International Journal of Cyber-Security and Digital Forensics (IJCSDF) 9(2): 71-89
The Society of Digital Information and Wireless Communications (SDIWC), 2020 ISSN: 2305-0011

Investigating Intrusion Detection Security Techniques in Cloud-Based Networks

Meisam Sharifi Sani

Master of Software Engineering, Science and Research. Kerman. IRAN

Meisam.sharifi.s@gmail.com

ABSTRACT

Cloud Computing Technology, with its abundant advantages, has created new progress in the world of computing and has pushed Information Technology (IT) Industry a step forward. Therefore, that great organization have deposited a large number of their processes and information to clouds. Security and intrusion detection into a cloud-computing network show itself more than other networks. Many studies have introduced intrusion detection protocols for these networks, but few have investigated the issue of security. Therefore, the present study investigates security techniques for the cloud-computing environment based on the architecture of intrusion detection and finally compares some of these methods with each other.

KEYWORDS

Security, cloud computing, intrusion detection

1 INTRODUCTION

Cloud computing refers to programs and services which are run in a distributed network and use virtual resources. Moreover, in this way internet, common protocols, and network standards are accessible. Conceptually, the point is that resources used in cloud computing are virtual and unlimited, and characteristics of physical systems in which software is run are completely apart from the user system [1],[2].Regarding ever-increasing growth of technologies and users' needs diversity in the field of IT, cloud computing position has developed than before. The cloud phenomenon is rapidly turning into an important service in internet computing. Cloud computing technology is transforming into a popular technology in life. To encourage using cloud computing, besides generating and developing necessary telecommunication and hardware infrastructures, security issues, especially availability, resources integrity, protecting privacy, and consequently, intrusion detection systems are essential [1]. Losing direct control on properties and proper mismanagement probability by the cloud server, which are the most important threats in this kind of computing, make cloud atmosphere distinguished from traditional models for client organization regarding security [3]. This issue in hybrid models and cloud public services and also in the private services model, when represented by the third party, is the most important security hazard. In such conditions, using cloud services necessities responsibility transfer and, on course controlling a part of the organization's information and systems to a server outside the organization [4]. Furthermore, organizations may depend more on a server, and especially they encounter challenges in transferring data and services into the organization or to another server. In fact, using cloud computing advantages may lead to generating new services, and it takes away necessary organizational agility in the incidence of security accidents [5]. Although sharing resources is among the basic cloud computing advantages, this issue may create a big security hazard for the organization. Since illegal activities that may be done by others utilizing common resources directly damage the organization's fame and credit. Extremer hazard happens when one of the cloud services client organizations get access to other clients' properties due to the incidence of an attack or in other abnormal situations [6]. Despite existing hazards in cloud computing, a different approach has been introduced to

confront threats. Investigating this approach makes it possible to categorize it into two general groups. Access control, countermeasure, and response. Access control is making sure of legal users' access and preventing illegal access to information systems [7]. Countermeasure and response are finding created problems and findings proper reaction against them. Gartner also introduced seven security issues that users have to be aware of them: premium user access, obeying the rules, data location, data separation, detection, research support, and surviving duration. So many solutions have been introduced to encounter threats. However, a proper solution and an acceptable level of security have not been achieved yet. To establish security and prevent destructive attack effects, intrusion detection systems are used [8],[9]. When end-user use cloud services and save their data in servers' infrastructures, the most important security aspects are related to privacy and users' data confidentiality. End users want to know where their information is saved and who has control over and access to their information, and also users are inclined to have a guarantee that even servers don't have illegal access to their sensitive and important data [10]. End-users use represented services by cloud servers, although they exactly don't know where these services resources are located when a security incidence happens [11]. This shows a potential problem that is sometimes beyond the control of cloud servers. Saved data by cloud servers are not influenced by servers' guidelines but is influenced by the servers' residence country. Users have to agree with related conditions and requirements when using such services, which accordingly grants the right to disclose user's information by accepting rules and requirements of law enforcement to the servers [12]. Cloud computing environments have attracted the attention of many organizations, and many organizations are migrating to cloud environments. There are different and famous architectures in these environments. Still, the more this architecture be compatible with standards, rules, and best experiences of today's communication and information technology, the more suitable structure it will have and makes organizations more secure through this migration into cloud environments. In fact, the goal of intrusion detection systems is not to prevent the attack. Still, the goal is to explore and identify attacks, to detect security problems in computer networks, and to announce them to the system manager. Generally, there are three security issues in networks security:

Confidentiality: information that is transferred through the network has to be accessed only by qualified individuals. Destroying confidentiality makes information available by illegal individuals.

Integrity: sent message to the receiver must not be changed. In fact, integrity guarantees message perfectness.

Availability: data and resources have to available every moment. Hackers damage availability through disrupting bandwidth. DOS attacks are the most important ones which influence network servicing [13].

2 ARCHITECTURES OF INTRUSION DETECTION SYSTEMS

Intrusion detection is a wide range of designed security techniques to identify (and report) destructive systems and network activities or registering evidence of intrusion. Based on location in the network system and activity domain, intrusion-detecting systems are categorized into two groups of Host Intrusion Detection (HID) and Network Intrusion Detection (NID). To obtain the maximum efficiency and security, a combination of these intrusion systems are used which are known as Distributed Intrusion Detection System (DIDS) [14],[15]. In Figure 1. Shows the general architecture of cloud network intrusion detection systems.

