www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 720-723

e-ISSN : 2583-1062

Impact Factor : 5.725

A COMPARATIVE STUDY OF COMPUTATIONAL INTELLIGENCE IN COMPUTERSECURITY AND FORENSICS

Subbaiah. S[1], Ranjith Surya. K[2]

[1]Guide, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.

[2]Student, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.

ABSTRACT

The importance of protecting these systems from attack cannot be understated given the increased reliance that businesses and governmental organisations have on their computer networks. Computer security and forensics are essential for defending systems against intrusion or unauthorised access that could have unfavourable effects. They can also help to guarantee that a network infrastructure will endure and remain cohesive. A system that uses high-quality approaches will be more safeguarded and offer hints that could be helpful in any criminal inquiry. Artificial neural networks, fuzzy logic, and evolutionary computing are some of the methods that can be utilised to address computer security and forensics-related problems. The utilisation of neural networks, fuzzy logic, and evolutionary computation is the main focus of this paper.

1. INTRODUCTION

Since it was first developed, artificial intelligence (AI) has served as a lively topic of discussion for authors and scholars, who have written numerous books, essays, and papers on the subject. AI is remarkable for offering intelligent systems that model the nature of life, human beings, etc., in order to achieve better simulations, even if it shares similarities with many other systems. Techniques such as neural networks, fuzzy logic, and evolutionary computation are all part of computational intelligence (CI). Other techniques that make advantage of swarm intelligence, artificial immune systems, etc. are also included. However, as computer networks are used more and more frequently, computer security has emerged as a critical issue in contemporary systems. A single breach of a network system can do a lot of harm to a company. Because of this, a Computer Systems must now be protected with security attack and its unfavourable effects. It is identified that there are four primary attack kinds that can be detrimental within the system:Denial-of-service (DoS) attack: This kind prevents users from accessing a resource, which renders the network inoperable. It accomplishes this by clogging or overtaxing the network. Remote to Local (R2L): This attack occurs when an attacker who does not have access to a resource removes a file or changes data by gaining access to the resource. U2R (User to Root) attack: Here, the attacker first compromises the system as a regular user before attempting to gain root access.Scanning or Probing: By scanning a certain resource, the attacker searches for any vulnerabilities or points of attack susceptibility. A frequent application of this technology is data mining. Other frequent attack techniques that cause damage to network systems include eavesdropping, data modification, identity spoofing, password-based attacks, man-in-the-middle attacks, comprised-key attacks, sniffer attacks, and application layer attacks. However, due to the widespread use of computers and computer networks in recent years, the field of computer and intrusion forensics has grown quickly. Computer and intrusion forensics are a crucial component in helping criminal investigations track down committed crimes, recover stolen or damaged property, and bring offenders to justice. High-quality approaches should be used within a system to defend it and should be able to provide some guidance for any criminal investigation.

2. PROBLEM STATEMENT, CONTRIBUTION

The employment of ANN, FL, and CE in computer security and forensics has been addressed in a number of publications, however the issue is that each of these studies looked at the three technologies independently. That is to say, no earlier publication has compared and evaluated the use of the three paradigms.

This paper's objective is to present and emphasise a comparison of the applications of ANN, FL, and CE in computer forensics and security. It also looks at how these three strategies may be combined and how computer forensics and security can benefit from this.

3. COMPARATIVE STUDY

Artificial Neural Networks

A neural network is a sizable parallel distributed processor made up of simple processing units that has an innate propensity to store and be ready for use experience-based knowledge. ANNs, commonly referred to as "neural networks," are built using a similar paradigm to biological neural networks but with distinct terminology, as illustrated in Table 1. ANNs mimic how the human brain functions, and by doing so, researchers hope to recreate the brain's capacity for learning.Recently, neural networks have been used in computer security applications and are seen to be

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 720-723

e-ISSN : 2583-1062

Impact Factor : 5.725

superior to expert systems. Due to its capacity for learning, it differs from expert systems that employ a set of security rules learned from the knowledge of human experience.

