A Comparative study of Computational Intelligence in Computer Security and Forensics

Sulaiman Al amro\textsuperscript{1}, Khalid Aldrawiesh\textsuperscript{1} and Ajlan Al-Ajlan\textsuperscript{2}
\textsuperscript{1}De Montfort University, Software Technology Research Laboratory (STRL)
Leicester, LE1 9BH, UK
\{salamro, Khalid\}@dmu.ac.uk
\textsuperscript{2}Qassim University, Information System Management (ISM)
Al-Melaidah, Buraydah, Qassim, 51452, KSA
aajlan@qu.edu.sa

Abstract
Because of the growing reliance that corporations and government agencies place on their computer networks, the significance of defending these systems from attack cannot be underestimated. Computer security and forensics are crucial in protecting systems from attack or from unauthorized access that might have undesirable consequences, and can help to ensure that a network infrastructure will remain integrated and survive. The use of high quality techniques within a system will provide a better protected system, and will offer clues that might help in any criminal investigation. Techniques such as artificial neural networks, fuzzy logic, and evolutionary computing can be used to help deal with issues associated with computer security and forensics. This paper concentrates on the use of neural networks, fuzzy logic, and evolutionary computation in computer security and forensics. It also examines the hybrids of these three techniques, and considers how they can be applied to computer security and forensics.

Keywords computer security, forensics, neural networks, fuzzy logic, and evolutionary computation.

Introduction
In the years since it was established, Artificial Intelligence (AI) has provided a rich topic of debate for writers and researchers who have produced a large number of articles, books and studies on the subject. While AI is similar to many other systems, it uses unique methods and is remarkable for providing intelligent systems that simulate the nature of life, human beings, etc., in order to achieve improved simulations. Computational Intelligence (CI) includes techniques such as neural networks, fuzzy logic, and evolutionary computation. It also includes other methods that use swarm intelligence, artificial immune systems, etc. However, with the ever-increasing use of computer networks, computer security has become an important issue in modern systems [Ryan et al, 1997]. A single infringement of a network system can cause much damage to an organisation. For this reason, computer security has become vital for protecting systems from attack and from its undesirable outcomes. Lippmann et al (2000) lists four main types of attack which can be harmful to the system:

Denial-of-service (DoS) attack: This type makes the network unable to operate because users are not allowed to access a resource. It does this by making the network full or busy.
Remote to local (R2L) attack: This is an attack in which an attacker who has no access to a resource removes a file or modifies data by acquiring access to the resource.
User to root (U2R) attack: Here, the assaulter begins by hacking the system as a normal user and later tries to obtain root privileges.
Scanning or Probing: In this type, the attacker attempts to find any weakness or susceptibility to attack by scanning a particular resource. Data mining is a common form of this technique.
Eavesdropping, Data Modification, Identity Spoofing, Password-based attacks, Man-in-the-Middle attack, Comprised-key Attack, Sniffer attacks, and Application Layer attacks are also common types of attacks that harm network systems. However, computer and intrusion forensics have been rapidly growing in recent years because of the presence of computers and computer networks everywhere [Mohay et al, 2003]. Computer and intrusion forensics represent an important approach in helping criminal investigations, not only to track crimes that have occurred and recover what has been stolen or
The use of high quality techniques within a system should help to protect a system, and should be able to offer some direction in any criminal investigation. Techniques such as Artificial Neural Networks (ANNs), Fuzzy Logic (FL), and Evolutionary Computing (EC) have been shown to have considerable ability in dealing with issues associated with computer security and forensics.

The paper is organized as follows: Section II states the problem and contribution. Section 3 draws a comparative study in the use of Artificial Neural Networks, Fuzzy Logic, and Evolutionary Computation in computer security and forensics. Section 4 will start with a brief overview of what hybrid computational intelligence is. It will then examine the hybrids of ANN, FL and EC and how they can be used to help computer security and forensics. Section 5 will provide the results of this paper.