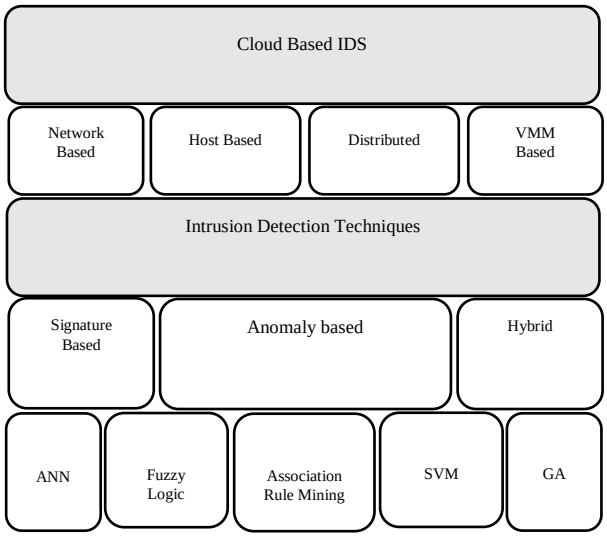

Figure 1. Cloud-based intrusion detection systems [16].

2.1 Host Intrusion Detection System (HIDS)

It is an intrusion detection system that is located in the host atmosphere and scans the activities. Generally, HIDS can detect attacks and threats like operating system input files, software input files, or database input files on the host computer. HIDS runs only on the host or single computers and is not aware of the whole network. These systems only investigate and observe input and output packs to a computer and alarm network manager or computer user in the case of intrusion detection or suspicious activity. Decisions excellent organizing ability exclusively and uniquely for each host is these systems' important point. In addition, HIDS provides specific information regarding where by who and when an intrusion has occurred. Less compatibility between the operating system and software and various soft wares are among HIDS disadvantages. This kind of intrusion detection architecture is dependent on log files, and consequently, if log-files data removed or attacker could manipulate input files, attack detection in these systems encounters with challenge and as a result in this kind of architecture logs protection process and intrusion detection system's output events have to be applied as best as possible. Another important point is that these systems don't identify some attacks happed in lower layers of the network [17]. In Figure 2. Shows the HIDS architecture.

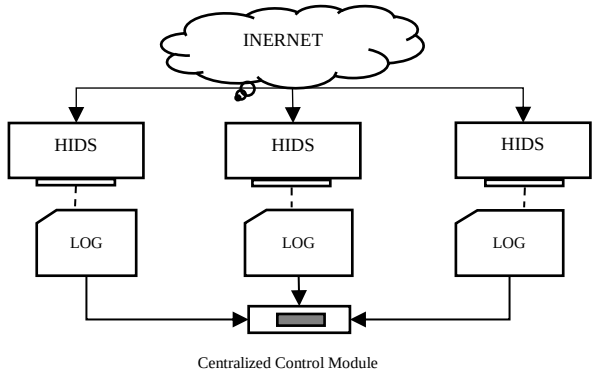

Figure 2. HID Architecture

2.2 Network Intrusion Detection System (NIDS)

NIDS has been widely located among systems in which network security importance has been increased, and many devices have been introduced to improve network security. NIDS is responsible for analyzing traffic throughout the network to identify threats. These systems identify destructive activities like Denial of Service Attacks (DOS), scan reports, and…throughout the whole network. Network-based systems are soft wares or hard wares which are located throughout the whole network and existing computers in a specific place or places of the network to monitor passing traffic, they analyze network traffic and in the case of an abnormal attack or behavior an alarming message sent to network manager [17]. It is one of the most popular systems, which is used to scan suspicious packs during every packing. Signature-based designs have favorable rates in such methods that are employed more effectively and more accurately in confrontation with security threats. However, they may be ineffective against attacks that have not been recognized yet. After destructive packs detected manually, they are confronted, and a signature is created for them [15]. In Figure 3 shows the NIDS architecture.

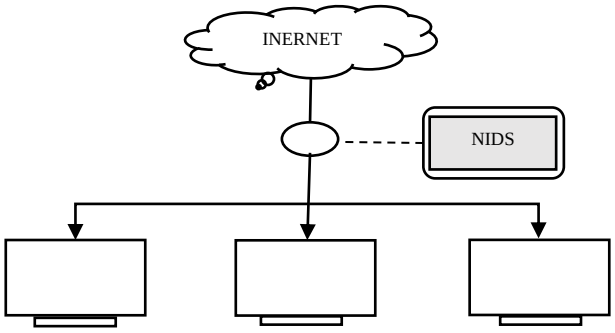

Figure 3. NIDS architecture

2.3 Distributed Intrusion Detection System (DIDS)

DIDS contains several detection systems on an extensive network, which all of them communicate with each other. It facilitates accident analysis and instant attack data utilizing a central server. Considering this cooperation, the security personnel network can have a comprehensive observation of what is happening inside its network. Also, it permits a company to effectively manage accidents analysis resources through focusing on its attack experiences and to provide a fast and easy way to detect new processes and patterns and to identify network threats in several parts of a network through analysis. These systems are made up of several NIDS or HIDS or a combination of these two kinds as well as a central management station. In this way, each intrusion detection system existing in the network sends its reports to the central management station. Central station is in charge of investigating arrived reports and noticing system security responsible. This station also has to update detection rules-base of each of the existing IDS in the network. Information is saved in the central management station. When the current system is used to send management data, extra security supplied by cryptography or Virtual Private Network (VPN) (more recommended). High complexity is the essential problem of DIDS. Ranges and functions vary from a producer to another producer, and accordingly, DIDS characteristics are not so evident [18]. In Figure 4. Shows the DIDS architecture.

