyser tool (VSA) [33], critical nodes and paths are determined. In this study, to assess the best mitigation strategy, the hybrid network is analysed under the avoid-, reduce-, and manage-type mitigation strategies, starting from critical nodes, as shown in the sequence flow chart in Figure 3.

The mitigation strategy assessment sequence has the following steps:

1. First, the overall system score is determined using the VSA tool, which also reveals the critical nodes of the system.
2. If the system vulnerability score is under the defined threshold, then the system is declared safe.
3. Otherwise, a mitigation strategy is selected from the avoid, reduce, or manage types.
4. The selected mitigation strategy is applied to the critical nodes.
   (a) If the revealed critical nodes are the same as the central nodes, then the selected mitigation strategy is only applied once; otherwise, an alternative mitigation strategy is selected and executed.

(b) The improvement in system vulnerability score is assessed in each iteration and compared with the defined threshold using the VSA tool. This assessment also reveals the subsequent critical nodes to be mitigated for the next loop.
(c) The processing for the selected mitigation strategy is repeated till the system reaches its saturation. This is when the critical nodes become the central node. At this stage, applying the same mitigation strategy may not further reduce the system score.
(d) At this stage, another strategy is adopted, and above steps are repeated.

5. This process is repeated till the system meets the selected threshold value.

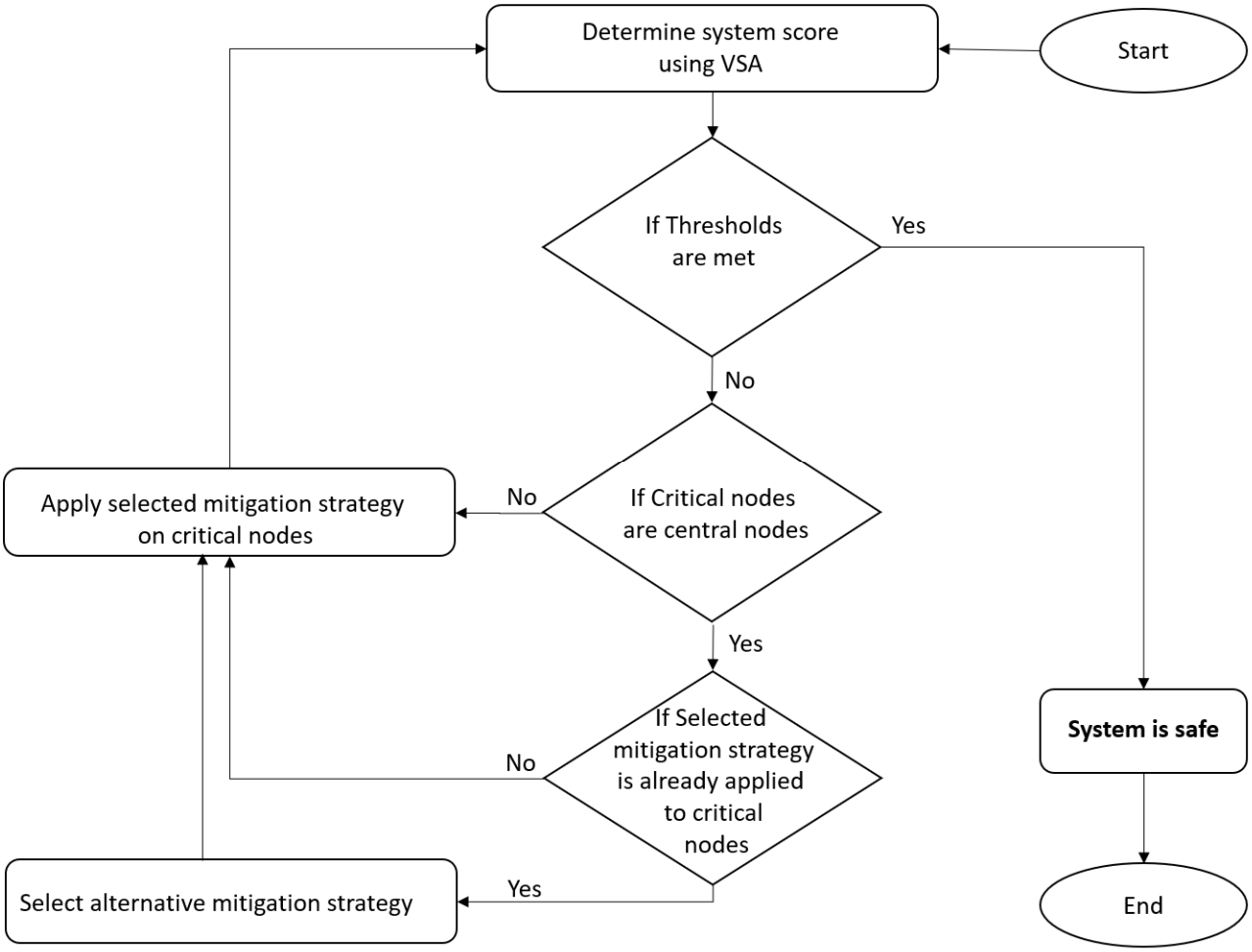

Figure 3. Mitigation strategy sequence.

In this study, we addressed the node vulnerabilities using the following mitigation strategies:

- For the "avoid"-type mitigation strategy, the vulnerable node is patched.
- For the "reduce"-type mitigation strategy, the unwanted network traffic is blocked to the vulnerable node.
- For the "manage"-type mitigation strategy, the access controls (e.g., multifactor authentication) are enforced on the affected node.

4. Sensitivity Analysis

Sensitivity modelling is a way to determine an unknown variable based on given input values. This is determined using various what-if assumptions on input data to simulate the outcome. We used this model to analyse the selected mitigation strategies to

predict the performance and financial impact. The mitigation strategy impact is analysed based on vulnerability scores and the criticality of the nodes. In this sensitivity study, we selected a hybrid network with multiple critical nodes. These nodes were evaluated using all three types of mitigation strategies (avoid, reduce, manage). The overall impact of mitigation strategies was calculated by taking the average of the improved VSA score of all connected nodes.

$$S_{is} = \frac{\sum_{i=1}^{n} X_i}{n} \tag{4}$$

where

$S_{is} \rightarrow$ *System impact score*;
$Xi \rightarrow$ *Path vulnurabilty score of the two conecting nodes*, $1 \leq X \leq 10$, as per the $\text{CVSS}_{\text{IoT-ICS}}$ framework [7];
$n \rightarrow$ *Total number of nodes*.