Statement of problem and contribution

There are several publications which have studied the use of ANN, FL, and CE in computer security and forensics, but the problem is that these publications have examined them separately. That is, there is no previous publication which has examined the use of the three paradigms and drawn a comparison between them.

The contribution of this paper is to provide and highlight a comparative study of the use of ANN, FL, and CE in computer security and forensics. It also examines the hybrids of these three techniques and how they can be applied to computer security and forensics.

Comparative Study

Artificial Neural Networks

A neural network is an enormous parallel distributed processor composed of uncomplicated processing units, which has an inborn tendency to retain knowledge gained through experience and to be ready for use [Haykin, 2008]. ANNs, also known simply as neural networks, are constructed on the model of biological neural networks and are similar to it, but different terms are used, as shown in Table 1. ANNs work in ways similar to that of the human brain, and the purpose of following the brain in this way is to attempt to replicate its ability to learn.

Neural networks have recently been applied to computer security and are seen as an improvement over expert systems. It is differ from expert systems that use a set of security rules acquired from the knowledge of human experience by its learning ability [Bonifacio et al, 1998]. ANNs have been applied in anomaly detection systems as a substitute for statistical analysis [Ryan et al, 1998]. They can also be used in misused detection in which its learning ability enables it to detect dangerous attacks, in cases where many attackers strike the network at the same time.

<table>
<thead>
<tr>
<th>Biological</th>
<th>Artificial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soma</td>
<td>Neuron</td>
</tr>
<tr>
<td>Dendrite</td>
<td>Input</td>
</tr>
<tr>
<td>Axon</td>
<td>Output</td>
</tr>
<tr>
<td>Synapse</td>
<td>Weight</td>
</tr>
</tbody>
</table>

Table 1: Correspondences between biological and artificial neural networks

Neural networks are capable of solving problems related to patterns, using several techniques such as clustering, classification and generalising; they are also able to predict events in the future on the basis of history [Mena, 2003]. These abilities may be useful for forensics, where they can be used to collect evidence after a crime has been committed. However, ANNs have four algorithms which can be helpful for forensics [8]; first, Classification which is a helpful algorithm for investigators by which to determine illegal activities that have been conducted within the system. Next, Clustering may have benefits for analysts who wish to group similar attacks on a particular system or systems. Grouping crimes in this way makes it easier to deal with a new attack which is similar to earlier ones, because these have been investigated and analysed. The third algorithm is generalising which can be used to identify data that have not been seen in the system. As a result, a new type of attack can be identified by the neural generalising algorithm, and this ability can help in the investigation of crimes. Finally, there are forecasting algorithms which can be useful for investigators by providing a list of suspicious people.

Fuzzy Logic

The theory of classical sets depends on the basic idea of a set in which any element is either a member of this set or not [Chen and Pham, 2001]. In most cases of daily life, such precision is inappropriate. By contrast, the fundamental concept of fuzzy sets is that an element has a certain degree of membership of a given fuzzy set, as shown in figure 1. Therefore, the result is not absolutely true or false, but can be true or false to some degree [Negnevitsky, 2005].

One of the most important capabilities that a network system needs to have in its security system is a fast response, and fuzzy logic has this ability when applied to a security system [Gomez and Dasgupta, 2002]. Fuzzy inference is the process of making decisions using fuzzy sets and it has four fundamental steps, namely, fuzzification, knowledge base, decision making and defuzzification [Chen and Pham, 2001].
There are four steps in fuzzy inference [Negnevitsky, 2005]: first, fuzzification is used to take the inputs, to decide the degree of these inputs and determine which fuzzy set they should belong to. Next, knowledge base is used to take the inputs which have been fuzzed, and to apply a set of fuzzy rules to them. Decision making is then used to unify the output from the second step into a single set. Finally, defuzzification is used to remove the fuzziness and transform the output to numerical values so that it can be easily understood by computers and other machines. Figure 2 shows the mechanism of fuzzy inference.