Biological	Artificial
Soma	Neuron
Dendrite	Input
Axon	Output
Synapse	Weight

Table 1: Correspondences between biological and artificial neural networks

Fuzzy Logic

The fundamental concept of a set, in which any element is either a member of this set or not, is the foundation of the theory of classical sets. Such precision is usually unnecessary in daily life. As shown in figure 1, the essential idea of fuzzy sets is that an element has a specific degree of membership in a particular fuzzy set. As a result, the outcome can be partially true or partially false rather than being totally true or false. Inference using fuzzy logic involves four steps. 1)The inputs are initially fuzzified in order to establish their degree and the fuzzy set to which they should belong. 2)The inputs that have been fuzzed are then subjected to a set of fuzzy rules using a knowledge base. 3)The result from the second stage is then combined via decision-making into a single set.

4) Defuzzification is employed to eliminate the fuzziness and convert the output to numerical values so that computers and other devices can readily understand it. The fuzzy inference technique is shown in Figure 2.

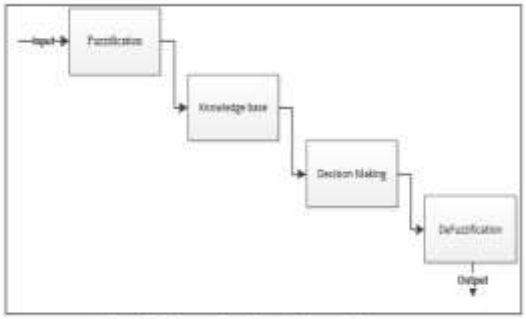

Fig 2: The mechanism of fuzzy inference

Evolutionary Computation

Theoretical and empirical approaches to EC have been established as the two basic methods.

The empirical approach is used to investigate evolutionary algorithms using statistical methods, while the theoretical approach searches through algorithms to find the mathematical truth about them.

Instead, all EC approaches mimic the natural evolutionary processes of selection, mutation, and reproduction by creating a population of people, evaluating their fitness, producing a new population using genetic procedures, and repeatedly repeating this process. Genetic algorithms (GAs), evolutionary strategies (GSs), and genetic programming are the three basic evolutionary computation approaches (GB). When it comes to computer security issues, genetic algorithms are particularly effective in spotting intrusions and harmful attacks. In a forensics system, evolutionary computing algorithms have been effectively employed to collect network forensics data and track new threats. The capacity of genetic algorithms to develop a set of optimised rules that identify unauthorised processes and carry out function-based process verification is one of the most helpful strategies in this situation.

4. HYBRIDS MODEL OF CI TECHNIQUES

The three varieties of computational intelligence, as well as its flaws, assets, and capabilities, have been covered in earlier parts. The usage of these three categories in conjunction for computer forensics and security will be discussed in this section. Fuzzy logic and an artificial neural network are combined to create a neuro-fuzzy system (NFS) or fuzzy neural network (FNN), which has the benefits of both. An NFS is a multi-layered system that can be characterised as follows, as depicted in Figure 3. Each neuron in layer 1 transmits external, precise input data to the following layer. The fuzzification layer in Layer 2 is responsible for identifying which fuzzy sets the crisp inputs belong to after receiving them. The inputs from the fuzzification layer are applied to a fuzzy rule neuron in layer 3, which is known as the fuzzy rule layer. Layer 4, the output membership layer, gets inputs from comparable fuzzy rule neurons and applies the fuzzy operation union to combine them with an output membership neuron. The outputs are finally defuzzied in the defuzzification layer so that the computer can interpret them.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 720-723