The system sensitivity analysis was conducted using a selected mitigation strategy. To measure the impact, the system impact score was recalculated after applying the mitigation strategy. The improvement was calculated as below:

$$S_g = \frac{S_{is} - S_{ism}}{S_{is}} \times 100\% \tag{5}$$

where

$S_g \rightarrow$ *System impact score gain rate*;
$S_{is} \rightarrow$ *System impact score*;
$S_{ism} \rightarrow$ *System impact score after mitigation*.

The system impact score gain rate (S_g) was used to drive the gain for all possible impact scores for a given mitigation strategy. The same mitigation strategies can be repeated to meet the specified threshold:

$$S_{isml} = S_g - \left(S_{is} \times \left(\frac{S_g}{100} \right) \right) \tag{6}$$

where $S_{isml} \rightarrow$ *system impact score after mitigation of l iterations* , *where* $l > 0$.

To gain the required level of confidence, the same or a combination of mitigation strategies are repeated. These iterations are denoted by l, and S_{isml} presents the system impact score for the lth iteration. To calculate the efforts required to achieve the system trust level, the following equation was used:

$$F_l = \frac{S_{is} - S_{isml}}{R \times n \times T} \tag{7}$$

where

$F_l \rightarrow$ *Mitigation cost for the lth iteration*;
$R \rightarrow$ *Resoursing efforts* (%) *required to apply* S_{isml} *on asingle node*;
$T \rightarrow$ *Time efforts* (%) *required to apply the* S_{isml} *on asingle node* .

Let us assume a system consisting of ten nodes with an initial system impact score (S_{is}) of 3, where three nodes have been identified as critical nodes and have been patched. After the patching, the link probability score has reduced for these critical nods from 3 to 2.5. Now, using Equation (5), the system impact score gain rate (S_g) is calculated. For simplicity, we have assumed that 8% of the resourcing efforts are required to apply the mitigation strategy on a single node. We have also assumed the time factor as being constant and equal to 1 in this study. Therefore, R = 8% for a single node (n = 1) and T = 1 in Equation (7) will reveal the F_l factor.

High F_l values mean higher mitigation strategy costs. By using Equation (7), the resourcing cost of all possible S_{is} values of the system can be computed and the resources can be directed efficiently to where it is more cost-friendly for a given mitigation strategy.

4.1. Case Study 1

To access and analyse the mitigation strategies, we implemented this proposed framework on a realistic supply chain system with a variety of nodes, as shown in Figure 4. It had traditional computer nodes, such as inventory management, database, operating systems, identity management systems, file transfer, and payment systems. These systems were combined in a system layer (SL). The internet-enabled devices, such as temperature sensors, gadgets, surveillance systems, and GPS nodes, were presented in the interaction layer (IL). The industrial control nodes, such as robotic arms and controllers, were part of the controller layer (CL).

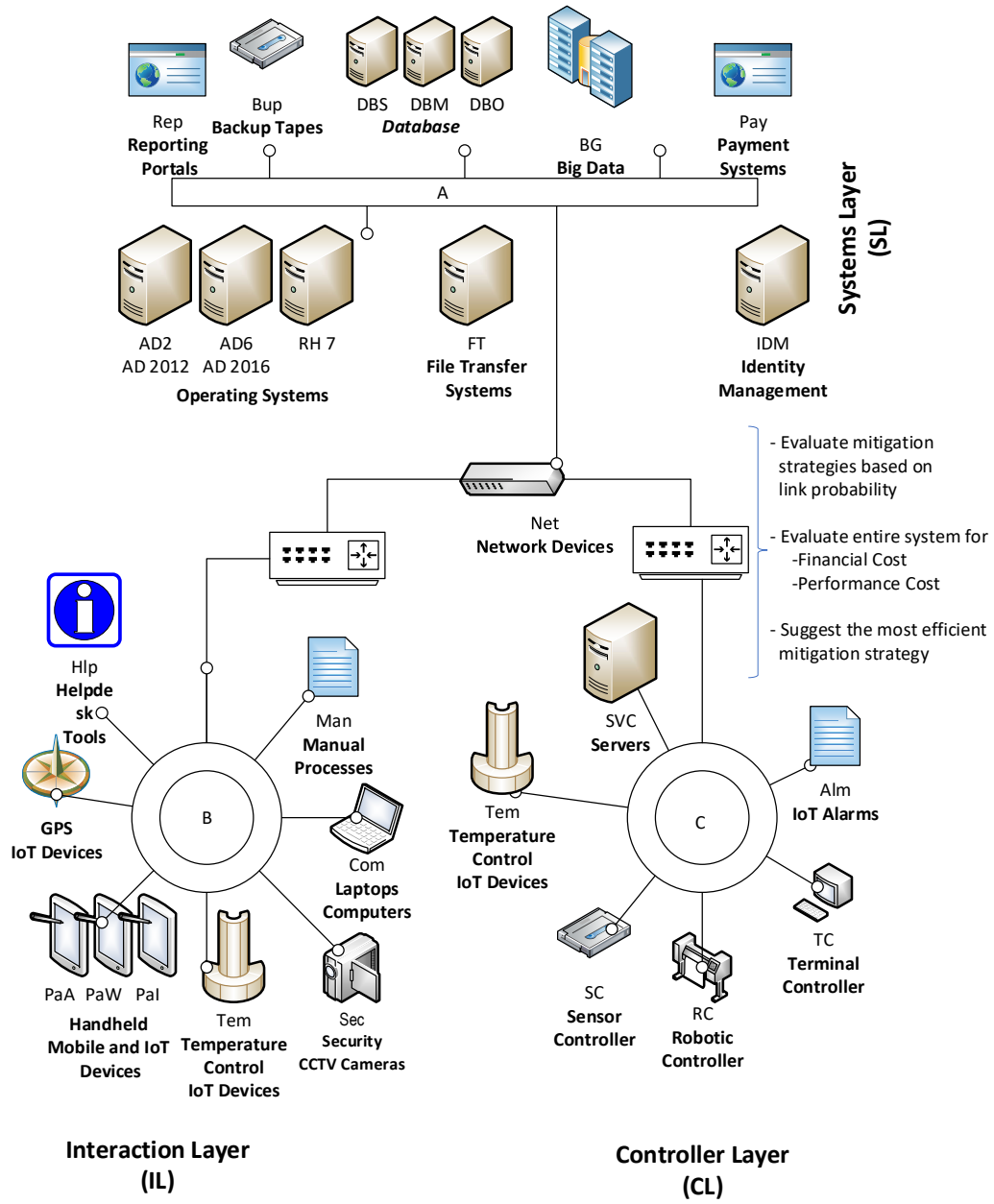

Figure 4. Supply chain hybrid network.