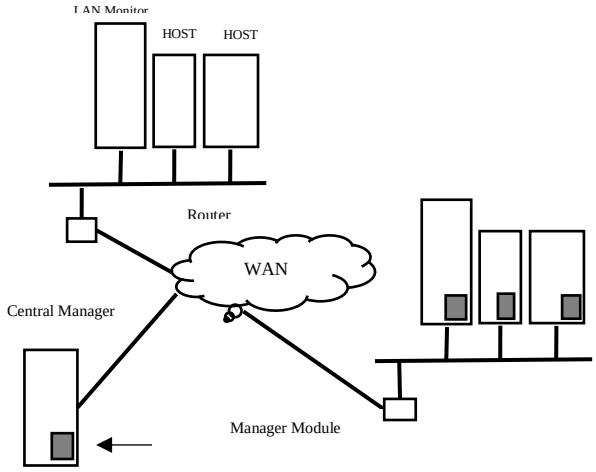

Figure 4. DIDS architecture [18].

2.4 Virtual Machine Monitor Intrusion Detection System

Using this technology makes it possible to place so many servers on a physical server. Because nowadays, most servers use 8% to 12% of their real ability in normal conditions, it will be possible to have optimal use of the remained unused resources by transferring several servers on a physical machine. It is possible to transfer soft wares running on an old machine to virtual servers with high ability regardless of their compatibility with new hard wares and when synchronous use of several operating systems in places with operating system multiplicity and is impossible to assign a single server to each of operating systems. It is possible to share the resources of some machines among virtual machines regardless of the virtual machine that has become hosted on which network. These resources are memory or process type and are implemented by adding a layer from software called Virtual Machine Monitor (VMM) to hardware. Usually, there is a virtual machine with a relatively high ability, which is called a privileged or special virtual machine that can manage and control other virtual machines. For a virtual machine system, the system's specific vulnerabilities cause the most common attacks. Moreover, these attacks are conducted by a program or software known as malware (destructive software). Viruses, worms, and Trojan horses are among the common malware. Indeed, some of them are destructive processes from the user, which do not influence the core of the operating system. Some of them ambush in base or process or change the space. In Figure 5. shows the architecture of the virtual machine monitor intrusion detection systems [19].

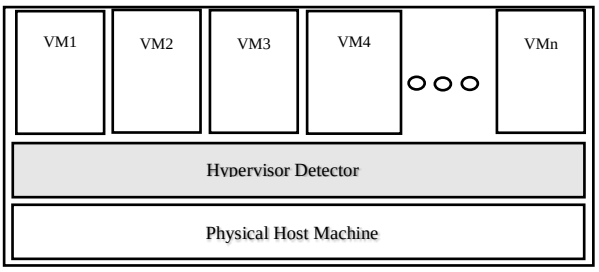

Figure 5. The architecture of virtual machine-based intrusion detection systems [19].

3 INVESTIGATING ATTACKS IN CLOUD NETWORKS

3.1 Worms

The worm sends its copies to other exiting computers utilizing the network.

In contrast with the virus, worms do not attach themselves to other programs. In addition, worms damage network by occupying bandwidth, while viruses most often destroy existing applications in an infected computer and lose the current information. Worms have two operational stages: exploring stage and transferring step. During exploration, the worm only examines network to find vulnerable points in the network. During moving, destructive code related to worm transfers to the victim system. Flow-based methods focus on worm identification during the exploration stage since pack content is needed to identify harmful codes during transfer.

In many cases, identifying worm considered the same as identifying scanning in the network. For instance, the introduced method by [20], which is represented for determining to scan in the network, is easily generalized to identify worms.

3.2 Denial of Services

In this type of attack, system resources are used more than ever, and it rejects standard requests for holding supplies. Attackers take away some computing from users who are in charge of handling legal requests. These types of attacks usually use weak software points to damage them and prevent from system's legal communications by overloading in communicational channels. That is, it makes the server out of responding. In this type of attack, authorized users' access to services encountered with problems or disconnected. This attack alternatively occurs on the internet. From 2001 to 2015, 24.5 IP addresses have been victimized by service limiting attacks per hour throughout the globe [21].

3.3 Port Scanner

Scanning attack is, in fact, sending a series of small packs to probe the target system. The nature of this attack is that it produces many network flows. This attack is made utilizing different hosts and through the different origin and destination ports. Scanning attacks categorized into three different groups [22]:

1- Vertical scan: abnormal behavior system does its measures on a specific port on many hosts.

2- Horizontal scan: unusual behaviors system sends its scanning packs on some ports of any particular port.

