FLORA: Fuzzy Logic - Objective Risk Analysis for Intrusion Detection and Prevention

Alwi M Bamhdi

Umm Al-Qura University, College of Computing, Al-Qunfudah, KSA

Abstract
The widespread use of Cloud Computing, Internet of Things (IoT), and social media in the Information Communication Technology (ICT) field has resulted in continuous and unavoidable cyber-attacks on users and critical infrastructures worldwide. Traditional security measures such as firewalls and encryption systems are not effective in countering these sophisticated cyber-attacks. Therefore, Intrusion Detection and Prevention Systems (IDPS) are necessary to reduce the risk to an absolute minimum. Although IDPSs can detect various types of cyber-attacks with high accuracy, their performance is limited by a high false alarm rate. This study proposes a new technique called Fuzzy Logic - Objective Risk Analysis (FLORA) that can significantly reduce false positive alarm rates and maintain a high level of security against serious cyber-attacks. The FLORA model has a high fuzzy accuracy rate of 90.11% and can predict vulnerabilities with a high level of certainty. It also has a mechanism for monitoring and recording digital forensic evidence which can be used in legal prosecution proceedings in different jurisdictions.

Keywords:
Anomaly detection, cybersecurity, cyber-attacks, fuzzy logic, information & data security, intrusion detection & prevention, risk analysis & assessment.

1. Introduction

Nowadays security, privacy, confidentiality, and safety of computerised data and information are major concerns in ICT systems in all sectors of our lives. Moreover, corporations, governments, public utilities, financial services, healthcare institutions, and private businesses store large volumes of data collected, processed, and stored on electronic devices, and communicated through various online services that are susceptible to cyber-attacks. For example, protecting patients' public and private health information and supporting assets in a healthcare ICT facility from internal and external cyber-attacks and other dangers involve high risk. Hence, deploying IDPS can prove an invaluable tool [1] that can detect suspicious threats and prevent further damage to protected systems [2], such threats diversify into new forms [3], including ransomware.

With the increasing number of attacks and vulnerabilities and the inability of IDPS to detect innovative cyber-attacks that have no monikers or patterns yet [4], developers are encouraged to adopt new anomaly detection strategies and mechanisms to uncover abnormal patterns of behaviour by profiling them [5] [6]. Although these detection strategies are extremely powerful tools; however, a potential weakness in their mechanism can originate from the incidence of unacceptable high false alarm rates that can cause inadvertent system behaviour and unnecessarily high levels of processing. Moreover, the anomaly detection function may erroneously identify a non-intrusive legitimate normal action as an attack and falsely retort by unnecessarily exhausting system resources [6].

This paper proposes a new approach for IDPS by designing and implementing a fuzzy logic risk management assessment and analysis technique to eliminate false alarm rates to an absolute minimum by devising FLORA (Fuzzy Logic – Objective Risk Analysis for Intrusion Detection), which measures the significance and the severity of each intrusion activity in a reliable manner. FLORA effectively establishes whether an activity is a genuine cyber-attack or a non-attack behaviour pattern, as well as provides an intrusion prevention strategy.

The paper consists of the following sections: Section 2 presents related works within the scope of the FLORA detection system. Section 3 outlines the limitations in existing IDPSs that FLORA attempts to overcome. Section 4 presents the proposed FLORA framework functional architectural model. Section 5 discusses the security risk management problem and solutions to overcome some of the limitations in existing IDPSs by deploying the FLORA system. Section 6 presents the procedures and experimental results pertaining to the FLORA system calculating the vulnerabilities and countermeasures against cyber-attacks with reasonable and manageable alarm rate ranges. Section 7 covers a discussion, challenges, and recommendations arising from this research work, and lastly, Section 8 provides a conclusion of the proposed FLORA system, and provides an indication of future work.

Manuscript received May 5, 2023
Manuscript revised May 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.5.20

2. Related Works

For more than four decades IDPS has been an active field of research and development with varying degrees of success. This section succinctly presents some of the latest related works on the reduction of false alarm rates and the relevant soft computing topics in IDPS.

A two-stage classification system using Self-Organizing Map (SOM) with a neural network and a k-means algorithm to link the related alerts with the proviso to further classify the alerts into true and false alarm categories was developed by [6]. Initial results from the experiments showed that the approach reduced unwarranted and unnecessary false alarm alerts by more than fifty percent. The authors of [8] went a step further by using a datamining technique to categorise the input alarm data and fed it into the Growing Hierarchical Self-Organized Map (GHSOM) model to adjust its IDPS architectural system during an unsupervised training process. This datamining technique clusters the alarm data into a compressed form that supports network support staff in ultimately taking the final decisions regarding the true and false nature of alarms.

A post-processing filtering method was proposed by [9] to reduce false positives based on the statistical properties of intrusion alerts categorised into three classes according to varying degrees of alarm severity. Special features of the alerts corresponding to true attacks were exploited to prevent unwanted known alarms to be discarded. Their filtering method limited false positives by a maximum of seventy-five percent to achieve some sort of optimality but was computationally expensive.

The authors of [10] proposed a "New Intrusion Detection Method Based on Antibody Concentration (NIDMBAC)" that intended to reduce false alarm rates without affecting the detection rates by employing a process of clone proliferation and defining four categories of intrusions as self, non-self, antigen, and detector, using a probabilistic calculation method. The theoretical and systematic analysis of the experimental results showed that their method performed much better than other comparable traditional methods but found little use in practical IDPSs.

An intrusion detection strategy was proposed by [11] which involved a hybrid statistical approach that used optimised datamining and decision tree classification techniques. The results from the statistical analysis process were adjusted to differentiate between actual attacks of the traffic data and false positives in order to reduce the misclassification of false positives. This adjustment feature had some problems to build an effectively correct detection system.

The authors of [12] investigated and reviewed several security risk assessment methodologies to identify vulnerabilities in cyber-critical infrastructure systems. They also found other security techniques that received less attention when analysing the security threat risks as a comprehensive one-stop policy. Their analysis advocated that combining a set of soft computing techniques would be a way forward to build smart IDPSs.

FLORA took the lead and challenges a step further by amalgamating artificial intelligence, datamining optimization, reinforcement learning, knowledge-based systems, and fuzzy logic for objective risk assessment and analysis of intrusions in a superior manner to combat unwanted anomaly cyber-attacks and false positive alarms to build credible IDPSs.

3. Limitations of Current IDPS Systems

A common weakness of IDPSs is their inability to accurately detect attacks due to their lack of risk analysis and assessment methods [13] and not having access to a comprehensive list of all known and unknown attacks at any one time. On the contrary, when an IDPS wrongly identifies an intrusion as threatening, a false positive occurs. Furthermore, when an IDPS fails to genuinely identify a malicious activity, it causes a false negative. These conflicting situations are also very challenging to solve, while culprit attackers are always steps ahead of new countermeasures.

An Intrusion Prevention System (IPS) is different from IDS in one respect, whereby an IPS responds to an attack from taking place provided the attack type is known [13-17]. An automated IPS either updates its tables dynamically with new attack types or while neutralising the attack changes the content of the attack to track its evolution like a botnet would typically do, or alerts the security environment manager to contain it via applying appropriate countermeasures. Moreover, the IPS could go a step further to change the configuration settings of the security controls to extricate an attack by reconfiguring a device/component, blocking the attacker's access to system resources, quarantining the attack for further analysis, or disabling the target under attack, or changing the firewall settings to block incoming attacks [1]. Some IPSs can either eradicate an attack or substitute it with an appropriate countermeasure to render them ineffective [13], but this, if not properly designed could result being an error-prone exercise.