To analyse our supply chain system with the above mitigation strategies, we assumed the financial performance and resourcing cost for each of these mitigation strategies. In an actual setup, the system administrator can assign values that are most aligned with the organisation's IT policy and budget.

- Strategy 1 used "avoid"-type policies.
- Strategy 2 used "reduce"-type policies.
- Strategy 3 used "manage"-type policies.

It is logical that system administrators will set goals based on the enterprise policies, financial considerations, and IT performance statistics to adopt a single strategy or combination of strategies to mitigate risk. These goals are likely to vary across organisations and will be defined by the system admins. In this case study, we assumed the goals for mitigation strategy as "no more than 30% of financial cost and not compromising the performance of the system by more than 10%." The resourcing cost was kept constant at this stage for simplicity.

To implement these concepts to our selected supply chain model, first, we accessed and assigned each node with a real-world vulnerability from the NVD database, where its vulnerability score was calculated using the environmental metrics of the $CVSS_{IoT\text{-}ICS}$ framework and used as the node vulnerability [33]. The use of environmental metrics allowed the system admins to factor in the local dynamics in their calculations. The link probability between connected nodes was derived using the fitness model of graph theory [32]. This was then passed as a path probability between two nodes. Our selected mitigation strategies were evaluated based on these path probabilities, as per Figure 3.

In the next set of calculations, this model was extended to the whole tree to execute the above strategies. We used our previous work to successfully determine the critical nodes and the easiest path of this hybrid network [7]. Then, the three mitigation strategies discussed earlier were employed for this hybrid network as in Figure 5.

First, critical nodes of the tree were patched using the avoid-type strategies. For this sensitivity analysis, we assumed that a constant 15% of resources were allocated to patch a single critical node. The resource allocation values depend on the system admin's environmental experience and may change. Therefore, after applying the patch, the first iteration revealed an S_{is} value of 3.12, as per Equation (6). The same calculations were repeated for the "reduce" and "manage" types of strategies, revealing the S_{is} values shown in Table 1.

In the next step of the calculation, we considered the cascading impact by transferring the reduced risk to all nodes for each strategy to achieve a specific threshold of the system impact score (S_{is}) by repeating the mitigation strategy. These iterations are denoted as l in Equation (6) (S_{isml}) and presented in Figure 6. The VSA tool evaluated TC and net nodes as critical nodes. After the first execution of the mitigation strategy, the critical node shifted to a net node only. The second execution of the same mitigation strategy revealed the four critical nodes. These four critical nodes remained unchanged for the third and fourth iterations of the same strategy.

Depending on the complexity of the tree, it was noted that after a few iterations, the impact trends became linear, where the cost continued to rise with the same proportion, and the critical nodes were shifted to central nodes.

When the "avoid" type of mitigation strategies was applied, the overall impact score of the system was reduced significantly, hence improving the performance. Figure 7 is a graphical representation of the results produced in this case study, where the average gain in system scores is listed on the Y-axis and the mitigation strategies are on the X-axis. "Iteration 1" was the first execution of avoid-type mitigation strategies; similarly, the second iteration of the same strategy was applied on the results of the first iteration, with a cascading impact. The third iteration was executed on top of the second iteration's results. The same was the case for the "reduce"- and "manage"-type mitigation strategies and their iterations.

Table 1. Mitigation methods and their impact scores for case study 1.

Method	S_{is}
Avoid (patch)	3.12
Reduce (network control)	5.12
Manage (workaround)	5.96

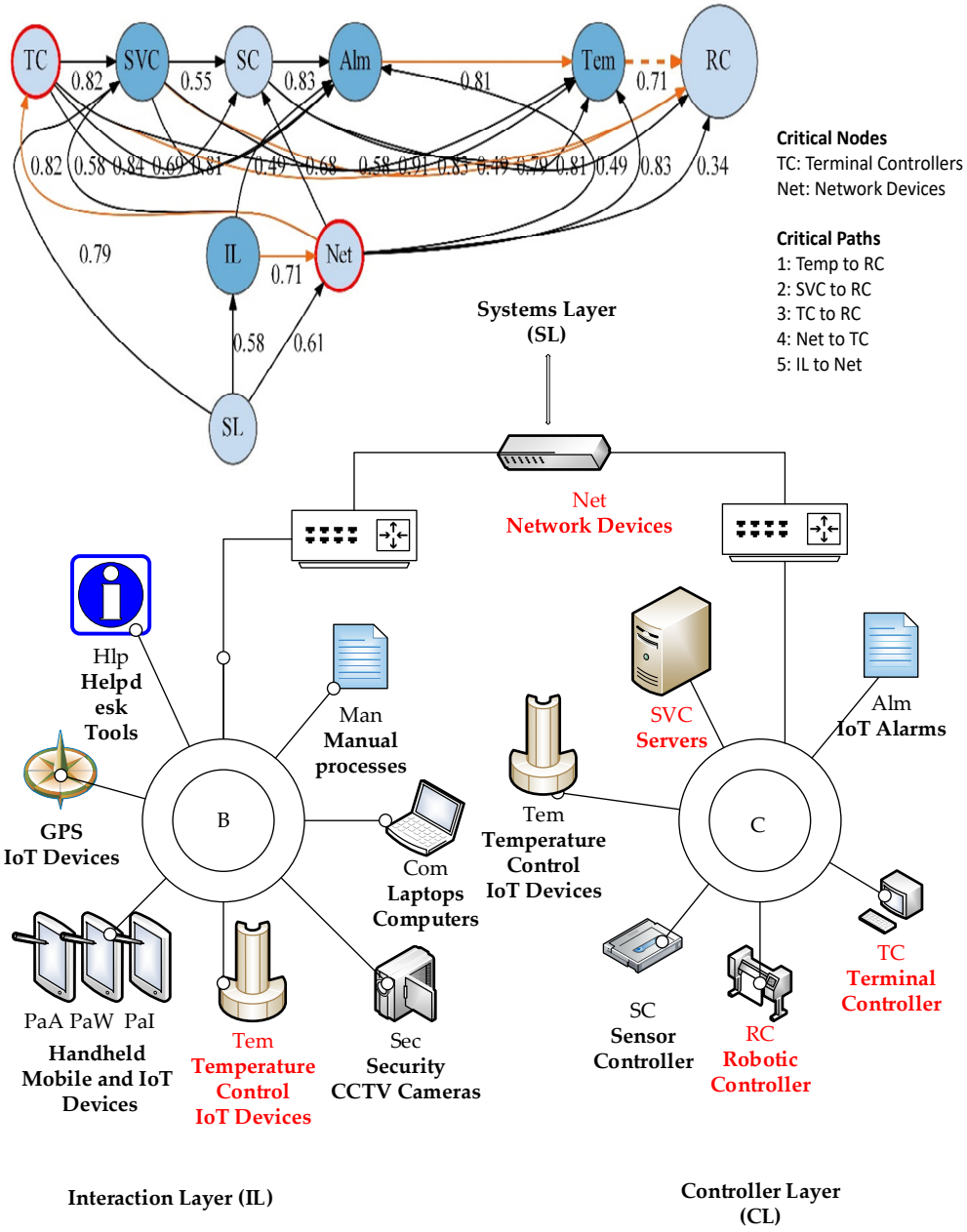

Figure 5. Critical nodes and paths for the supply chain hybrid network.