e-ISSN : 2583-1062

Impact Factor : 5.725

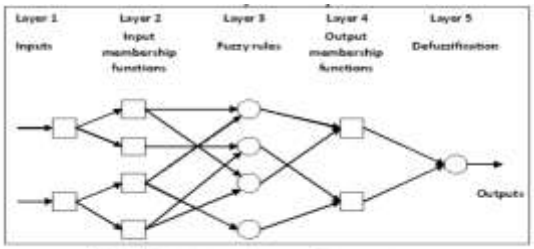

Fig 3: The structure of a neuro-fuzzy system

In order to evaluate whether activity in the system is normal, an NFS, which combines the learning capabilities of ANNs with the human-like capabilities of FL, is an appropriate approach to security systems.However, as illustrated in figure 5, neuro-fuzzy agents can be utilised in network intrusion detection systems (NIDSs) to identify known and unexpected behaviours by utilising fuzzy and neural networks. If-then fuzzy rules are employed when the agent's system logic is known (figure 4a), however a neural network is used in figure 4b when the incoming and outgoing network traffics are unknown. NFS can be trained differently and customised in computer forensics to be suited for the needed response time.

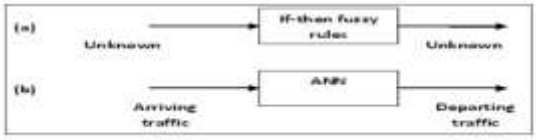

Fig 4 a: Known, if-then fuzzy rules **b**: Unknown, neural network

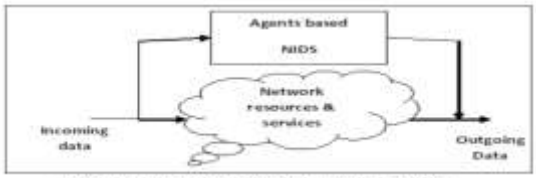

Fig 5: The structure of neuro-fuzzy agents in a NIDS

The technique for combining an ANN with a GA can be accomplished in a number of phases, as shown in Figure 6. First, chromosomes are used to represent the problem domain. The second step is the random selection of an initial set of weights, which can be visualised as a collection of gene chromosomes where each gene corresponds to a weighted connection in the network. Thirdly, a fitness function is developed to evaluate the chromosome's performance. The performance of the neural network must be assessed by the fitness function. By assigning each weight present in a chromosome to a corresponding link in the network, chromosomes are evaluated. The population size is defined at the end, together with the weights, crossover and mutation probability, and generation numbers.

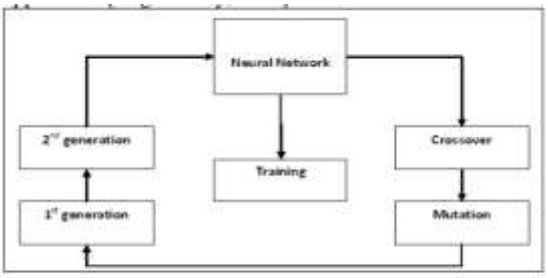

Fig 6: The mechanism of EAANs

5. RESULT

This work has given a result that suggests which technique can be applied to which field of security and forensics through the comparative examination of ANN, FL, and EC, and their concepts, abilities, advantages, limitations, etc. They have the following benefits, which have made them particularly effective at addressing computer security and forensics-related problems: First, they have the same level of intelligence as humans and can adapt to unexpected changes in conditions. Second, when complicated issues arise in network systems, they have a great deal of ability to handle them. In a third place, they are adaptable systems that can take on the requirements of specialised applications. Fourthly, they have the capacity to learn and adapt to shifting conditions. Additionally, they can be hybridised to improve performance. Table 2 displays the capabilities of each EC type and the extent to which they can be implemented, taking into account computer security and forensics. For instance, because it provides if-then fuzzy rules that can specify the typical and abnormal operations of a system, fuzzy logic is the best sort of EC for developing security rules. EC and ANN, on the other hand, have a limited capacity to develop security rules.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 720-723

e-ISSN : 2583-1062

Impact Factor : 5.725

Type / Ability	Learning	Classification	Clustering	Generalising	Security rules	Ambiguous Situations	Optimal solution	Recovery
ANN	√√√	√√√	√√√	√√√	√	X	√	X
FL	X	√√	√√	√	√√√	√√√	√	X
EC	X	√	√√	√	X	√	√√√	√√√

Table 2: Shows how ANN, FL, and EC can be applicable to abilities and this table is stated as: √√√ strongly applicable, √√ applicable, √ can be applicable, and X not applicable.