With high false alarm rates of anomaly detection, IPSs can inadvertently identify a legitimate, non-intrusive activity as a cyber-attack, respond inaccurately to it, and unnecessarily exhaust system resources. The main limitation of anomaly systems is the inability to detect an

attack accurately, thus unnecessarily generating high rates of false alarms. For example, a component′s valid operation behaviour may be construed as an abnormal pattern. While normal component behaviour can easily and rapidly change on the fly, when anomaly-based IDPSs go out of sync with the normal, they are susceptible to generating false positives. Such cyber-attacks may be recorded based on changes to the ″normal″ pattern behaviour rather than representing ″actual″ attacks.

3.1 Overcoming limitations of current systems

It is imperative to apply formal risk assessment techniques to analyse all detected cyber intrusion activities by measuring their exposure and impact factors and assist in validating the alert and reducing false alarms to an absolute minimum and allowing an acceptable level of ICT operation. The main problem with false alarms is their level of complexity, which is due to the complexities of dynamically reconfigurable ICT systems and poorly designed IDPSs and their deployment in such ICT ecosystems [6].

According to [17], the most optimum option is to incorporate a Collaborative-IDPS (CIDPS) with soft computing and self-managing functional components to overcome IDPS complexities. The CIDPS framework architectural model, data and information management flow to and from the CIDPS intermediate layer, traversing through various multi-agent components, such as the fuzzy risk manager function, the knowledge and multi-agent manager, and the autonomic manager are illustrated in Figure 1. The main goal of the fuzzy risk manager function is to control unnecessarily triggered false positive alarms, whereas the autonomic and knowledge manager agents respond to intrusions in the host computers and network device elements, and provide appropriate feeds to other components to ultimately offer countermeasure operations. The autonomic manager′s main function is to monitor and enable the IDPS to automatically and seamlessly detect changes in hardware and software. This form of CIDPS gelling as a multi-agent federated cooperative intrusion detection and prevention system using computational intelligent techniques overcomes many deficiencies found in non-collaborative IDPS as corroborated by [3].

3.2 CIDPS framework architecture

The autonomic trust manager in CIDPS consists of four interlinked agents. The checker agent monitors the conditions of system resources by referring to the ontology to detect anomalous activities. Should any unexpected change be detected, the ontology is automatically updated with the new information and also sent to the analyser agent that evaluates the complex behaviour pattern to comprehend the current state of the system, and set the markers to predict future abnormalities. In addition, the checker agent uses the risk analysis estimation facility to decide on the most appropriate action to be taken by consulting the Knowledge Base (KB) and verifying the correctness of the analysis before executing the final set of procedures. The checker agent then updates the KB for subsequent use. The planner agent is responsible for structuring the actions required to achieve the desired goal by producing a string of commands to invoke the threatened components and elements. The executor agent receives commands and executes the healing functions and updates the IDPS policies. This set of four interlinked agents, with the help of computational intelligence using machine learning classifiers and inference engine are supported by the following four essential properties of “self-automated” autonomic computing:

1) Configuration: provides the rules for system components to execute at runtime.
2) Healing: operates cyclically from detecting abnormalities until the problem is verifiably resolved.
3) Optimization: allows for the optimising the affected resources without impacting other resources.
4) Protection: detects non-compliant functional activities and updates security and risk policies hosted in the KB to avoid the recurrence of defects and intrusions.

3.3 FLORA operational within CPIDS

Referring to Figure 1, when an intrusion is detected, the vulnerability scanner agent inspects the impacted components within the affected system by probing deeper into the vulnerability. The vulnerability assessment data is then analysed in conjunction with network behavioural data. In real-time the scanner agent establishes a map of the attack and assesses the possible consequences of the impact upon the target system. The applicable target system centred ontology is opened where the high-level concepts such as cyber-attacks, masquerades, liabilities, and incidents are stored, and a rating is assigned to the affected asset by the risk calculator looking up the risk profiler KB, and the intrusion prevention solution gets to work by taking proactive deterring actions to contain or discard the intrusion, ensure correct system operation, and reduce overall operational overheads to a minimum. For example, intrusion prevention rules which do not apply to certain components, systems, and applications in a specific Internet Protocol (IP) address range can be immediately disabled but noted. This approach significantly reduces false positives in future incidents of a similar nature, especially in high-traffic

network environments. However, these rules may be re-enabled at any time if new intrusion data certifies that a particular component, system, or application has become susceptible to a known attack to ensure system optimization and operational efficiency.

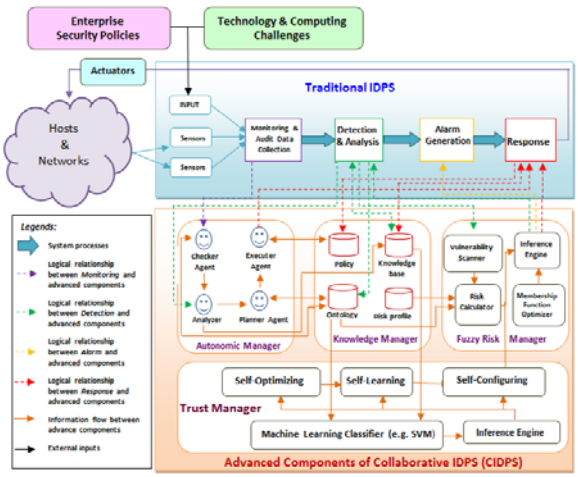

Figure 1: Boosted collaborative IDPS functional framework architecture with soft computing components

To comprehensively evaluate the false alarm reduction strategy, it is essential to quantify the actual exposed risk factor of the asset under attack and any other associated residual risk, which is what FLORA does within the CIDPS framework architecture, incorporating four critical multi-agents functionalities:

1) Fuzzy reinforcement learning manager;
2) Knowledge manager with risk profiling abilities;
3) Computational intelligence manager using AI and ML artefacts; and
4) Autonomic trust manager.

These four management functions are embedded within the trust manager to deploy, test, and evaluate CIDPS's efficiency in the host and communication networks. The risk analysis and risk assessment processes become more apparent when using fuzzy logic applications. The CIDPS functional framework risk analysis provides a comprehensive and efficient categorization of the multiple risk factors. The framework ensures that complex variables are painstakingly correlated when making risk analyses and assessments before CIDPS takes the final set of actions [17].

4. Proposed FLORA Strategy Model

The FLORA concept and principles are unique by taking IDPS one stage further in creating added value. It enhances IDPS to be more complete in its functionality and operation.

The research proposes a strategy to decrease the false alarm rates in IDPSs by implementing the FLORA model that calculates the significance and the threshold impact severity of each encountered alleged activity. FLORA can determine more accurately whether an activity or object is categorised as an intrusion attempt or normal operational behaviour misjudged by the detection procedure. FLORA model is organized into five layers, constructed from Level 0 to Level 4 as shown in Figure 2 with the following IDPS functionality attributes:

Level 0: It is responsible for journalising all the configured physical and virtual ICT computing resources, communication and transmission network devices and elements, monitoring components, IDPS sensors and actuators accessed by the Level 1 resource manager.