Moreover, fuzzy systems have a number of aspects which make them suitable for intrusion detection [Dickerson et al, 2006]. First, they have the ability to combine inputs taken from different sources. Secondly, some encroachments cannot be clearly determined; thus, fuzzy systems are best able to deal with these intrusions. Thirdly, fuzzy systems have the ability to recognise a degree of membership, and this can make alarms sound differently, depending on the attack (low-medium-high). Thus, if the attack is very dangerous, the alarm will sound high, etc. In addition, fuzzy rule-based detection systems provide a perfect method to capture the imprecise tendency of occurrences in the computer network system [Yao et al, 2006]. Indeed, fuzzy logic is perfect if the differences between normal and irregular classes are not specified, because the use of fuzzy spaces enables an object to be a member of different classes at the same time [Gomez and Dasgupta, 2002].

Further, fuzzy logic tools have the ability to help by giving a useful report on how a computer has been utilized [Meyers, 2005]. Furthermore, fuzzy logic is a good tool for forensics investigators when they are uncertain about the file type or the text string they are seeking [Shinder, 2002]. Fuzzy logic, which allows linguistic variables to be presented in mathematical formulas, can help in making the evidence provided by witnesses more significant [Verma, 1997]. Using a fuzzy engine will solve the problem of misspelled words, or even of the use of the wrong word, by relying on the selection of the degree of fuzziness [Johansson, 2003]. Filter I is a fuzzy logic filter that is used to analyse data in files, which can be very useful for forensics [Wai, 2002]. However, it is very difficult to avoid integrity leakage while conducting a forensic investigation, but it can be achieved by using the concept of fuzzy measures, which differ from traditional data analysis by having great robustness and scalability [Pan et al, 2008].

**Evolutionary Computation**

Two main approaches to EC have been identified by [Fogel, 2006]: theoretical and empirical. The theoretical approach is used to search through algorithms to seek the mathematical truth about them, while the empirical approach is used to examine evolutionary algorithms by statistical means. Alternatively, by creating a population of individuals, appraising their fitness, producing a new population via genetic procedures and repeating this process several times, all EC methods imitate the natural evolutionary processes of selection, mutation and reproduction [Negnevitsky, 2005]. There are three main methods of evolutionary computation: genetic algorithms (GAs), evolutionary strategies (GSs) and genetic programming (GP) [Mitchell, 1998]. Genetic algorithms provide an efficient way to solve problems associated with computer security, especially in detecting intrusions and malicious attacks [Sinclair et al, 1999]. Also, GP has the ability to learn new events in the network and to use computer programs to detect malicious attacks; these properties make it more powerful in the area of computer security and intrusion detection [Crosbie and Spafford, 1995].

Evolutionary computation algorithms have been used efficiently within a forensics system to gather network forensics data and to track novel attacks [Merkle, 2008]. One of the most useful approaches here is to use the capability of genetic algorithms to create a set of optimised rules that recognise unauthorised processes and perform function-based process verification [Bradford and Hu,
However, a problem has arisen in computer forensics concerning how to determine the type of a file fragment. This problem can be solved by using a genetic algorithm, because it can provide a better classification solution than traditional techniques [Calhoun and Coles, 2008]. Furthermore, genetic algorithms can also be used in other areas of forensics and can save time for investigators.

**Hybrids Model of CI techniques**

In previous sections, the three types of computational Intelligence, their weaknesses, strengths and abilities have been discussed. This section will consider the combination of these three types for use in computer security and forensics.

A neuro-fuzzy system (NFS) or fuzzy neural network (FNN) is a combination of fuzzy logic and an artificial neural network that has the advantages of both. As shown in Figure 3, an NFS is a multilayered system which can be described as follows [10]. In layer 1, external crisp input data are transmitted to the next layer by each neuron. Layer 2 is called the fuzzification layer, which receives the crisp inputs and determines which fuzzy sets they belong to. Layer 3, which is called the fuzzy rule layer, receives inputs from the fuzzification layer and applies them to a fuzzy rule neuron. Layer 4, the output membership layer, receives inputs from analogous fuzzy rule neurons and combines them with an output membership neuron by applying the fuzzy operation union. Finally, in the defuzzification layer the outputs are defuzzified in order to make them understandable by the computer.