3- Block scan: different numbers of ports are scanned on different amounts of hosts by abnormal behaviors. In Figure 6. Shows Categorizing scanning attacks.

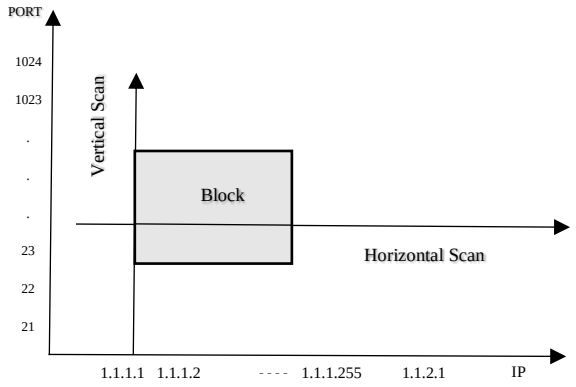

Figure 6. Categorizing scanning attacks

3.4 Botnet

During the Botnet attacks, a group of infected computers is led and controlled by a commander remotely. This network of infected computers is a suitable instrument to start vast attacks. It is difficult to identify this type of infected computers. Since by identifying and isolating the attack commander, other computers will not be dangerous anymore. But no other effective method hasn't been determined so far, and this research field is in elementary stages [23]. This type of attack is different from scanning and service limiter attacks is that to identify botnet attack, the network has to be observed for a long time to identify commander or infected computers under control. Although it is possible to identify in real-time during scanning and service limiter attacks.

In fact, most of the Botnet attacks managed by the IRC channel (a method of internet relay chat. IRC is mainly designed for group conversations, and conversations taken place in places called the channel. Also, person-to-person communication is possible through private chat). A network flow is identifiable through the data level, and there is no need to investigate sent traffic content.

4 INTRODUCING DIFFERENT INTRUSION DETECTION METHODS

To confront systems and computer network intruders, various methods known as intrusion detection methods have been created which are in charge of observing occurred events in a system or computer network. Detection methods used in intrusion detection systems are categorized into two general groups of signature-based or abuse-based and anomaly-based [24].

4.1 Signature-Based Intrusion Detection Method

This method, which is used in many successful intrusion detection systems, is a signature-based or pattern-matching intrusion detection system. Signature means a collection of principles that detects an attack that is being conducted. A group of rules loads the device, which is supposed to detect an intrusion. Each signature contains information that shows the device what to follow in passing data. When passing traffic compared with the existing pattern in signature, error message created to notice network manager of an intrusion. In many cases, IDS, besides notifying network manager, re-sets up a related connection to an intruder or confronts more with intervention utilizing a firewall or taking access control measures [24]. Since the signature-based method does not need learning from the environment, it is simple to implement it. This method acts upon passing packs research and compares from the network with attacks whose signatures are available in the database. This method works effectively in the exploration of unknown attacks whose signatures exist in the intrusion detection system database. But it is not able to detect new sentences whose signatures don't exist in the database, and to detect new attacks database with original attack signatures have to be updated [25]. This pre-processed architecture observed for finding and comparing activity patterns in the network environment with the existing signature in the comparative database, and an alarming message is sent. Since the signature-based intrusion, detection method identifies detected attacks with high reliability and low incorrect alert rate, this method has been used in many commercial intrusion detection systems. In Figure 7. Shows a general architecture for the signature-based process.

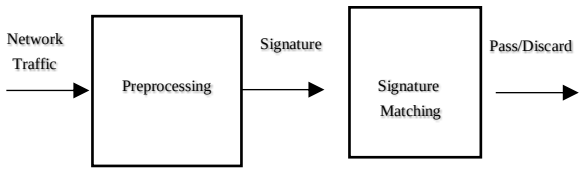

Figure 7. The architecture of signature-based intrusion detection [25].

4.2 Anomaly-based Intrusion Detection Method

It refers to detecting existing patterns in a given collection of information that doesn't conform with predetermined right (standard) behavior, so detected patterns are called anomalies, which often translated to vital and efficient information in several applied fields. Anomaly-bases intrusion detection method compares user's behavior with normal behavior saved in the database through statistical methods use it to detect unknown attacks, and tries to find activities, which are not compatible with typical behavior pattern and seem raucous and abnormal. In fact, to detect anomalies, a specific pattern has to be found; behaviors, which obey this pattern, discovered normal and devious ones are anomalies. An essential issue in this method is creating a view of normal behavior because users' normal behavior may change. Therefore, the intrusion detection system, which uses this method, has to update itself with these changes. Another issue in constructing a sample behavior model is selecting features that are used as input to build the model. Security experts determine input parameters in the present models, and there is no guarantee that all influential parameters in intrusion detection selected rightfully. If essential features dependent on intrusion have to be ignored wrongly, detecting attacks from normal behavior will be so difficult. In addition, not omitting features, which are not related to intervention, may decrease intrusion detection efficiency. The ability to detect new attacks is the strong point of this method, and the high incorrect alert rate is its weak point [24]. Detecting anomalies is one of the essential functions of data mining which identifies unusual and abnormal data or even specific and rare pattern in a data collection. An accepted definition of anomaly is observing a datum's high deviation from other data. Therefore, it

creates this possibility which maybe this datum has been produced by another mechanism. It is essential to detect anomaly because it may show a destructive activity in the system. For example, a network abnormal traffic pattern may reveal that a host has been hacked and its information sent to an illegal destination [23]. Because input data has a different kind, they have to be pre-processed. For example, regarding network traffic data inputs, the IP address of a hierarchical datum is three, and the protocol of a categorical datum is four. The port number is a numerical datum. Preprocessing methods are unique based on the anomaly detection method. After data pre-processing and preparation, anomaly detection methods (generally categorized into two groups of supervised and unsupervised) implemented on pre-processed and prepared data.