Hybrid computational intelligence has emerged in order to achieve better performance, as demonstrated in table 3.

In this study, four hybrid CI approaches have been investigated: Fuzzy Evolutionary Systems (FES), Neuro-Fuzzy Systems (NFS), Evolutionary Neural Systems (ENS), and Evolutionary Neural Fuzzy Systems (ENFS). An NFS is a combination of ANN and FL that combines the human-like reasoning and thinking capabilities of fuzzy systems with the ability to learn within a neural network. In terms of security, this system use FL to identify known assaults, and ANN is called upon when a certain behaviour is unidentified. As an alternative, FES can find optimal solutions more quickly and effectively than conventional methods. Finally, in terms of computer forensics and security, ENF systems possess all the capabilities of ANN, FL, and EC.

System/ Type	Computer Security	Computer Forensics
Neuro-fuzzy systems	Extract information from multiple sources	Can be differently trained and tailored to be appropriate for the required response time
	Use fuzzy rules to detect known attacks	Can be used with a quick search through large databases for fingerprint images
	Use neural network for unknown attacks	Used to help investigators in emotion recognition
	ANFIS can be used to train and during training can be used to classify patterns	Used efficiently in speaker verification
Evolutionary Neural Systems	Can automatically search for patterns	Can be used to recognise unconstrained fingerprints
	Detect novel attacks because of ability to adapt	Avoiding the trapping of neural networks in a local minimum
	Flexible system	Can be used for face recognition
	Can provide a better classifier in a short time	Provide evidence as fast as possible
Fuzzy Evolutionary Systems	Can combine more than EC algorithms with FL to achieve a higher performance	Can identify the type of attack very rapidly
	Can be used to detect changeable attacks	Used for fingerprint recognition
	Can be retrained to detect novel attacks	Can be used to identify speakers
Evolutionary Neural Fuzzy Systems	Have all the above abilities of ANN, FL, and EC in computer security	Has all the above abilities of ANN, FL, and EC in computer forensics

Table 3: overview of hybrid CI systems in computer security and forensics.

6. CONCLUSION AND FUTURE RESEARCH

It is clear that computer security is a major problem for businesses, governments, etc. It aids in preserving the network system's availability, secrecy, and integrity. However, computer forensics have demonstrated a great potential to strengthen the integration and attack resistance of network infrastructures.

Artificial neural networks, fuzzy logic, and evolutionary computing are some of the methods that can be utilised to address computer security and forensics-related problems.

This essay has demonstrated how these three approaches are used in computer security and forensics, as well as their uses, capabilities, benefits, and limitations.

7. REFERENCES

[1] Engelbrecht, A.P. 2007. Computational intelligence: an introduction, 2nd edition, Sussex: John Wiley & Sons Ltd.

[2] Ryan, J., Lin, M. and Miikkulainen, R. 1998. Intrusion Detection with Neural Networks. Advances in Neural Information Processing Systems 10:72-77.

[3] Lippmann, R., Haines, J., Fried D., Korba, J. and Das, K. 2000. The 1999 DARPA Off-Line Intrusion Detection Evaluation. Computer Networks, 34:579-595.

[4] Mohay, G., Anderson, A., Collie, B., Vel, O. and McKemmish,R. 2003. Computer and Intrusion Forensics, Massachusetts, Artech house, Norwood.

[5] Haykin, S. 2008. Neural Networks and Learning Machines, 3rd edition, New Jersey.: Prentice Hall, Inc.