![Fig 3: The structure of a neuro-fuzzy system](image)

An NFS is an appropriate approach to security systems, combining the learning ability of ANNs with the human-like ability of FL in order to determine whether activity in the system is normal [Maghooli and Moghadam, 2006]. However, neuro-fuzzy agents can be used in network intrusion detection systems (NIDSs) in order to determine known and unknown behaviours by making use of fuzzy and neural networks [Abouzakhar and Manson, 2006], as shown in figure 5. When the agent’s system logic is known, if-then fuzzy rules are used (figure 4a), whereas when the incoming and outgoing network traffics are unknown, a neural network is used (figure 4b). In computer forensics, NFS can be trained differently and tailored to be appropriate for the required response time. They can also be used with a quick search through large databases for fingerprint images [Quek et al, 2001]. They also can be used to help investigators in emotion recognition and speaker verification [Yarmey, 1995].

![Fig 4 a: Known, if-then fuzzy rules b: Unknown, neural network](image)

![Fig 5: The structure of neuro-fuzzy agents in a NIDS](image)

There are two problems associated with ANNs when used by themselves: these can be solved by combining them with EC. First, they cannot provide optimal solutions; i.e. they are unable to provide a desired solution to a given problem. Secondly, optimal ANN topology cannot be systematically identified: “The ‘right’ network architecture for a particular problem is often chosen by means of heuristics, and designing a neural network topology is still more art than engineering” [Negnevitsky, 2005, p.285]. As shown in Figure 6, the mechanism for combining an ANN and a GA can be achieved in several steps. First, the problem domain is represented as chromosomes. Secondly, within small intervals, a set of initial weights is randomly selected; this can be represented as a set of gene chromosomes in which each gene matches a weighted link in the network. Thirdly, a fitness function is defined to appraise the performance of the chromosome. The fitness function must evaluate the performance of the neural network. The evaluation of chromosomes is achieved by allocating each weight included in the chromosome to a corresponding link in the network. Next, the genetic operators (crossover and mutation) are selected. The
crossover operator generates a single child with genetic material taken from the two parents by taking the chromosomes of two parents. The genes in the child’s chromosomes are represented by the analogous parent’s genes. On the other hand, a gene in the chromosome is randomly selected by the mutation operator and a small value is added to every weight in this gene. Finally, the population size is defined; here, the number of weights, the mutation and crossover probabilities and the generation numbers are defined. Several neurons and their interconnections then evaluate the success of the application [Negnevitsky, 2005].

![Fig 6: The mechanism of EAANs](Image)

The combination of GA/ANN is appropriate for computer security. In particular, this approach is fitting for intrusion detection because it is robust, parallel and non-linear, making it suitable for real-time applications with high precision requirements [Wang et al, 2001]. In addition, this technique can search automatically, and has a robust adaptation and great flexibility. Such an evolutionary neural network (ENN) can be used in an IDS. In computer forensics, ENN can be used to recognise unconstrained fingerprints and also to avoid the trapping of neural networks in a local minimum [Reddy and Reddy, 2004].

Fuzzy systems can also be combined with evolutionary algorithms to produce fuzzy evolutionary systems (FESs). In addition, both computer research and practical applications have shown that fuzzy evolutionary algorithms have the ability to search for optimal solutions more rapidly and efficiently than standard GAs [Xu and Vukovich, 1994]. Indeed, many evolutionary algorithms can be combined with fuzzy systems to provide excellent IDSs [Haghighat et al, 2007]. These evolutionary algorithms can be used separately, or can be combined with each other to achieve the same purpose with higher performance. However, the use of fuzzy genetics in IDSs can be explained in two steps [Fries, 2008]: the first is to use a genetic algorithm to create a subset of optimal communication features; the second step is to use the genetic algorithm to optimise a set of rules which are then used to distinguish abnormal from normal communication behaviours. In forensics, a genetic-fuzzy system can be used to identify types of attack, which is very important in recovering from such attacks. This can be achieved by incorporating the identification of attack types within the system.