Despite so many methods in anomaly exploration in network traffic, there are also challenges in this field, such as [23]:

1- Absence of a comprehensive and practical method to explore anomaly. For example, wire anomaly detection in the network may not be so possible in a wireless network.

2- Noisy data may look like abnormal data, and it is difficult to distinguish them.

3- Since a normal behavior has to be continuously deducted so maybe a behavior won't remain in normal behavior group forever, therefore anomaly detection intrusion methods may not be useful in the future and as a result newer and more advanced intrusion detection methods are required, since intruders explore these methods and identify ways to overcome them.

Considering challenges in anomaly-based intrusion detection methods, many types of research and studies have been conducted in this field. Since supervised methods are based on knowledge, which is prepared by a supervisor, and an external factor and needs educational data (labeled data) thus, it is not able to detect unknown attacks and damages, today most of studies conducted in the field of active security systems, which try to detect attacks and damages without previous knowledge.

4.3 Hybrid Method

This method, which is usually a better one, intrusion detection system, use the advantages of both states. First, it finds the detected attack system based on signature-based method techniques. It uses the anomaly-based method for other new attacks, which doesn't have a pattern to identify them in its database [24].

5 INTRODUCTION ANOMALY-BASED INTRUSION DETECTION METHOD

5.1 Artificial Neural Network

The artificial neural network is an information processing unit which inspired by mid human function. Artificial neural networks are made up of the arbitrary number of nodes or neurons and link input collection to output, without previous knowledge about that phenomenon or system, they can learn complicated nonlinear relations between input and output variables in a system. Neural networks are divided into two groups of supervised and unsupervised. Generally, neural networks are organized in layers that are made up of some interconnected nodes, which include an activation function. Typically, neural networks can distinguish among neurons connection methods, different kinds of computing neurons operations, network transfer operation method, and their learning methods, including learning rate. Considering neurons intercommunications, it is possible to distinguish between layered and non-layered networks. Input data transferred through the input layer by hidden layers (middle layers) to the output layer. Links and contacts structure and number of layers and neurons determine network architecture, which has to be regulated before using neural networks. Although in specific cases, it is possible to use single-layer neural networks successfully, but, commonly, neural networks have at least three layers (input layer, hidden layer or middle layer and output layer). Artificial neural networks used for various learning functions such as real-valued function, discrete values, and vector function [26]. Multilayer Perception (MLP) neural networks are widely used in computer networks intrusion detection. This type of neural network can obtain approximation with the desired accuracy until each continuous function contains enough hidden units. It means that such models can construct a definite issue decision boundary in features space, and so they act as nonlinear split

function. When a neural network is used to categorize passing packs through the network, there is an input node for each feature vector element, and usually, there is an output node for each class that feature will belong to it. Hidden nodes are connected input nodes which weights are assigned to these connections. These weights are modified during the teaching process. MLP neural network is a learning algorithm with the back-propagated rule. This is a gradient Descent Method, which shows the difference between computing by network and expected output by an error function. This error function is based on Mean Squared Error (MSE). MSE can be calculated for the completely educational data collection. To achieve successful learning, real network output has to approximate expected output with constant value reduction of this error. The back-propagated rule calculates the error for each input and releases error from one layer to the previous one. Nodes connection weights are equal with or based on back-propagated error, and so reduce neural network education error. Input and output layers and neural hidden cells are variable. Input and output neurons vary based on input and output vectors, and the number of hidden layer neurons is based on expected efficacy. And the more the number of hidden layer neurons be, the more complicated the MLP neural network will be [25].

The learning process in intrusion detection systems based on the neural network contains these three stages [25].

1- Data collection: using the automatic analyzer to process TCP/IP raw data collected from network and transforming it into a perceptible form for the machine utilizing criterion collection, including network analyzed connection records and data.

2- Teaching: a neural network is taught for different kinds of attack, and normal behavior and output contains two values: intrusion and normal data.

3- Test: running on a test data collection.

Neural networks in intrusion detection systems used to categorize attack patterns and normal behavior and also to determine the type of attack. It takes time to teach neural networks due to the high amount of data (educational vectors). However, when neural networks parameters determined in the teaching process, categorizing a record conducted rapidly and in a short time. Therefore, neural networks in intrusion detection can act as an instant categorization to detect the type of attack for which they have been taught. The time needed to collect the necessary information to compute features is the only factor that makes neural networks to act in an offline state [25].