Level 1: It represents the resource manager's functions that manage traffic collectors and action modules, as defined by the topology and IDPS configuration tables. The traffic collectors are responsible for collecting the data and pieces of evidence of an intrusion such as network packets, log files, system call traces, etc. from all software and hardware resources and forwarding the information to Level 2.

Level 2: It is the "heart" of the fuzzy logic and objective risk analysis IDPS system. It is responsible for all the activities pertaining to attack detection performed by the FLORA Intrusion Detection Manager (IDA) shown in Figure 3. It consists of the following software modules:

- The ***monitor module*** receives input from traffic collectors in the network devices and hosts computers. It is responsible for collecting, analysing, and monitoring the data for intrusions, malicious activities, and security policy violations while providing the first line of defence by alerting against such abnormal events in real-time on monitor screens.

- The ***analyser module*** can ideally be configured by a human administrator or sophisticated automation, mimicking the administrator functions from several templates that define safety measures and IDPS high-level goals. The module uses monitored data and the internal knowledge hosted in the knowledge base as inputs to analyse the suspicious traffic detected by the monitor module and either confirms

or rejects the outcome of the generated alerts. The analyser module also performs alarm categorization and correlation of attacks or events against a set of rules that defines possible countermeasures to prevent further unnecessary alarm alerts against known attacks, temporary quarantining, and possible unknown intrusions for later analysis and processing, which might further require either updating of existing countermeasure rules or introducing new rules. The analyser model is responsible for calculating and estimating the risk of intrusions using fuzzy logic and predefined high-level criteria goals from policies, rules, standards, guidelines, and operational data, etc. Most importantly, it confirms the validity of the alerts and identifies false positive alarm alerts by measuring the risks caused by the threat. Figure 4 shows the general internal process functions of the fuzzy logic system.

- The ***planner module*** supplies the procedures and script to plan execution actions for the affected element based on the risk severity analysis observed by the analyser module. For example, the requirement to enact a change may occur when the analyser module determines that some policy violation has taken place.

- The ***controller module*** provides the mechanism to schedule for the action module to perform the necessary changes to the affected elements determined by the planner module by verifying the changes through a series of actions and simultaneously populating the knowledge base with such updated information.
- The ***action module*** executes the scheduled changes to the affected component, device, or element based on the following: norms:

  - ***Coarse-grained***, e.g., adding or removing virtual servers or to and from a web server cluster in a cloud.
  - ***Fine-grained***, e.g., modifying the IDPS configuration parameters in a network device or web server in a cloud.

The data and information collected by the traffic collectors allow the CIDPS to monitor all of the dynamic behaviour of the elements and components to be protected, and execute changes similarly in a real-time dynamic manner.

Level 3: It consists of all the safety measures like security, identity management, trust management, privacy, and, digital forensics audit as well as the essential related data and information that are kept in the knowledge database. The acquired experiences of previous actions and events, intuitive pre- and post-IDPS activities, and actual or predictive learning machine learning outputs are also stored in the knowledge database. It is the repository and source of all knowledge about every possible detail that IDPS incorporating risk analysis and assessment have access for decision-making to minimize the false positive alarms, and to maximize the IDPS operations. The Interaction with the knowledge base is through the knowledge management process, which gives a single point of access via the integrated interface layer.

Level 4: It is the integrated CIDPS interface layer for FLORA, which is the penultimate contact point between the IDPS system administrator. It is a "window" to all the system components and modules. At this level, the administrator defines the security-related strategies, policies, rules, and operational instructions through scripting or software programs. This function is largely automated with the aid of autonomic computing, data analytics, and machine learning tools but allows for human intervention as and when necessary.

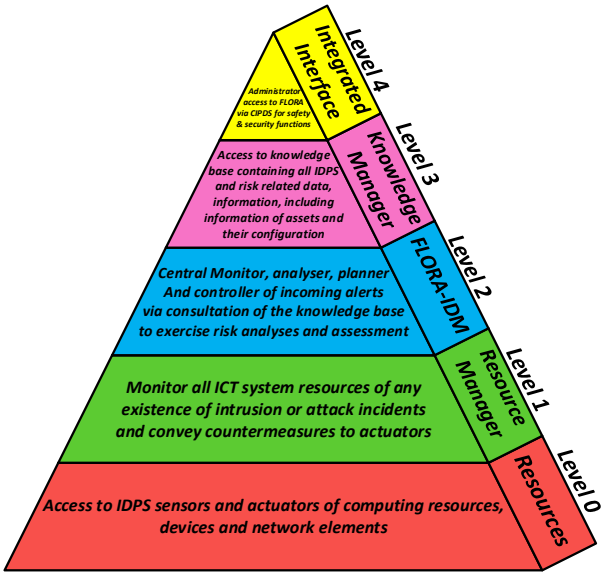

Figure 2: Proposed FLORA information and processes management strategy model

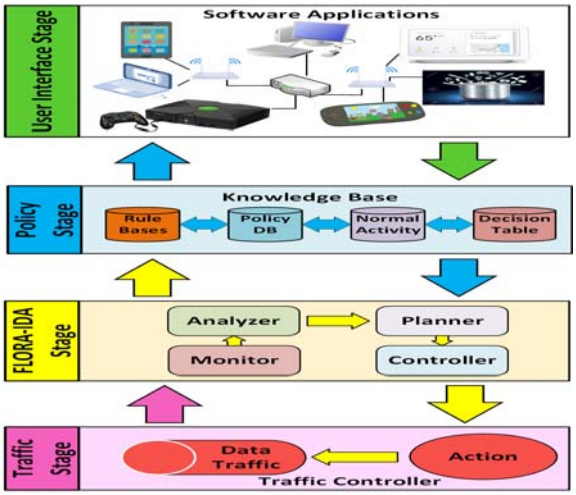

Figure 3: Fuzzy Logic - Objective risk analysis IDPS architectural system components

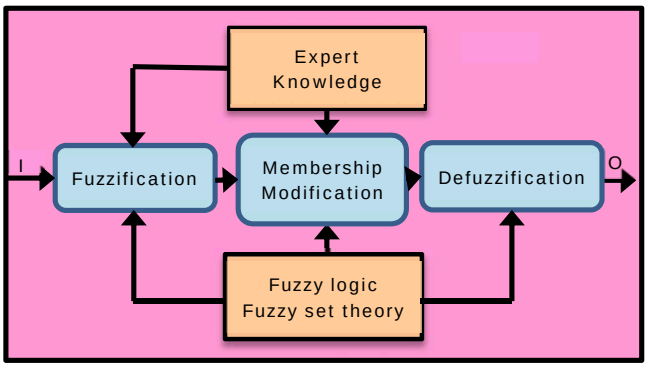

Figure 4: The input-output (result) fuzzy logic module's processing flow structure

5. Security Risk Management

Risk management entails a systematic approach to analysing and assessing security risks [18]. It requires determining important resources to be secured, determining credible threats from numerous adversaries, assessing vulnerabilities and dangers, and analysing the adequacy of countermeasures. To suitably analyse false alarms, it is necessary to quantify the risk exposure of the threatened asset and the residual risk borne by the asset [14]. This false alarm reduction tactic requires risk identification and risk assessment prescribed processes to implement a robust risk management system.