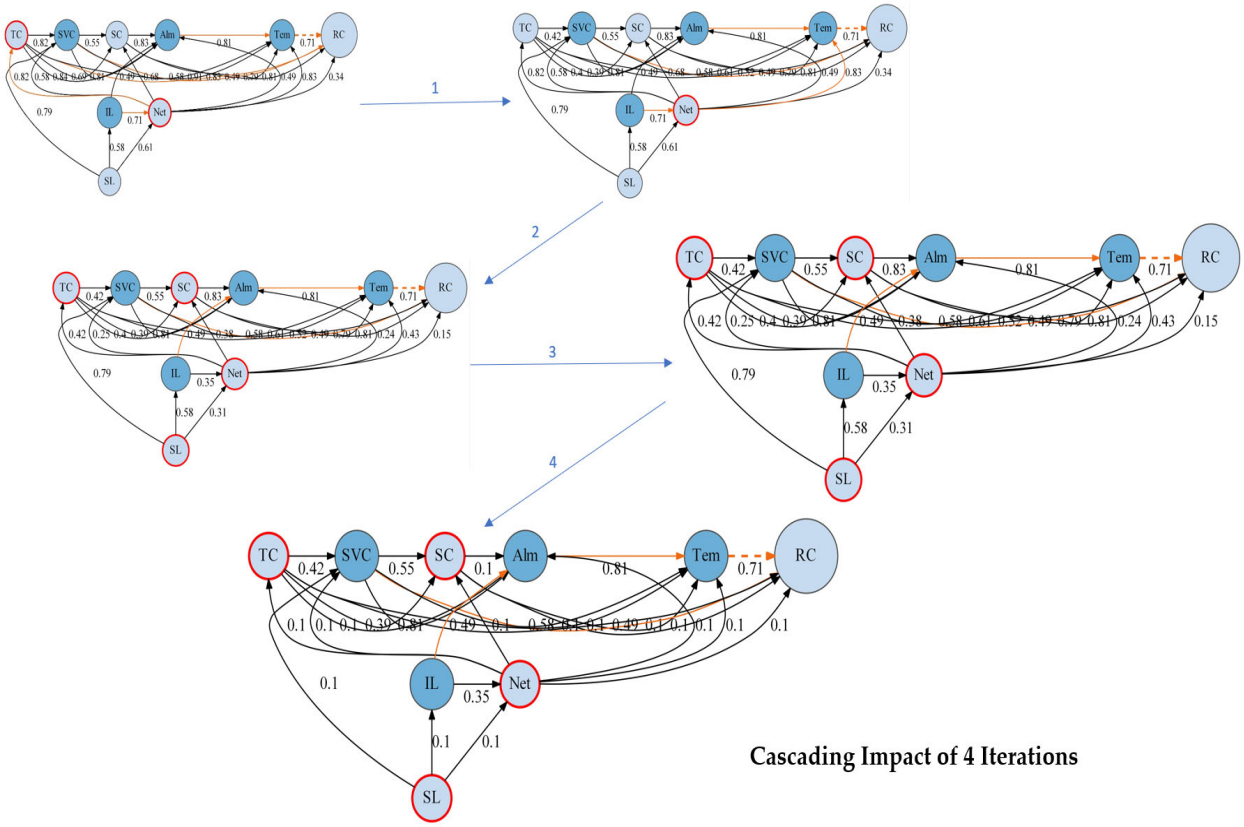

Figure 6. Changes to critical nodes and paths with the execution of mitigation strategies.

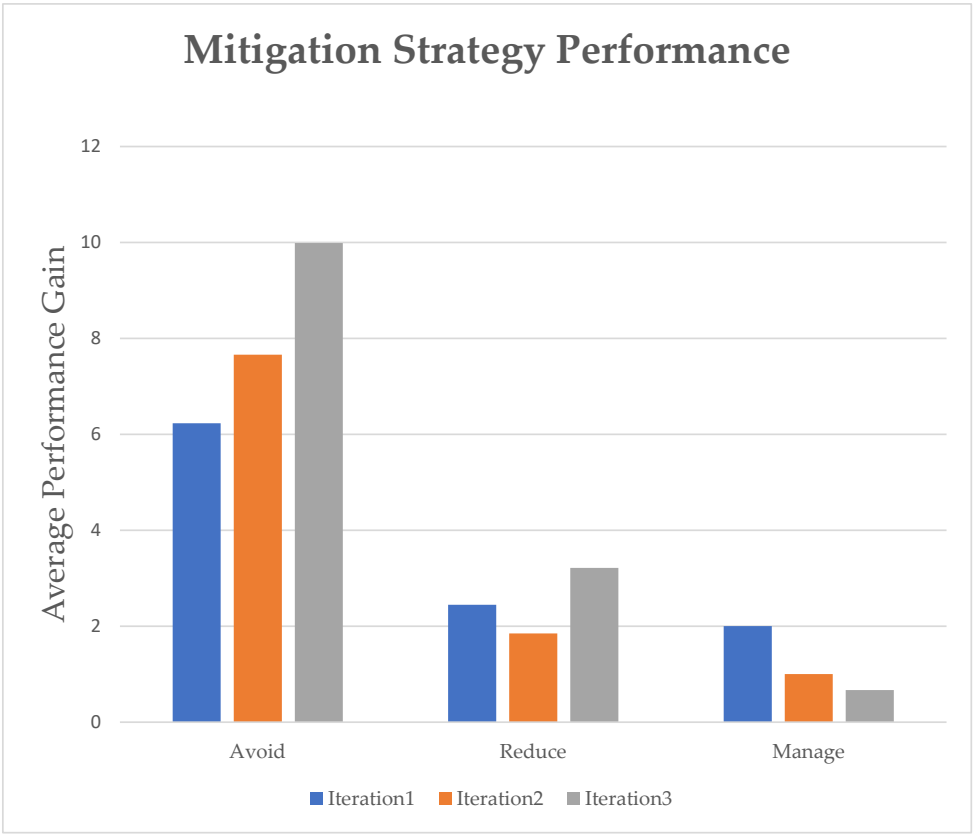

Figure 7. The efficiencies of the various strategy types for case study 1.