5.2 Fuzzy Logic

Fuzzy logic is has been derived from a fuzzy set. According to this theory, the reasoning is approximate instead of deriving reasoning exactly from classic logic propositions. Fuzzy methods are used to detect anomalies, and the feature can be considered as fuzzy variables. In fuzzy logic space, a thing is allowed to belong to more than one class at a specific time. This concept is useful when the difference between classes is not defined well [25]. During intrusion detection, there is an $m+1$ class in which everything has to be categorized. Among these classes, there is a particular class called normal behavior class, and the rest of m classes are related to attacks (based on detected intrusion and attacks). Data set includes things (for example, data set be a table, the thing here means table records), which everything has $n+1$ features and is used by learning algorithms. First, n features determine the characteristics of a thing and the last features of a class to which the thing belongs. Therefore, the fuzzy categorizing system must have an $m+1$ member set of rules to solve intrusion detection issues, which one of them relates to normal class and class m related to abnormal and attack. In this system, conditions part defined by observed parameters and conclusion part is an irresolvable phrase for categorization feature. Deduced fuzzy rules do not use more than five features in the construction of a rule, which simplifies the description of normal, and abnormal (attack) behaviors. More simple fuzzy rules have distinct and important advantages in real programs. First, rules are interpreted more simple, and second, a categorization is rapidly implemented, which is based on fuzzy rules. It is important to note that it is complicated and difficult to deduce from data with many features. Although fuzzy logic

effectiveness in intrusion detection and especially in port scan attacks detection and scanning attacks is confirmed, it takes a lot of resources and time to teach as its main weak point.

5.3 Genetic Algorithm

The genetic algorithm is a searching method inspired by biological evolution and natural genetic, which introduces an approximate answer, which is an approximate solution for the optimization issue. A genetic algorithm is called a general searching method, which copies natural biological rules. The genetic algorithm applies conservation law on a series of problem answers to achieve better answers. In each generation utilizing selection process compatible with answers, value, and reproduction of selected answers utilizing actors have been imitated from natural genetics, better approximations achieved for the final answer [27]. The process usually begins with random population reproduction from chromosomes, which contains all possible answers to an issue which issue candidate answer is among these answers. Each chromosome's different locations are numbered as the bit. These locations can be referred to as genes. An evaluation function computes the priority of each chromosome based on a possible solution. This function is called a fitness function. During the evaluation, the merge operator used to simulate natural reproduction and mutation operator is used for species mutation. It is necessary to move to proper chromosomes for survival, and the combination of selected chromosomes and proper chromosome s have to be combined. When a genetic algorithm used to solve different problems, these three factors influence algorithm efficiency. 1. Fitness function 2. Individuals' agency, 3. Genetic algorithm parameter [28]. The genetic algorithm begins with chromosomes" randomly reproduced population. Then utilizing different methods, this population increases, and chromosomes improve. Before running a genetic algorithm, suitable coding (show) has to be found for the considered problem. Binary strings are the most common method to show chromosomes in genetic algorithms. Each decision variable becomes binary, and then a chromosome is created by variables juxtaposition. In addition, a fitness function has to be invented to relate value to each coded solution. During algorithm running, parents are selected for reproduction, are combined with mutation, and merge operators to reproduce new children. This process repeats several times to the population of the next generation is produced. Then this population is investigated, and if convergence principles are met, the process mentioned above will be ended. Convergence happens when a constant percent of rows and columns of a matrix becomes identical [29].

The genetic algorithm used in the intrusion detection system has two modules; each of them works in a specific stage. In the teaching stage, a set of categorized rules is constructed based on network data and utilizing a genetic algorithm in an offline environment. In the intrusion detection stage, constructed rules in the teaching stage are used to categorize input connections and input data to network in the areal-time environment [28].

A genetic algorithm is used for deducing new rules for the intrusion detection system. Using these rules separates normal network traffic from abnormal traffic (attack). Rules in a genetic algorithm rule set are in the form of if-then. Genetic algorithm rule explanation:

```
If {condition} than {act}
```

Condition is related to the data that has to be investigated, and if the rule condition is true, the act is a reaction that has to be done. A condition is investigated for network protocols port numbers, used protocols, connection duration, origin, and destination IP address. The act is related to reactions such as sending the alert message and generating log messages when the condition is true [29].

Different network features such as connection duration used protocols, origin and destination ports, and attack names are used to investigate intrusion detection. For instance, if six first features connect by logical AND operations to construct condition rule, then the feature of attack name turns into the rule act part. The following simple example categorizes a network connection as the denial of Neptune service attack:

```
If (duration = "0:0:1" and protocol = "finger" and source_port=18181 and destination_port =91 and (attack_name = "Neptune") than source_ip= "11.11.11.11" and destination_ip = "112.168.214.10")
```

After producing classification rules, fitness rules used in the previous stage to determine rules competency and suitability:

Each rule is shown with if A Then B condition, its accuracy, which is expressed as fitness, is represented as the following equation:

```
Fitness=w1* support + w2* confidence
support = | A and B | / Nconfidence = | A and B | / | A|
```

Here N is the total number of connections in under investigation network, A is the total number of network connections compatible with A condition, and A and B is the total number of network connections that are compatible with if A Then B rule. $1w$ and $2w$ weights also used to control the balance between two phrases of support and confidence [29]. The genetic algorithm's strong point is the ability to extract the best classification rules and to select optimal parameters. Its weak point is that it is unable to have a constant optimal pass time for sure, and data over-fitting is another problem. In Figure 8. Shows the simple stages of a genetic algorithm in intrusion detection systems.