5.1 Risk Identification

Risk identification commences with the process of self-examination to correctly identify assets under attack and categorised them into prioritised groups according to their overall level of importance. In particular, this process identifies the weaknesses and threats each asset group exhibits. The risk identification process is involved in the following several activities:

Creating an inventory of assets, classifying and organising those assets into meaningful groups such as information and data assets, people, processes, software, hardware, and network elements. This inventory reflects the sensitivity and security priority weight assigned to each asset. The weights reflect the relative significance of the attributes, while attribute scores are expressed in percentage terms and ratings ranging from a low of 0.1 to a high of 1.0, reflecting the policy proclamation and the assigned judgmental-based estimation value as shown in Table 1. Calculating the asset value simply involves multiplying each score by the weight of the relevant attribute, and the scores are totalled to derive an aggregate weighted score for each asset class.

Any threat to any catalogued asset is defined as the potential to cause harm that needs to be contained or eliminated. Relative weighed values and score ratings are assigned to threats according to their severity in terms of significance, outcomes, and frequency of attacks as shown in Table 2, which is in some ways similar to Table 1. It is impossible to accurately know everything about every threat and its impact on a novel or newly injected cloned attack on an initial encounter, but the frequency of such attacks over a period of type will evolve to provide more accurate detection. This function factors uncertainty to be added into the evaluation of the exposed risk for each threat as would be the case in efficiently detecting malicious malware and inadvertent human operating errors, but lacks the ability to detect deliberate acts of espionage that can take different disguised forms without realizing its intent. The uncertainty percentage in the FLORA-modelled system is estimated by the judgment of experienced security experts in formulating the risk analysis and assessment policy.

Once vulnerable assets are ascribed to specific threats upon identification, all that needs to be added are the necessary controls to obviate attacks as a safety measure by assigning an estimated percentage value to mitigate that risk. This likelihood of an attack is the overall rating of the probability that a specific vulnerability on the next encounter will be exploited as perceived and shown in Table 3. As an example, the likelihood of a system being physically accessed within an indoor isolated secured environment would be rated 0.1, while the likelihood of receiving malware in an e-mail during a week would be rated 1.0.

Defining the magnitudes of a threat attacking vulnerable assets are evaluated on five levels ranging from insignificant to catastrophic as shown in Table 4. For instance, the magnitude of a web server being attacked by system-aware

ransomware would be rated 0.1, while the magnitude of a network being attacked by a DDoS would be rated 1.0.

Table 1: Score ratings for information data asset attributes

ASSET SENSITIVITY	DATA CONFIDENTIALITY	VIABILITY IMPACT	SCORE RATING
Critical	Classified	Critical	1.0 to 0.91
Very High	Confidential	Very High	0.90 to 0.71
High	Private	High	0.70 to 0.41
Medium	Public	Medium	0.40 to 0.21
Low	Open	Low	0.20 to 0.10

Table 2: Score ratings for security threat attributes

THREAT SIGNIFICANCE	THREAT OUTCOMES	ATTACK FREQUENCY	SCORE RATING
Critical	Critical	Almost	1.0 to 0.91
Very High	Very High	Likely	0.90 to 0.71
High	High	Possible	0.70 to 0.41
Medium	Medium	Unlikely	0.40 to 0.21
Low	Low	Rare	0.20 to 0.10

Table 3: Possible levels for information and data asset security threats

LIKELIHOOD	LEVEL	DESCRIPTION
1.0 to 0.91	Almost certainly	Is expected to occur in most cases
0.90 to 0.71	Likely	This will probably occur in most cases
0.70 to 0.41	Possible	This may occur at some point in time
0.40 to 0.21	Unlikely	This may occur at some point in time
0.20 to 0.10	Rare	This may occur only in exceptional cases

Table 4: Magnitudes levels for information and data asset threats

MAGNITUDES	LEVEL	DESCRIPTION
1.0 to 0.91	Cataclysmic	Fatality, sabotage or natural disasters
0.90 to 0.71	Major	Sabotage, extensive damages, or major asset losses.
0.70 to 0.41	Moderate	Extensive damage or high pecuniary losses.
0.40 to 0.21	Minor	Remediable or medium pecuniary losses.
0.20 to 0.10	Insignificant	No damages or low pecuniary losses.

5.2 Risk Assessment

Risk assessment evaluates the level of proportional risk of each asset's threat and vulnerability [19] and FLORA assigns risk ratings to quantify the risk exposure of the asset and its residual risk expressed by that asset, which enables the IDPS to measure the concomitant risk. The two new types of risk are "leftover risk (LR)" and "inherent risk (IR)". Leftover risk is created by the asset to itself as a factor of its vulnerabilities and controls, and its composite value to the enterprise. It is the risk persisting after efforts have been exhausted to reduce the IR to its present state without any further actions at mitigation and no controlling measures to reduce the risk from the initial levels of encounter to calculable levels acceptable to the enterprise system. The difference between LR and IR is an important distinction.

The leftover risk is calculated for each asset based on its sensitivity, the confidentiality of the data it holds, its impact on the business – e.g. availability or profitability, and its likelihood of vulnerabilities defined by Equation (1), where La is the leftover risk of ath asset, ρ the probability of vulnerability occurrence, Ea effective impact value of ath asset, and ϕ the percentage of the current risk control.

$$L_a = \rho * E_a - \varphi \quad (1)$$

The inherent risk factor is calculated when a threatened asset of significance with recurring frequency of cyber-attack occurs as defined by Equation (2), where IT is the inherent risk of ath asset, ET the effective impact value of Tth threat, wT the weighted value of Tth threat, and σ the uncertainty of current vulnerability.

$$I_T = E_T * w_T - \sigma \quad (2)$$

5.3 Risk control countermeasure

When the leftover and the inherent risks are blended using fuzzy logic, the IDPS is in a position to decide which countermeasure to apply to an identified cyber-attack. There are three control countermeasures that are defined to apply to the attack:

- Avoidance (Av). Apply a countermeasure to prevent or reduce the magnitude of the attack. This countermeasure is implemented by applying a prevention mechanism, such as terminating the network connection or user session that is being attacked, or by either preventing the offending attacker from gaining access from a user's account or simply blocking access to the targeted service, application, host or other associated resources.
- Transference (Tr). Shift the risk to other areas or outside entities. One example of transferring the risk is using a botnet-related honeypot to track deeply into attacks for further investigation. (Since this is outside the scope of this reported research, it would be most useful when

designing and implementing a digital forensics investigation module to catch the culprit for prosecution.)

- Acceptance (Ac). Comprehending the magnitude and acknowledging the risk without any attempt to mitigate the risk because of its insignificance.

6. Analysis & deployment of FLORA model

The FLORA model consists of fuzzy logic semantic variables and expressions for input and output risk parameters used in the experiment. Five Membership Functions (MF/MFs) are used for each input variable as low, medium, high, very high, and critical, and three MFs for each output countermeasure variable as Avoidance, Transference, and Acceptance. LR conveyed by an asset and IR generated by an attack are the vital two input parameters that result after calculation as the countermeasure output parameter. Table 5 shows the characteristics of the input and output variables and the min-max range of values and Table 6 shows the score rating ranges of LR and IR divided into five classes of fuzzy sets from Critical to Low with in-between Very High, High, and Medium.

6.1 Membership I/O functions for FLORA model

According to [6], the type of MFs for fuzzification is mainly dependent upon the relevant event for the best addressing of the problem. In the fuzzy logic model, the ″Trapezoidal-shaped Gaussian MF″ is adopted to express the fuzzy sets for the input and output variables. The input variables are partitioned according to the experimental parameter ranges. The degree of belonging of the values of the input variables to any selected class is called the degree of membership as shown in Figure 5 for the leftover risk and inherent risks.