As per Figure 7, for the "avoid"-type mitigation strategy, iterations 1 and 2 produced more average gains by reducing the system score S_{is}, but it was the third iteration that not only reduced the vulnerability score significantly but it was also the most cost-effective with performance gains closer to 10 since, at this point, the critical nodes became the central nodes.

The same system was applied with the "reduce"-type of mitigation strategies with multiple iterations, where our strategy was to reconfigure the network nodes connected to critical nodes to stop the spread of the vulnerability. The first iteration of reconfiguring the network nodes reduced the system impact score. As the network node was one of the most central nodes in this topology, the second iteration of reconfiguring the next set of connecting devices was the least effective due to the number of neighbouring nodes required to be reconfigured. The reduce-type of mitigation strategies showed best results in its third iteration when the network nodes become the central nodes.

To continue our analysis for the "manage" type of mitigation strategies, where a vulnerability is avoided by a workable workaround on the node, i.e., implementation of multifactor authentication (MFA) to access the node. In manage-type mitigation strategies, the overall vulnerability of the system was not reduced much after many iterations (iterations 1, 2, and 3). The real benefits and cost return for this type of mitigation were in its first iteration. The repetitions (iterations 2 and 3) of this strategy hardly reduced the S_{is} score and, therefore, it was not a resource-friendly option.

4.2. Case Study 2

To confirm our findings from case study 1, we repeated the same process for another set of topologies consisting of IoT, ICS, and system devices as shown in Figure 8. In this topology, the system devices were remote in the cloud and connected to IoT and ICS systems with dedicated networks. The ICS and IoT devices were connected and controlled from cloud-based edge devices. This form of topology is getting popular with recent advancements in cloud computing.

To analyse this hybrid network, the same set of mitigation strategies (avoid, reduce, and manage) were applied. Like case study 1, the assumed goal of the system admins for this case study was also to adopt a single strategy or combination of strategies to mitigate a threat with "not more than 50% financial cost and not compromising the performance by more than 30%." The resourcing cost was kept constant at this stage, like in case study 1. The assumed financial and performance values were different from the previous case study to assess the proposed framework for a variety of goals.

We adopted the same methodology as in case study 1, where the vulnerabilities were assigned from the NVD database. The node vulnerabilities were calculated using the environmental metric of the $CVSS_{IoT\text{-}ICS}$ framework and the link probability between connected nodes was evaluated. The critical nodes were discovered using the VSA tool and their vulnerabilities were mitigated using each mitigation strategy separately. These steps were repeated to determine the cascading impact of each mitigation strategy.

Figure 9 is a graphical representation of the results produced by case study 2, where the average gain in the system score is listed on the *Y*-axis on and mitigation strategies are on the *X*-axis. "Iteration 1" is the first execution of the selected mitigation strategies. In the same sequence, the second and third iterations were executed on top of the results produced by the first and second loops, respectively. The same was the case for the "reduce"- and "manage"-type mitigation strategies and their iterations.

In case study 2, the network topology was decentralised and mostly consisted of cloud-based devices with limited control and permissions for the organisation's admins. As per Figure 9 for the "avoid"-type mitigating policies, where we patched the critical network nodes, the first and second iterations started to reduce the system score and show some performance gain, but it was the third iteration that not only reduced the score significantly but also was the most effective, as at this phase, the central nodes were the same as the critical nodes.

When the same system was applied with the "reduce" type of mitigation policies, where on premises network devices were reconfigured to reduce the spread of the vulnerability. It showed the best results in its first iteration when the critical network nodes were already central nodes. As the network nodes are central and have connections to several other nodes, the reconfiguration of all connected nodes in the second iteration and further extending to the third iteration were less cost-effective as compared with the first iteration.