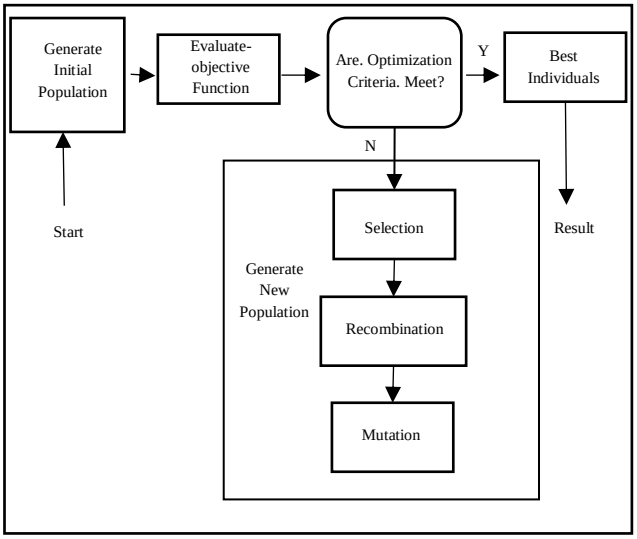

Figure 8. Genetic algorithm in intrusion detection systems

5.4 Data Mining Methods:

Different methods of data mining, such as statistical methods and machine learning are used to pre-process collected data from the network and also to investigate network data to detect anomalies which result in network intrusion detection. Although it is possible to use unsupervised machine learning methods for intrusion detection since most of the conducted studies in the field of intrusion detection labeled data sets are used so supervised methods have better efficiency in these data sets. These methods are introduced and compared with each other in the following:

5.4.1 Statistical Methods

Generally, statistical purposes make statistical models (for normal behavior) then a statistical deduction test used to determine whether a new model belongs to this model or not. Cases with low probability to be produced based on a regular model consider as an anomaly. Both parametric and nonparametric statistical methods used to detect abnormality in statistical model designing. These methods are a signal processing method and principal components analysis method [30].

5.4.1.1 Clustering

Clustering refers to unsupervised learning algorithms that can cluster data based on similar data without pre-labeled educational data. Although there are different types of clustering methods, two methods of normal clustering and co-clustering are used to detect anomalies in the network [23]. Processing rows and columns are the differences between normal and co-clustering methods. Normal clustering like k-means method clusters based on rows values while in co-clustering data set columns and rows cooperate in the production of groups synchronously. This method can produce a c cluster from the C column of the primary data set and also r cluster from R row of the original data set. Despite other clustering methods, co-clustering defines a clustering criterion and then optimize it. This method finds sub-sets synchronously from data set matrix columns and rows utilizing the determined rule. Advantages of co-clustering rather than normal clustering are:

1- Columns and rows synchronous clustering may represent a more compact show while maintaining the primary information.

2- Co-clustering may be used as a dimension's reduction method, and it is useful to generate new features.

3- Co-clustering significantly reduces computing complexities. For example, the k-means algorithm has $O\,(mnk)$ time complexity in which m is the number of rows, n number of columns, and k number of clusters. In co-clustering with O $(mkl + nkl)$ time complexity l is the number of clusters columns, and it is evident that: $O\,(mkl + nkl) < O\,(mnk)$

There are three general hypotheses to use clustering to detect anomalies [23]:

- Hypothesis 1: when there is a set of normal data and clusters formed based on this data set, new data that is not able to adapt with none of these clusters is considered an anomaly. For example, since density-based clustering algorithms do not consider noisy data density, new noisy data is considered as an anomaly.
- Hypothesis 2: When a cluster contains both normal and abnormal data, it has been observed that standard data are near to the center while normal data are far from the cluster center. Based on this hypothesis, abnormal events are identified by a distance score.
- Hypothesis 3: in clustering with different produced cluster sizes, clusters with smaller size and more scattered data are considered as an anomaly, and big and massive clusters are normal clusters. Cases, which are belonged to a group, and their size and density, is smaller than the threshold level may be considered an anomaly.

5.4.2 Machine Learning Methods

Machine learning techniques are suitable when there is not preliminary knowledge about data patterns; for this reason, sometimes they are called bottom-up methods. The critical advantage of this method is that it usually does not need experts to determine considered requirements to detect intrusion, so they are so fast and economical.

5.4.2.1 Decision Tree

The decision tree is one of the classified algorithms in data mining. Detailed algorithms learn how to generate a model out of an educational data set. Classification may be considered as a mapping from a set of features to a specific class. A tree is a predictive modeling method that generates trees, structural models, from existing patterns in education, data utilizing statistical methods, and machine learning. The decision tree is preliminarily made up of pre-classified data. The most important issue in the decision tree is the selection of features from the educational data set, which generates the best data items separation to different classes. Based on these features values, data are separated. This process is used as a reflection from each sub-set of data items. When all data items in the present data sub-set placed in a class to which they have belonged, the process has been stopped. A node from the decision tree determines that its data has been divided. Each tree node has several crests that are labeled based on possible feature value in the parent node. One peak connects two nodes or connects a node and a leaf. Leaves are marked with the same decision value for data classification [31]. The main advantage of decision tree rather than other classification methods is that this method produces a set of visible and perceptible rules, which are used simply in real-time security systems such as intrusion detection systems and a firewall. Decision trees work well in big data sets, which is an important advantage of in-network data with high volume. In addition, these models can be used as rule-based models with the least processing. The decision tree's accuracy generalization is another useful feature for intrusion detection models. There are always new attacks in the system, which have slight differences with detected attacks, and detected attacks with small changes are built on them. Due to decision trees' accuracy generalization, it is possible to detect such attacks by this type of intrusion detection. Demanding high calculations to constructing a decision tree is this methods' weak point [31].