The output MF is the countermeasure variable characterised in the fuzzy sets into classes as shown in Figure 6 for qualitative risk:

- *Avoidance* signifies a high-risk exposure requiring some action to purge that threat.
- *Acceptance* signifies low-risk exposure requiring no action for that threat.

Transference signifies expert judgemental intervention is needed to take remedial action.

The trapezoidal area for both Figures 5 and Figure 6 is a function of a vector, x, and four scalar parameters a, b, c, and d, as defined by Equation (3):

$$f(x;a,b,c,d) = max\left(min\left(\frac{x-a}{b-a}, 1, \frac{d-x}{d-c}\right), 0\right) \quad (3)$$

Table 5: Fuzzy linguistic definitions and ranges of variables for each parameter

INPUTS		
PARAMETERS	LINGUISTIC VARIABLES	RANGE
Leftover risk (LR)	Low, Medium, High, Very High, Critical	0-100
Inherent risk (IR)		0-100
OUTPUTS		
Countermeasure	Avoidance, Transference, Acceptance	0-100

Table 6: Score ratings for fuzzy logic leftover and inherent risks

LEFTOVER RISK (LR)	INHERENT RISK (IR)	SCORE RATING
Critical	Critical	91 to 100
Very High	Very High	71 to 90
High	High	41 to 70
Medium	Medium	11 to 40
Low	Low	0 to 10

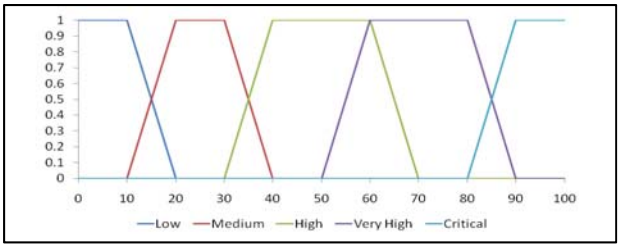

Figure 5: Inputs membership functions for leftover and inherent risks

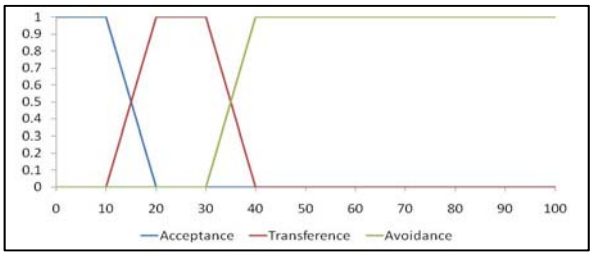

Figure 6: Output membership functions for qualitative risk

Scalar parameters a and d locate the "feet" and b and $c$locate the "shoulders" of the trapezoid. It is stated by [1] that expert knowledge is required to characterise the inputs and outputs and to link them by a set of "inference rules" using "if-then" statements to obtain optimum outcomes.

According to this principle, from the number of fuzzy sets of inputs, there are twenty-five possible combinations of inference rules in the FLORA system. The fuzzy output set indicates the applicable countermeasure that should be applied to a cyber-attack.

6.2 Fuzzy rule sets

The type of response of the IDPS is based on the calculated leftover and inherent risk factors. For example, in the case of leftover and inherent risk determined to be very high, the appropriate action is to apply safeguards as preventative measures to either eliminate or reduce the magnitudes of the cyber-attack. In the case of low risk, the appropriate action is to understand the outcome as harmless having no consequences, and accept the risk as shown in Table 7. This method and analysis reduce the false alarm rate in the anomaly detection module and make the system more robust and reliable.

It can also be observed from the matrix in Table 8 that the upper and lower triangular parts are equivalent leading to the same results. For instance, the one intersection between LR-VERY HIGH with IR-HIGH leads to Transference, and the other intersection between IR-VERY HIGH with LR-HIGH leads to Transference, both intersection actions occurring at the same time. A set of 15 fuzzy rules for FLORA was constructed based on the characteristics of the input and output variables quantities shown in Table 6 and from the matrix of the actual qualitative risk analysis derived from Table 7.

Table 7: Qualitative risk matrix derived from quantitative LR & IR data

TYPES OF RISKS		INHERENT RISK (IR)				
		CRITICAL	VERY HIGH	HIGH	MEDIUM	LOW
LEFTOVER RISK (LR)	*CRITICAL*	Avoidance	Avoidance	Avoidance	Transference	Transference
	VERY HIGH	Avoidance	Avoidance	Transference	Transference	Transference
	HIGH	Avoidance	Transference	Transference	Transference	Transference
	MEDIUM	Transference	Transference	Transference	Transference	Acceptance
	LOW	Transference	Transference	Transference	Acceptance	Acceptance

The program execution logic of the qqualitative risk analysis matrix derived from quantitative LR & IR data to formulate countermeasures is as:

Rule # 1: if (LR is Critical) and (IR is Critical) then (Avoidance)

Rule # 2: if (LR is Critical) and (IR Very High) or (IR Critical) and (LR Very High) then (Avoidance)

Rule # 3: if (LR is Critical) and (IR is High) or (IR is Critical) and (LR is High) then (Avoidance)

Rule # 4: if (LR is Critical) and (IR is Medium) or (IR is Critical) and (LR is Medium) then (Transference)

Rule # 5: if (LR is Critical) and (IR is Low) or (IR is Critical) and (LR is Low) then (Transference)

Rule # 6: if (LR is Very High) and (IR is Very High) or (IR is Very High) and (LR is Very High) then (Avoidance)

Rule # 7: if (LR is Very High) and (IR is High) or (IR is Very High) and (LR is High) then (Transference)

Rule # 8: if (LR is Very High) and (IR is Medium) or (IR is Very High) and (LR is Medium) then (Transference)

Rule # 9: if (LR is Very High) and (IR is Low) or (LR is Very High) and (IR is Low) then (Transference)

Rule # 10: if (LR is High) and (IR is High) then (Transference)

Rule # 11: if (LR is High) and (IR is Medium) or (IR is High) and (LR is Medium) then (Transference)

Rule # 12: if (LR is High) and (IR is Low) or (IR is High) and (LR is Low) then (Transference)

Rule # 13: if (LR is Medium) and (IR is Medium) then (Transference)

Rule # 14: if (LR is Medium) and (IR is Low) or (IR is Medium) and (LR is Low) then (Acceptance)

Rule # 15: if (LR is Low) and (ER is Low) or (IR is Low) and (LR is Low) then (Acceptance)

6.3 Fuzzification and Defuzzification

Fuzzification is basically the process of transforming a crisp set of input values accurately into aggregated semantic variable values into either a fuzzy set or a fuzzy set to a fuzzier set. Defuzzification is the process of obtaining a single value from the output of the aggregated fuzzy set used to transfer fuzzy inference results into a crisp output based on a decision-making algorithm that selects the best crisp value based on a fuzzy set. In short: defuzzification is the conversion of an input fuzzy logic aggregated quantity to a precise value, and fuzzification is the conversion of an input value to a fuzzy logic quantity [6]. FLORA using these processes, by considering the union of the output of each rule, the resultant MFs are developed whereby the overlapping areas of the fuzzy logic output set are counted as one providing more and better results. From one of many experiments, Figure 7 illustrates an example of the appropriate ascent between the input parameter changes and the countermeasure values, which are predicted by FLORA.