Fuzzy systems lack the learning ability of neural networks and the optimal solutions of evolutionary computation, but do have the advantage of providing knowledge in linguistic form [Castellano et al, 2007]. As a result, the combination of evolutionary, neural and fuzzy systems crossbreeds the learning abilities of neural networks with the reasoning mechanism of fuzzy systems and the ability to search for optimal solutions of evolutionary computing. Such networks can be used to construct an efficient intrusion detection system, and each of its components plays a role in making the system more successful [Toosi and Kahani, 2007]. First, features are extracted from the audit data by a number of neuro-fuzzy classifiers in order to group activities in the network. Each input to the system is assigned a degree of membership which determines the dataset to which it belongs. Secondly, a fuzzy inference system is used to decide whether an activity is normal or not. The outputs of the neuro-fuzzy classifiers are mapped to the final output space in order to recognize them. Finally, the structure of the fuzzy sets is optimized by means of genetic algorithms, which are used in order to achieve the best result.

Evolutionary fuzzy neural systems can be applied to help investigators find evidence when a crime has occurred. However, the identification of glass is a significant task in forensic science, where good evidence has a fundamental role in investigations. The abilities of a neuro-fuzzy-genetic system make it an appropriate approach for the identification of glass types. The first step is to construct the neuro-fuzzy classifier that assigns each input to an associated fuzzy set. Next, an initial rule base for the neuro-fuzzy classifier is generated. The final stage is to apply genetic algorithms in order to provide optimal solutions and improve the result. Such a system has the ability to identify the type of glass more accurately than by using just a neuro-fuzzy classifier system [Gorzalczyz, and Gradzki, 2000].

The result

In the comparative study of ANN, FL, and EC, and their concepts, abilities, advantages, drawbacks, etc., this paper has produced a result that indicates which technique can be applied to which field of security and forensics. They have been shown to be most efficacious in dealing with issues associated with computer security and forensics because they have the following advantages: first, they are sufficiently intelligent (like humans) to deal with sudden
changes in circumstances. Secondly, they have considerable ability to deal with complex problems when they appear in network systems. Thirdly, they are flexible systems which can acquire the need of specialized applications. Fourthly, they can learn and adjust to changing environments. Last, but not least, they can be hybridised to provide better performance.

ANN takes its idea from the biological neural networks in the human brain, and has the great ability of learning and adjusting itself to new circumstances. In computer security, ANN has shown significant ability in detecting novel attacks and learning them through training. ANN has three particular abilities that make it an appropriate approach for computer forensics, viz, classification, clustering, and generalising. These help investigators by identifying a group of crimes that are similar to each other, distinguishing between legal and illegal behaviour in the system, and recognising attacks that have not been detected in the system.

Fuzzy logic is a human-like reasoning approach that resembles the ambiguity of human daily life. It has the ability to describe core aspects that may not be apparent: i.e. it can provide precise outcomes by its ability to assess degrees of membership and linguistic variables. However, security in itself is imprecise, and therefore a fuzzy system is a proper approach to computer security. There are a great many advantages to using fuzzy systems in security, such as defining attacks by applying a set of fuzzy rules, and exploiting the speed of its response. Many cases in forensics, such as unclear file types, bad handwriting, etc., are uncertain, but fuzzy systems have shown considerable ability in dealing with these kinds of ambiguous cases.