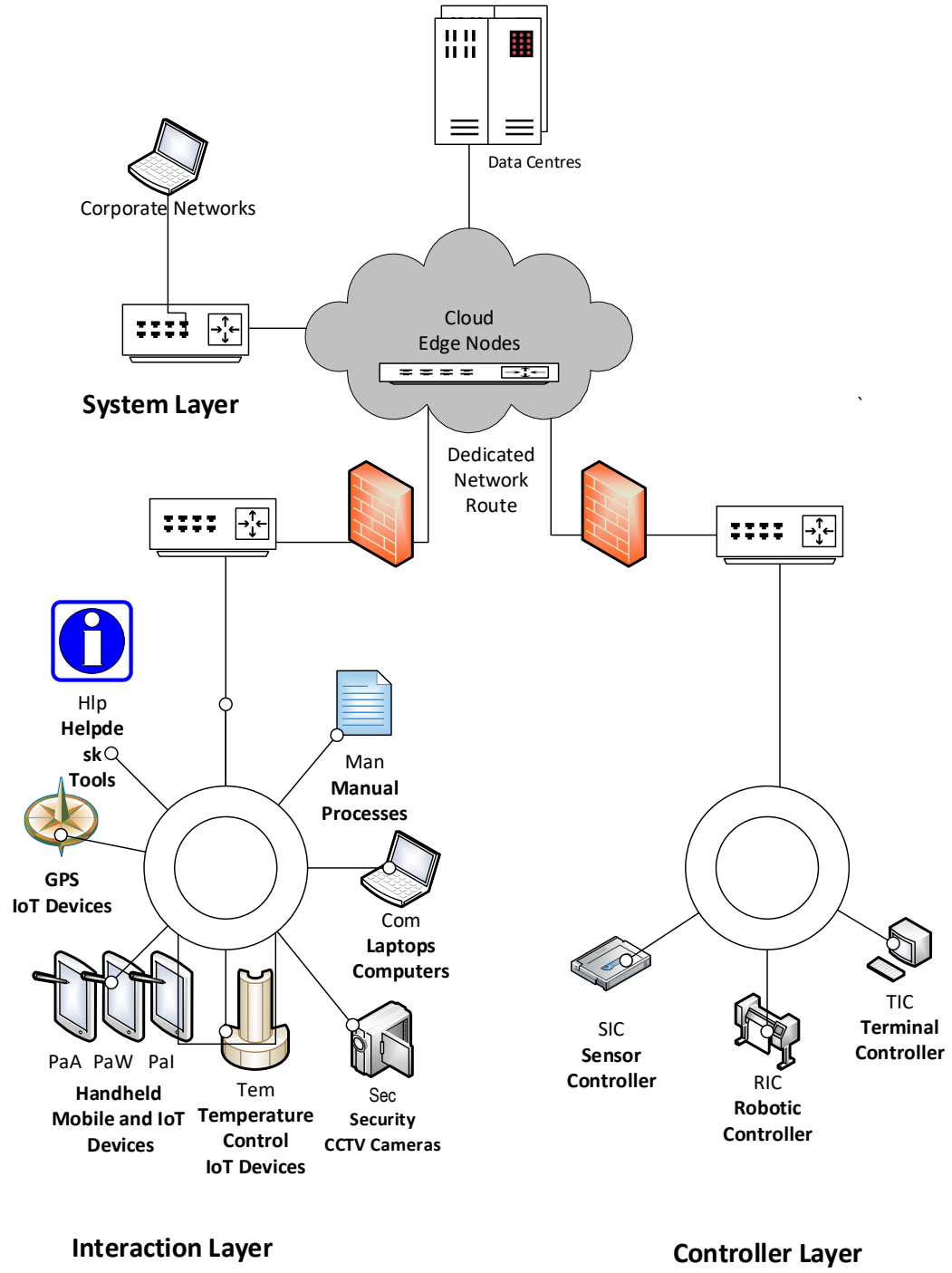

Figure 8. Hybrid network topology for case study 2.

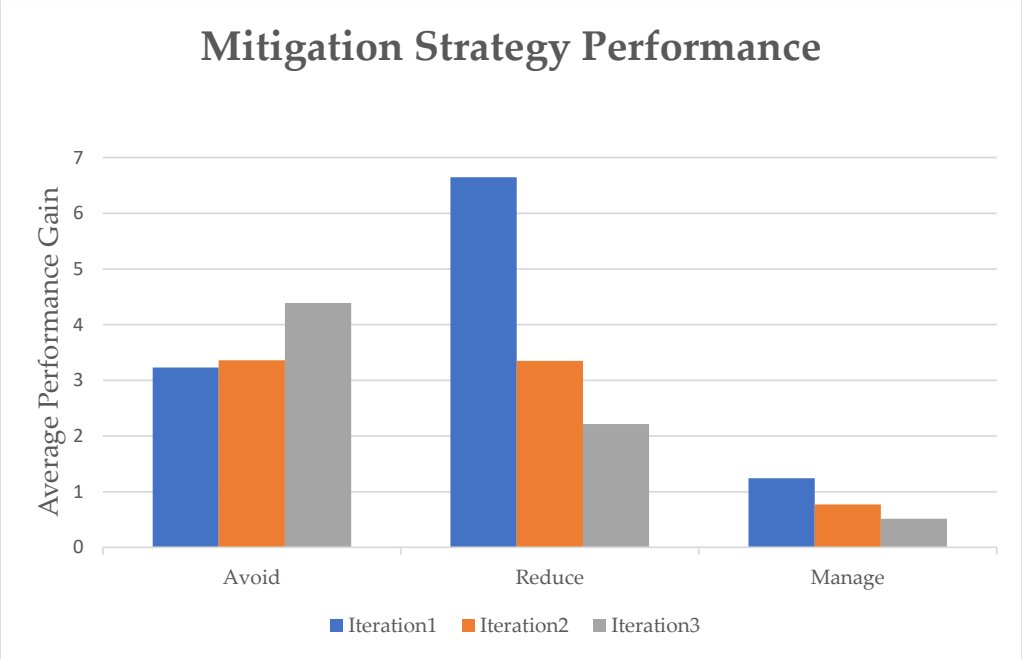

Figure 9. The efficiencies of the various strategy types for case study 2.

Like in case study 1, regarding the manage-type mitigation strategies, where access to critical nodes was restricted using MFA, the overall vulnerability of the system was not reduced significantly after many iterations. The real benefits and cost return for this type of mitigation were in its first iteration. The further execution of the manage-type strategy in connected nodes did not help in reducing the system score.

This framework was based on a graph-based attack tree model and has been broadly applied for cyber security modelling, but it also inherits the scalability challenges for complex and dynamic topologies [34].

To address these challenges, it is recommended to subdivide the complex topologies into subsystems, like in case study 1, where the nodes in the system layer of Figure 4 were computed separately and their combined impact is denoted in Figure 5 with a node called SL. The subsystem combined impact score (S_{im}) was computed and used as a combined node vulnerability to assess its impact on other nodes. These techniques of dividing the complex systems into subsystems and using the combined impact helped in scaling the dynamic and dense topologies. Along with that, it is also recommended to use a single vulnerability at a time for a given node to access its impact for the target node using the VSA tool.

5. Discussion

These results revealed that the "avoid" strategy was the most effective strategy when high-risk vulnerabilities were involved, and network nodes were not the critical nodes. Though these strategies were considered costly, they significantly reduced the system vulnerability score and improved the confidence level. The combined effect of all the above policies is represented in Figure 10. In this figure, the *Y*-axis represents the performance gain, strategy iterations are listed on *X*-axis, and executed strategy types are on the *Z*-axis. As denoted in Figure 10, The "avoid"-type mitigation strategy was the most effective and cost-friendly when the central nodes became the critical nodes, as presented by iteration 3. However, further repartition of the "avoid"-type mitigation strategies did not produce much impact. As "avoid"-type mitigation strategies require a significant amount of resources, these are recommended for the typical IT nodes, as they have a longer life cycle and are located closer to the IT admin with required permissions. The IT system vulnerabilities and their impacts are well documented and evaluated in non-production

environments before making their way to production systems. For example, USBs are scanned and accessed for risk before providing read or write access.