The close ascent of the countermeasure values shows that the FLORA model can more accurately predict countermeasure values of cyber-attacks. The FLORA model gives a very promising solution to predict countermeasure values in a specific range of parameters compared to similar work reported in [11].

Additionally, after performing the defuzzification, the correlation matrix is computed as shown in Table 8. Standard statistical analysis is used to complement the fuzzy logic system to better determine the active attributes of each class since some attributes in semantic terms can be expressed to discover more production rules for better accuracy. These rules describing the classes allow FLORA to perform speedily to counteract the cyber-attack threats much more effectively and efficiently.

After classification has been performed through FLORA, each class of the patterns acquired is inspected. There are several methods of inspection. The easiest method is to use the statistical analysis of each class. Using central tendency and dispersion statistical measures, one can form several rules that govern each class attribute. There are several ways to measure the variability of the data. In this research, the concept and the technique of "measures of dispersion" using "standard deviation" were used, since it provides an average distance for each value from the mean, giving a range difference between the highest and lowest data values spectrum [15]. Metaphorically, the range is computed as $xmax - xmin$, although this is very similar to the formula for midrange. Although this is not an altogether reliable measure of dispersion, since it uses only two values from the dataset. The extreme values on either side of the spectrum can distort the range to be very large while most of the values may be very close to each other. For example, the range of this set of data 1, 1, 2, 4, 7, is therefore, 7-1=6, where 1 is the lowest value and 7 is the highest value. The statistical spectrum range is defined as the same as its mathematical construct. Thus, instead of being a single number, it is the interval over the spectrum of the data which occurs in the range of $\{xmin, xmax\}$ or $xmin$ to $xmax$. Thus, in the example above, the range is 1 to 7 or $\{1, 7\}$. This strategy has been used in FLORA. An example of this scheme consisting of thirteen rules in pseudo-programming algorithmic logic for 100 samples, and ten inputs (i.e., 5 features a piece for LR and 5 IR respectively) to satisfy one of the main conditions of accuracy that satisfy 100% of sampled cases for countermeasures as:

Rule # 1: if IR Very High in [86.173, 87.212] and LR Critical in [91.123, 98.704] and IR High in [41.3, 67.624] then Transference.

Rule # 2: if LR Low in [7.955, 8.611] and LR Critical in [98.704, 99.915] and IR Very High in [71.414, 87.212] and IR High in [41.3, 67.624] then Avoidance.

Rule # 3: if LR High in [47.424, 58.355] and LR Low in [8.611, 9.186] and LR Critical in [98.704, 99.915] and IR Very High in [71.414, 87.212] and IR High in [41.3, 67.624] then Acceptance.

Rule # 4: if LR High in [58.355, 69.285] and LR Low in [8.611, 9.186] and LR Critical in [98.704, 99.915] and IR Very High in [71.414, 87.212] and IR High in [41.3, 67.624] then Transference.

Rule # 5: if LR Low in [6.778, 9.762] and IR Very High in [87.212, 89.855] and IR High in [41.3, 67.624] then Acceptance.

Rule # 6: if IR Low in [1.448, 7.651] and LR Low in [0.033, 6.778] and IR Very High in [87.212, 89.855] and IR High in [41.3, 67.624] then Avoidance.

Rule # 7: if LR High in [52.354, 58.22] and IR Low in [7.651, 9.179] and LR Low in [0.033, 6.778] and IR Very High in [87.212, 89.855] and IR High in [41.3, 67.624] then Avoidance.

Rule # 8: if LR High in [58.22, 60.819] and IR Low in [7.651, 9.179] and LR Low in [0.033, 6.778] and IR Very High in [87.212, 89.855] and IR High in [41.3, 67.624] then Acceptance.

Rule # 9: if LR Low in [0.861, 9.198] and IR Critical in [91.718, 98.217] and IR High in [67.624, 69.901] then Transference.

Rule # 10: if LR Very High in [76.721, 79.65] and LR Low in [9.198, 9.581] and IR Critical in [91.718, 98.217] and IR High in [67.624, 69.901] then Transference.

Rule # 11: if LR Very High in [79.65, 82.58] and LR Low in [9.198, 9.581] and IR Critical in [91.718, 98.217] and IR High in [67.624, 69.901] then Acceptance.

Rule # 12: if LR Low in [3.089, 6.221] and IR Critical in [98.217, 98.653] and IR High in [67.624, 69.901] then Avoidance.

Rule # 13: if LR Low in [6.221, 9.353] and IR Critical in [98.217, 98.653] and IR High in [67.624, 69.901] then Transference.

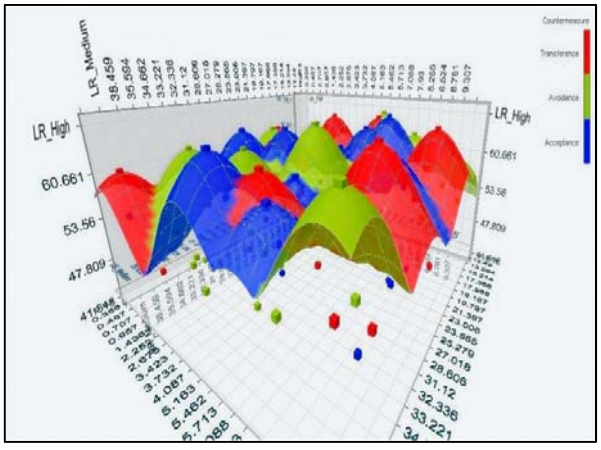

Figure 7: Countermeasure value in relation to change of leftover risk and inherent risk factors

Table 8: Correlation matrix after performing the defuzzification phase

VARIABLES	LR_Low	LR_Medium	LR_High	LR_Very High	LR_Critical	IR_Low	IR_Medium	IR_High	IR_Very High	IR_Critical
LR_Low	**1.000**	0.040	0.067	0.205	0.006	0.208	-0.025	-0.038	-0.049	-0.003
LR_Medium	0.040	**1.000**	-0.068	0.094	0.025	-0.088	-0.102	-0.094	-0.023	0.084
LR_High	0.067	-0.068	**1.000**	-0.082	0.114	0.172	0.027	0.048	0.016	0.073
LR_Very High	0.205	0.094	-0.082	**1.000**	0.054	0.092	0.006	-0.064	-0.153	0.094
LR_Critical	0.006	0.025	0.114	0.054	**1.000**	-0.055	0.054	0.194	0.067	0.098
IR_Low	0.208	-0.088	0.172	0.092	-0.055	**1.000**	-0.028	-0.019	0.075	-0.201
IR_Medium	-0.025	-0.102	0.027	0.006	0.054	-0.028	**1.000**	0.152	-0.124	-0.117
IR_High	-0.038	-0.094	0.048	-0.064	0.194	-0.019	0.152	**1.000**	0.007	-0.029
IR_Very High	-0.049	-0.023	0.016	-0.153	0.067	0.075	-0.124	0.007	**1.000**	-0.070
IR_Critical	-0.003	0.084	0.073	0.094	0.098	-0.201	-0.117	-0.029	-0.070	**1.000**