Evolutionary computation derives its concept from the evolution of nature, which takes the advantages gained from one generation and passes them on to the next. It can also choose the best or optimal solution to a problem that has appeared in a system because genetic algorithms and programming are used, and these can be adjusted to restart from a particular point when a problem arises. EC algorithms can also be used to search and gather network evidences from a large amount of network data, and can provide valuable reports on malicious behaviour in such networks. Taking into account computer security and forensics, Table 2 shows the abilities of each EC type and the degree to which they can be applied. For instance, Fuzzy logic is the best type of EC for constructing security rules because it has the if-then fuzzy rules that can specify the normal and abnormal activities of a system. On the other hand, EC and ANN, has less ability to create security rules.

<table>
<thead>
<tr>
<th>Type</th>
<th>Learning</th>
<th>Classification</th>
<th>Clustering</th>
<th>Generalising</th>
<th>Security rules</th>
<th>Ambiguous Situations</th>
<th>Optimal solution</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANN</td>
<td>√√√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FL</td>
<td>X</td>
<td>√√</td>
<td></td>
<td>√√√√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC</td>
<td>X</td>
<td>√</td>
<td>√√</td>
<td>√√√√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

In order to obtain improved performance, hybrid computational intelligence has come to light, as shown in Table 3. There are four hybrid CI techniques that have been scrutinised in this paper: Neuro-Fuzzy Systems (NFS), Evolutionary Neural Systems (ENS), Fuzzy Evolutionary Systems (FES) and Evolutionary Neural Fuzzy Systems (ENFS). An NFS is a hybrid of ANN and FL, which has the ability of learning within a neural network, and has the human-like reasoning and thinking design of fuzzy systems. In security, this system uses FL to detect known attacks, and, if certain behaviour is unknown, then ANN is invoked. It can be trained and tailored to be appropriate to the required response time, making it useful for forensic investigation. On the other hand, ENS provides a system that is capable of learning, adjusting, and providing optimal solutions. It also provides an automatic search and has robust adaptation and great flexibility, making it applicable to computer security. In addition to these abilities, this system can provide forensic investigation evidence extremely quickly. Alternatively, FES has the ability to search for optimal solutions more quickly and more efficiently than traditional techniques. It can combine various EC algorithms with FL to achieve a high quality security system. It can also be quickly used to identify the type of attack when a forensic investigation has been initiated. Finally, ENF systems have all the abilities of ANN, FL, and EC in computer security and forensics. It provides a system that has the capability of learning, adjusting to and searching for optimal solutions, and has human-like reasoning and thinking.

Depending on the outcome of this paper, it is apparent that each one of the three types of EC has its own power. However, when choosing the best type to be used to enhance computer security and forensics, one can decide depending on the security policies within the organisation; i.e. one cannot decide which is the best because they all have shown excellent ability when they are used in computer security. For example, when a fast response is extremely important within an organization, a fuzzy logic is the best EC type to be used.
It is evident that computer security is a critical issue within organizations, government agencies, etc. It helps to maintain the integrity, secrecy and availability of the network system. However, computer forensics have shown their significant ability to make network infrastructures more integrated and capable of surviving attack. Techniques such as artificial neural networks, fuzzy logic, and evolutionary computing can be used to help deal with issues associated with computer security and forensics. This paper has shown the use of these three techniques in computer security and forensics, their applications, abilities, advantages, drawbacks, etc. We also discovered that the hybrids of the three techniques provide better solutions to the deficiencies than when only one type of CI is used.

Depending on the particular circumstances, fuzzy logic has shown considerable ability in both computer security and forensics. Several questions arise in this research proposal, but one is of particular significance: Is it possible to extend and improve fuzzy logic to meet the changing requirements of computer security and forensics? The most encouraging area for future research would be to investigate how to improve the performance of fuzzy logic to meet the requirements of computer security and forensics. Several studies and articles have shown that the future of fuzzy logic is not determined, i.e. there are no boundaries for searching in this area. Therefore, our future research will focus deeply on how to use fuzzy logic in computer security and forensics.

### References


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

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