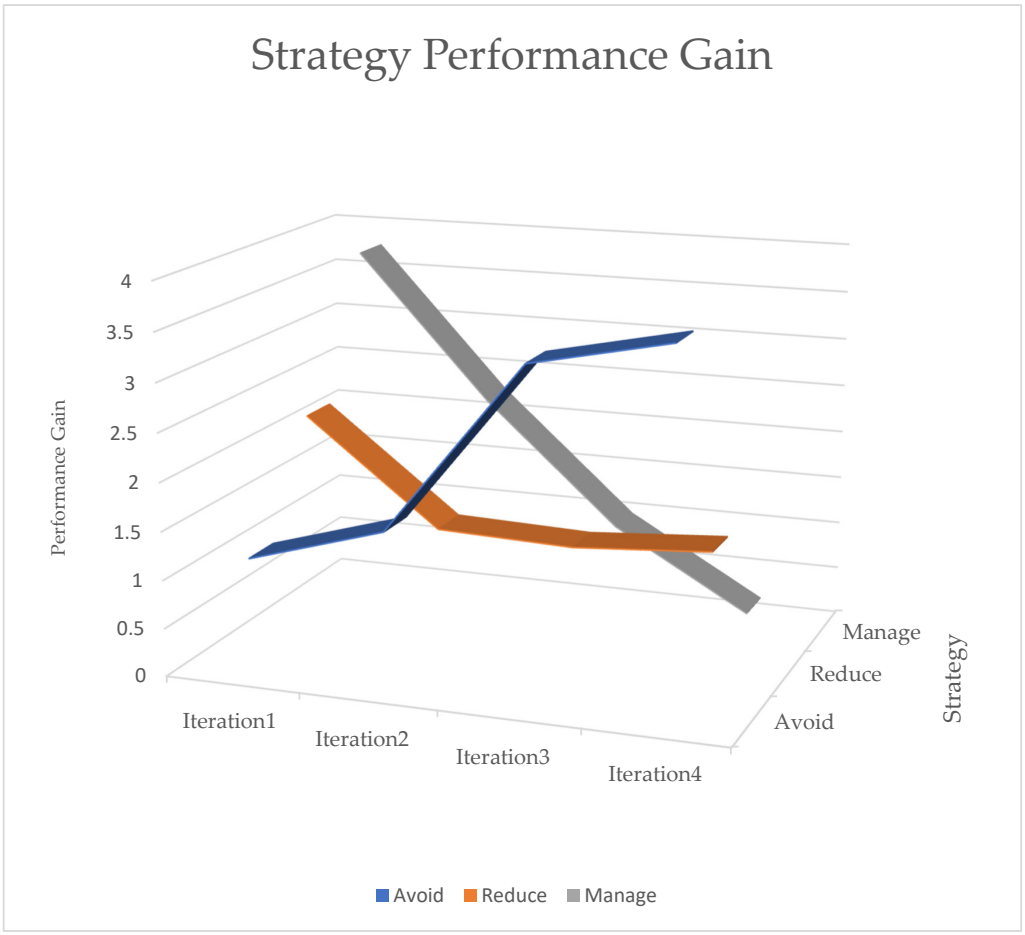

Figure 10. Combined analysis of the mitigation strategies of case studies 1 and 2.

The "reduce"-type mitigation strategies are effective for short-term measures to avoid the spread of any vulnerability in the system, especially when network nodes are critical nodes. These types of strategies are good for cloud-based topologies and portable devices, such as IoT, where the system admins have limited control over the nodes but can configure their firewalls to avoid the propagation of any attack. As the network nodes are central nodes in a cloud-based topology, further iterations of such mitigation require a significant amount of resources, as presented in Figure 10 (drop for iteration 2, 3, and 4 for the reduce-type strategy). This figure reveals that at this stage, the avoid-type strategies are more effective, as denoted by the second and third iterations in this figure. The "reduce"-type mitigation strategies should be adopted where IT admins have less control over critical nodes, nodes are remote or have less computation power, and nodes have a reduced life cycle to deploy the expensive patching, i.e., the IoT nodes. The reduce-type strategies should be adopted to stop the spread of vulnerabilities such as read-only access to USB ports for sensors.

The "manage" type of mitigation strategies provided effective results in its first iteration. Though this did not reduce the impact score, it provided an initial safeguard without impacting the production lines and was the most effective in its first iteration, as shown in Figure 10. A further iteration of the "manage"-type strategies did not reduce the vulnerability but incurred significant costs, as indicated by iterations 2, 3, and 4 in Figure 10. This was because neighbouring nodes were treated with this strategy without any significant reduction in vulnerabilities due to the increased efforts. As "manage"-type

strategies do not reduce the "impact score" (S_{is}), these are recommended for isolated and less-centralised nodes or closed networks, such as ICS, which have dedicated network zones and the most restrictive entry points. As in ICS, any patching (avoid) or configuration changes (reduce) are considered risky for the production line. For example, USB or any other connectivity to the nodes is not provided.

It is also clear from the study that patching the central node that has high vulnerability can reduce the impact score more quickly as compared with critical nodes having the least central location in the network. After a few iterations, half the critical nodes shifted to central nodes. The cost of patching the central nodes was much lower with a high performance gain as compared with other critical nodes. The most effective and cost-saving mitigation strategy was the one that addressed the risk at critical nodes along with central nodes.

6. Conclusions

Achieving the balance between improving the security and reducing the risk depends on the node type, the vulnerabilities inherited by these nodes, and developing the appropriate countermeasures to mitigate their risks. To address these issues, we developed an attack-tree-based methodology that could analyse the security of complex systems and can set priorities for system administrators according to the system criticality, possible impact of the vulnerabilities, and operational control available to promptly execute the mitigation strategies. This framework presented a viable method for system admins to protect their networks within resource and cost constraints. This research also made significant strides by using a CVSS-based method within the attack and protection tree security analysis. Rule sets were developed and assessed in a variety of applications. Future work includes the application of the attack and protection tree methodology in a variety of real-world security situations.

Author Contributions: Conceptualization, A.U.-R., I.G., J.K. and A.J.; methodology, A.U.-R.; software, A.U.-R.; validation, A.U.-R., I.G., J.K. and A.J.; formal analysis, A.U.-R., I.G., J.K. and A.J.; investigation, A.U.-R., I.G., J.K. and A.J.; resources, I.G., J.K.; data curation, A.U.-R., I.G., J.K. and A.J.; writing—original draft preparation, A.U.-R.; writing—review and editing, A.U.-R., I.G., J.K. and A.J.; visualization, A.U.-R.; supervision, I.G. and J.K.; project administration, I.G. and J.K.; funding acquisition, I.G. and J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Internet Commerce Security Laboratory (ICSL), Federation University Australia.