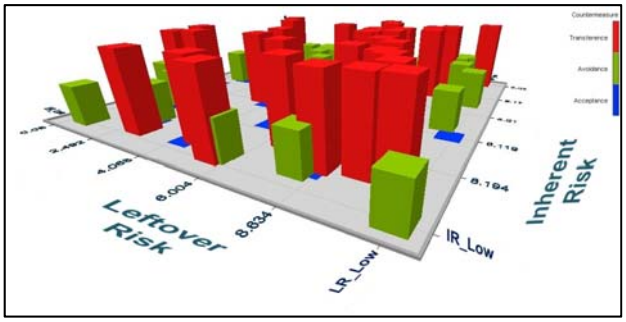

Figure 8: Final analysis of the resulting decision of the FLORA system depicted in a surface form

6.4 Results of the Fuzzy Logic Model

After constructing the fuzzy logic programmable rules, five experimental tests were performed in separate experiments, while the proposed fuzzy logic model was used to identify the abnormality of the system under the same conditions as shown in Table 9, which is to investigate the fuzzy logic model accuracy and error factors. The error factor is calculated to measure the gap between the predicted and measured values. The individual error percentage is calculated by taking the absolute difference between the predicted and measured values and dividing it by the measured value as given in Equation (4):

$$e_i = \left(\frac{|A_m - A_p|}{A_m}\right) * 100\% \qquad (4)$$

Where e_i is the individual error, *Am* is the measured value and *Ap* is the predicted value.

Meanwhile, accuracy is calculated to measure the closeness of the predicted value to the measured value. The model accuracy is the average of individual accuracies as shown in equation (5), where *a* is the model accuracy and *N* is the total number of datasets tested using this equation:

$$a = \frac{1}{N}\sum_{i=1}^{N}\left(1 - \frac{|A_m - A_p|}{A_m}\right) * 100\% \qquad (5)$$

Table 9: Confusion matrix for the estimated samples

From \ To	Avoidance	Transference	Acceptance	Total	% Correct
Avoidance	10	16	8	34	29.41%
Transference	0	32	1	33	96.97%
Acceptance	0	11	22	33	66.67%
Total	10	59	31	100	---

The accuracy for FLORA is determined after the error of the dataset result is calculated. The experimental outcomes of the countermeasure results and the fuzzy model predicted values for FLORA are shown in Table 10.

The highest percentage of error in the fuzzy model prediction is 0.32%. The low level of errors shows that the fuzzy predicted countermeasure results are very close to the actual experimental countermeasure values. Table 10 also shows that the fuzzy model accuracy is 90.11%. The value of the accuracy shows that the proposed model can predict the vulnerability of a system, and it can also be observed from the associated graph's trend lines.

Table 10: Accuracy and error of the fuzzy program logic FLORA model prediction

RISK PARAMETERS (INPUTS)		COUNTER MEASURE PARAMETER (OUTPUT)			STATISTICS				
Leftover Risk	Inherent Risk	1st epoch	2nd epoch	3rd epoch	Average	Standard Deviation (σ)	Measured	Error %	Proposed Fuzzy Model
90.00	70.00	90.00	100.00	70.00	86.67	15.28	76.00	0.18	76.80
10.00	40.00	80.00	90.00	70.00	80.00	10.00	68.00	0.18	78.30
70.00	50.00	67.00	70.00	100.00	79.00	18.25	98.00	0.32	99.07
98.00	98.00	90.00	100.00	69.00	86.33	15.82	95.40	0.06	96.80
67.00	43.00	80.00	79.00	98.00	85.67	10.69	99.00	0.19	99.60
							The average accuracy of the fuzzy method = 90.11%		

7. Discussion, Challenges & Recommendations

The development of the FLORA system, with an object risk analysis and assessment technique for online IDPS, was performed by modifying the FLORA′s controller module′s algorithm and combining it with an Object Risk analysis management mechanism that can significantly reduce false positive alarm rates during intrusion detection activities to a minimum, providing a high level of countermeasures against various types of cyber-attacks. The highest percentage of error in the FLORA model prediction is 0.32%, showing that the fuzzy logic mechanism predicting countermeasure results is very close to the actual experimental values and achieves a high fuzzy accuracy rate of 90.11%. It demonstrates that it can successfully predict vulnerabilities with a very high level of confidence. By far, it has superiority over comparable experimental IDPS specialising in DDoS alone that have a much poorer false positive alarm rate [17]. This is attributed to the basic

FLORA controller-IDPS without modification of the fuzzy logic algorithm but combining it with innovative risk management analysis and assessment mechanisms.

The main objective was to reduce the complexity and dimensionality of the selected feature set. In designing and developing FLORA, discretization, feature selection, and accuracy calculation were performed simultaneously which resulted in a highly prepared detection mechanism that also reduced the computational processing cost. It was, however, observed that for the detection of continuous attacks by FLORA's controller, if the same parameters are applied to all attributes, classification accuracy varied widely. The combinations of FLORA's controller with objective risk analysis for different attributes in different clusters yielded the best results regarding classification accuracy.

Although statistical analysis was used to determine the active attributes of each class, results indicate more work is required to try different statistical methods. In addition, while some attributes in semantic terms are expressed through the use of fuzzy logic and "patterns", more intensive work is also required by deploying advanced machine learning and optimization techniques to dynamically discover and derive production rules through a smarter ontology for much better and smarter accuracy. Also, deep neuro-fuzzy systems show promising application trends [21], which can further enhance the FLORA model and accrue substantial benefits. The combination of these techniques is currently a work in progress.

When one takes into account assessing IoT and Cloud Computing risks in open system environments and attack detection and prevention policies, then enterprises should deploy more robust sophisticated automated risk identification and assessment methodologies and procedures from the life-cycle starting at system requirements capture, design, development, testing, verification and validation phases, by applying the fundamental principle of the least privilege, coupled with firewalls, advanced detection tools, and other security technologies in order to identify any anomalous untoward behaviour that results from their compromises, and in the best case scenario, proactively and dynamically rectify the problem on demand. This is a huge challenge waiting to be performed by new research and development.

Using data analytics with advanced datamining, predictive artificial intelligence, machine learning, and optimization techniques in conjunction with autonomic computing techniques and practical defensive mechanisms would further enhance reducing or eliminating risks and false alarm rates to their absolute minimum in the next generation of IDPSs.

Since it is difficult to collect evidence to support IoT and Cloud Computing cybercrime cases without deductive knowledge, and even more challenging to connect various pieces of evidence into a chain of custody, it is critically important to consider the classification of the crime, the methods of collecting evidence, and all relevant laws and regulations in an extremely consistent manner through the build-up of a semantically rich ontology and the use of blockchain technology for authenticity [20]. The systematic classification of data, using advanced data mining techniques to categorize data and information about various assets [21] for aiding more accurate analysis should be the norm. Such classifications should also initially assist analysts to predict the target class for each new case in the data and information flow to enrich the ontology. Cloud computing platforms supporting IoT-related cybercrimes can be categorized into three basic classes namely IoT as a target, IoT as a tool, and IoT as an eyewitness. This alone signals the need for a comprehensive semantic ontology in its sphere of operation.

There is also tremendous scope in advancing new research in the IDPS field, by drawing in advanced digital forensic computing and cybercrime investigation methodologies and techniques to complement it. Digital forensics would be a significant advantage as an add-on, to not only minimise various types of security risk through proactive preventative methods but also hold the culprit responsible to be prosecuted. These challenges are open to new ideas and areas of research and development.

8. Conclusion

As cyber-attacks become more complex and intractable, the prerequisite to deliver efficient and effectual intrusion detection and prevention solutions intensifies. Many current IDPSs have limitations and drawbacks such as centralised analysis of false alarms. The deficiency of centralised IDPSs is best eliminated by designing and deploying federated and distributed collaborative self-governing agents based on autonomic computing coupled with artificial intelligence techniques. In this research, a FLORA solution was proposed that is more effective than many comparable IDPSs. FLORA provides an intelligent IDPS, which minimized the number of false-positive alarms, owing to the ingenious use of risk assessment and analysis management functions, using a combination of collaborative and autonomic system components with fuzzy logic. It also provides craftier prevention by focusing on attacks ascertained by false-positive alarms. The main objective was to establish how to make FLORA-based

IDPS much smarter from different points of view and with the aid of an assortment of technologies and techniques.

Future research and development initiatives are required to extend the concepts of FLORA by implementing the use of an incessantly evolving ICT security ontology encompassing intrusion detection and prevention, and digital forensics information cradle, built upon the life-cycle components of risk management analysis (assets, threats, vulnerabilities, and countermeasures), and forward advance predicting intrusions techniques from continuously scanning of an up-to-date knowledge database. There is also a huge challenging opportunity as future work to implement the fuzzy logic risk management architectural model using the latest artificial intelligence and autonomic computing advance techniques, to enhance intelligent IDPSs further that allows for fully automated self-management computing with dynamic adaptivity and awareness comprising of self-configuration (in real-time), self-healing (error correcting), self-optimization (optimal functioning of automated resource control), self-protection (proactive detection and preventive protection from attacks). It is perceived to dramatically improve detection and prevention performance, as well as reduce the necessity to deploy manual reverse engineering to categorise alarms, which itself is largely an error-prone exercise. Autonomic computing could also enable the development of a semantically rich ontology-driven, self-updating knowledge database of newly detected attacks, thus, aiming at further reducing false alarm rates, while providing a sophisticated platform for deploying countermeasures in preventing such attacks. It is also envisaged that deploying data analytics with advanced predictive artificial intelligence and optimization techniques in the next generation of IDPSs would accrue substantial benefits. My research is currently investigating how to accommodate a more advanced form of digital forensic computing capability from the cyber security attacks discovered by FLORA to aid law enforcement agencies.

Acknowledgments

The author sincerely wishes to thank Dr. Qais Qassim and Professor Ahmed Patel for allowing the use of data and technical content from their previous research initiatives and published works.

Declarations

Compliance with ethical standards was followed according to the journal's ethical guidelines. There is no conflict of interest presented in this research manuscript. All relevant data supporting the findings of this research study has been referenced and included in this manuscript. Neither human nor animal was used in the experiments. The author received no financial support for the research work and its publication.

References

[1] Patel, A., Qassim, Q., Wills, C. A survey of intrusion detection and prevention systems, Information Management & Computer Security. 18:277-290. (2010).

[2] Gupta, B. B., Srinivasagopalan, S. Handbook of Research on Intrusion Detection Systems. IGI Global. ISBN10: 1799822427. (2020).

[3] Shamshirband, S., Anuar, N. B., Kiah, M. L. M., Patel, A. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Journal of Engineering Applications of Artificial Intelligence. 26:2105-2127. (2013).

[4] Huebscher, M. C., McCann, J. A. A survey of autonomic computing—degrees, models, and applications. ACM Computing Surveys (CSUR). 40(3):1-28. (2008).

[5] Amin, S. O., Siddiqui, M. S., Hong, C. S., Lee, S. RIDES: Robust intrusion detection system for IP-based ubiquitous sensor networks. Sensors. 9:3447-3468. (2009).

[6] Patel, A., Taghavi, M., Bakhtiyari, K., Júnior, J. C. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications. 36:25–41. (2013).

[7] Tjhai, G. C., Furnell, S. M., Papadaki, M., Clarke, N. L. A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm. Computers & Security. 29:712-723. (2010).

[8] Mansour, N., Chehab, M., Faour, A. Filtering intrusion detection alarms. Cluster Computer. 13:19-29. (2010).

[9] Spathoulas, G. P., Katsikas, S. Reducing false positives in intrusion detection systems. Computers & Security. 29:35-44. (2010).

[10] Zeng J., Li, T., Li, G., Li, H. A New Intrusion Detection Method Based on Antibody Concentration. In: D. S. Huang, K. H. Jo, H. H. Lee, H. J. Kang, V. Bevilacqua (Eds.) Emerging Intelligent Computing Technology and Applications. With Aspects of Artificial Intelligence. Springer Berlin Heidelberg, 5755:500-509. (2009).

[11] Anuar N. B., Papadaki, M., Furnell, S., Clarke, N. Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). Security and Communication Networks. 6:1087-1116. (2013).

[12] Qassim, Q.S., Jamil, N., Daud, M., Patel, A., Ja'affar, N. A review of security assessment methodologies in industrial control systems. Information and Computer Security. 27(1): 47-61. (2019).

[13] Bringas, P., Penya, Y. Next-Generation Misuse and Anomaly Prevention System. In: J. Filipe, J. Cordeiro (Eds.) Enterprise Information Systems. Springer Berlin Heidelberg. 19:117-129. (2009).

[14] Qassim, Q., Patel, A. and Mohd-Zin, A. Strategy to Reduce False Alarms in Intrusion Detection and Prevention Systems. International Arab Journal of Information Technology (IAJIT), 11(5):500-506. (2014).

[15] Zhou, Y. P., Fang, J. A. Intrusion detection model based on hierarchical fuzzy inference system. In: Information and Computing Science, 2009. ICIC'09. Second International Conference on, IEEE. pp. 144-147. (2009).

[16] Chen, P. Y., Kataria, G., Krishnan, R. Correlated failures, diversification, and information security risk management. MIS Quarterly. 35:397-422. (2011).
[17] Patel, A., Alhussian, H., Pedersen, J.M., Bounabat, B., Júnior, J.C., Katsikas, S. A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems. Computer Security. 64:92–109. (2016).
[18] Bajpai, S., Sachdeva, A., Gupta, J. P. Security risk assessment: Applying the concepts of fuzzy logic, Journal of Hazardous Materials, 173: 258-264. (2010).
[19] Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments. NIST special publication 800-30, Revision 1. (2012).
[20] Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E. and Pavué, C. Blockchain solutions for forensic evidence preservation in IoT environments. In 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France. IEEE. pp. 110-114. (2019).
[21] Talpur, N., Abdulkadir S. J., Alhussian, H., et al. Deep Neuro-Fuzzy System application trends, challenges, and future perspectives: a systematic survey. Artificial Intelligence Revew. 13:1-49. (2022).

Alwi M Bamhdi, is the Associate Professor in the Department of Computer Sciences, College of computing (Al Qunfudhah), Umm Al-Qura University, Saudi Arabia. He received his MSc (2010) and PhD (2014) in Computer Science respectively from Heriot-Watt University, Scotland, UK. His research interests include Computer Networking, Mobile Ad Hoc Networks, Wireless Sensor Networks, Internet of Things, Cloud Computing, Information & Cyber Security, Digital Investigations & Forensics, Blockchain Technology, Computer Vision, Software Engineering and Performance Evaluation. He has published many papers in his specialized areas of MANETS as well as in other areas of Computer Science and Information Technology within the scope of his research and teaching activities.