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

References

1. Williams, N. How COVID-19 has Impacted on Ways of Working. *Occup. Med.* **2021**, *71*, 40. [CrossRef]
2. Basu, S.; Bardhan, A.; Gupta, K.; Saha, P.; Pal, M.; Bose, M.; Basu, K.; Chaudhury, S.; Sarkar, P. Cloud computing security challenges & solutions—A survey. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 347–356. [CrossRef]
3. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
4. Alouffi, B.; Hasnain, M.; Alharbi, A.; Alosaimi, W.; Alyami, H.; Ayaz, M. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access* **2021**, *9*, 57792–57807. [CrossRef]
5. Wang, B.; Li, X.; de Aguiar, L.P.; Menasche, D.S.; Shafiq, Z. Characterizing and Modeling Patching Practices of Industrial Control Systems. *Perform. Eval. Rev.* **2017**, *45*, 9. [CrossRef]
6. Kulik, T.; Tran-Jørgensen, P.W.; Boudjadar, J.; Schultz, C. A Framework for Threat-Driven Cyber Security Verification of IoT Systems. In Proceedings of the 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Västerås, Sweden, 9–13 April 2018; pp. 89–97.
7. Ur-Rehman, A.; Gondal, I.; Kamruzzaman, J.; Jolfaei, A. Vulnerability Modelling for Hybrid Industrial Control System Networks. *J. Grid Comput.* **2020**, *18*, 863–878. [CrossRef]

8. Dewri, R.; Ray, I.; Poolsappasit, N.; Whitley, D. Optimal Security Hardening on Attack Tree Models of Networks: A Cost-benefit Analysis. *Int. J. Inf. Secur.* **2012**, *11*, 167–188. [CrossRef]
9. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2658–2693. [CrossRef]
10. NIST CyberSecurity Framework. Available online: https://www.nist.gov/cyberframework (accessed on 5 February 2021).
11. National Cybersecurity Strategies Guidelines & Tools. Available online: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools (accessed on 5 February 2021).
12. CSI-NSAS Top 10 Cyber Security Mitigation Strategies. Available online: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf (accessed on 8 February 2021).
13. Kumar, V.; Balaji, B.P. Information Management in Cloud Environment Risks and Mitigation Strategies. In Proceedings of the 2018 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS), Noida, India, 21–23 February 2018; pp. 137–140. [CrossRef]
14. Alsaleh, M.N.; Al-Shaer, E.; Husari, G. ROI-Driven Cyber Risk Mitigation Using Host Compliance and Network Configuration. *J. Netw. Syst. Manag.* **2017**, *25*, 759–783. [CrossRef]
15. Matta, V.; Di Mauro, M.; Longo, M.; Farina, A. Cyber-Threat Mitigation Exploiting the Birth-Death-Immigration Model. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 3137–3152. [CrossRef]
16. Bandekar, A.; Javaid, A.Y. Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices. In Proceedings of the 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Honolulu, HI, USA, 31 July–4 August 2017; pp. 1631–1636. [CrossRef]
17. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU J. Marit. Aff.* **2019**, *18*, 509–520. [CrossRef]
18. Chaudhuri, A. Cyber Threat Mitigation of Wireless Sensor Nodes for Secured, Trustworthy IoT Services. *EDP Audit. Control Secur. Newsl. EDPACS* **2016**, *54*, 1–14. [CrossRef]
19. Mukhopadhyay, A.; Chatterjee, S.; Bagchi, K.K.; Kirs, P.J.; Shukla, G.K. Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Inf. Syst. Front.* **2019**, *21*, 997–1018. [CrossRef]
20. Sándor, H.; Genge, B.; Szántó, Z.; Márton, L.; Haller, P. Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 152–168. [CrossRef]
21. Poudel, B.P.; Mustafa, A.; Bidram, A.; Modares, H. Detection and mitigation of cyber-threats in the DC microgrid distributed control system. *Int. J. Electr. Power Energy Syst.* **2020**, *120*, 105968. [CrossRef]
22. Roberts, C.; Ngo, S.-T.; Milesi, A.; Peisert, S.; Arnold, D.; Saha, S.; Scaglione, A.; Johnson, N.; Kocheturov, A.; Fradkin, D. Deep Reinforcement Learning for DER Cyber-Attack Mitigation. In Proceedings of the 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Tempe, AZ, USA, 11–13 November 2020.
23. Zhou, T.; Xiahou, K.; Zhang, L.; Wu, Q. Multi-agent-based hierarchical detection and mitigation of cyber attacks in power systems. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106516. [CrossRef]
24. Kholidy, H.A. Autonomous mitigation of cyber risks in the Cyber–Physical Systems. *Future Gener. Comput. Syst.* **2021**, *115*, 171–187. [CrossRef]
25. Arulkumaran, G.; Gnanamurthy, R.K. Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Adhoc Network. *Mob. Netw. Appl.* **2019**, *24*, 386–393. [CrossRef]
26. Brugere, I.; Gallagher, B.; Berger-Wolf, T. Network Structure Inference, A Survey. *ACM Comput. Surv.* **2018**, *51*, 1–39. [CrossRef]
27. Churchwell, C. *Denial of Service Attacks: Defensive versus Offensive Countermeasures*; ProQuest Dissertations Publishing: Ann Arbor, MI, USA, 2018.
28. Bjerken, A.A. *Identifying Why Organizations Fail to Adopt Active Cyber-Security Strategies Assessed Using the Unified Theory of Acceptance and Use of Technology Survey (UTAUT-S)*; ProQuest Dissertations Publishing: Ann Arbor, MI, USA, 2017.
29. Radanliev, P.; De Roure, D.; Walton, R.; Van Kleek, M.; Montalvo, R.M.; Santos, O.; Maddox, L.; Cannady, S. COVID-19 what have we learned? The rise of social machines and connected devices in pandemic management following the concepts of predictive, preventive and personalized medicine. *EPMA J.* **2020**, *11*, 311–332. [CrossRef] [PubMed]
30. Kawanaka, T.; Matsumaru, M.; Rokugawa, S. Software measure in cyber-attacks on production control system. *Comput. Ind. Eng.* **2014**, *76*, 378–386. [CrossRef]
31. NVD Home. NVD-800-53. Available online: https://nvd.nist.gov/ (accessed on 5 February 2021).
32. Bianconi, G.; Barabási, A.L. Competition and multiscaling m evolving networks. In *The Structure and Dynamics of Networks*; Princeton University Press: Princeton, NJ, USA, 2011; pp. 361–367.
33. Ur-Rehman, A.; Gondal, I.; Kamruzzuman, J.; Jolfaei, A. Vulnerability Modelling for Hybrid IT Systems. In Proceedings of the 2019 IEEE International Conference on Industrial Technology (ICIT), Melbourne, Australia, 13–15 February 2019; pp. 1186–1191. [CrossRef]
34. Hong, J.B.; Kim, D.S. Scalable security analysis in hierarchical attack representation model using centrality measures. 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.