5.4.2.2 Bayesian Networks

Bayesian networks are powerful instruments to classify, make decisions, and reasoning in uncertainty conditions. Naïve Bayes is a simple form of Bayesian networks that has an efficient mechanism for deduction development. This model is generated based on probable relations

among variable orientations, and this method is generally used in combination with other statistical designs. Bayesian networks have various advantages, including the ability to codify dependency between variables, predicting events, and creating a relationship between previous knowledge and present events. Bayesian networks have been recently used due to their high ability to obtain integrated results from probable information about a situation and or a condition in different computer sciences branches [32].

The Bayesian network is a model that codifies probable relationships between variables. Generally, this method is used in combination with statistical designs in intrusion detection systems. Naïve Bayesian algorithm (NB) is for machine learning in which there are educational data set with labels and predetermined target class. Educational data set is defined with $A1\ to\ An$ feature, and each function is shown with a1, a2…. An feature values depend on related class C. the objective of a sample classification has not been observed, class values aren't determined and feature values are determined that is establishing a class related to a sample is based on that sample values and features. The Bayesian approach in unobserved samples classification is to assign the sample to a level that example has the most probability to belong to that class. Codifying probable relationships between variables of different parts and the ability to combine previous knowledge about dependency between variables with present educational data is one of the main advantages of Bayesian networks. This classification method enjoys high accuracy in classification in the case that informative information is correct and without error. Difficulty in the use of continuous features is one of the disadvantages of this method. Also, if previous knowledge contains a mistake, there will be no guaranty to train a proper classification [32].

5.5 Support Vector Machines Method (SVMs):

SVM is one of the supervised learning methods, which is used for classification and regression. This method is among almost new ways that show excellent efficiency rather than other older methods in classification. SVM classifier work based on data linear classification and in data direct division effort has been made to select a line with more safety margin. SVM takes input features with real values with nonlinear mapping to a space with higher dimensions and separates data by putting a linear border. Finding a separation border to separate data has been changes into quadratic optimization, and the linear border is used for division. However, not all issues such as essential functions are separated linearly, and SVM used to solve this problem. These functions transform linear functions into nonlinear ones and make the direct separation, possibly by taking data into a space with higher dimensions [33]. Each sample depicts data as a point in the next n-space on data dispersion chart (N is the number of features the data sample has), and feature value related to information determines one of point coordinates on the table. Then it classifies different and discrete data from each other by depicting a straight line [33]. In SVM, only data in support vectors are the bases of machine learning and model construction, and this algorithm is not sensitive to other data points. Its purpose is to find the best border between

Data to have the possible distance from different classes (their support vectors).

- Such an algorithm has innate limitations. For example, how to determine parameters for each mapping function has not been recognized yet.
- Support vector-based machines need complicated and time-consuming calculations and consume high memory because of computational complexity.
- Discrete and non-numerical data are not consistent with this method and have to be transformed.

However, SVMs have an integrated theoretical basis, and their produced answers are general and unique. Today, support vector machines have been transformed into the most common prediction techniques in data mining [17]. In Fig.9 shows the vector machine architecture.

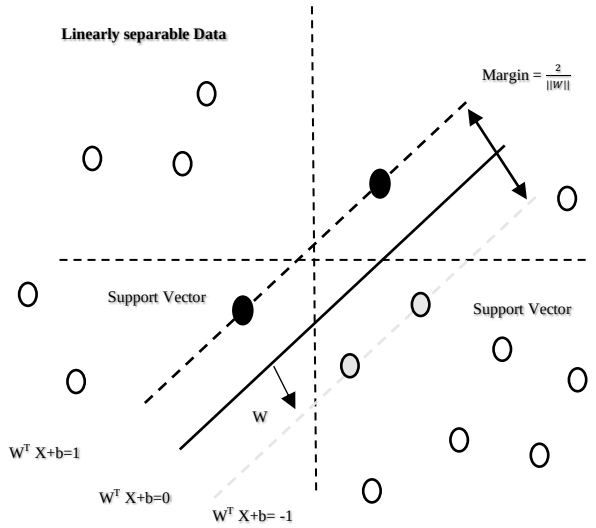

Figure 9. Support vector machine method in intrusion detection systems [17].

6 COMPARING USED METHODS IN INTRUSION DETECTION

Table 1. Comparing anomaly-based methods in intrusion detection systems

NO.	Study	Purpose	Outcomes
1	Barbara et al. [34]	Abuse detection following anomaly detection.	Improving the reliability of hardware and software components, improving the robustness of a model in machine learning and data mining.
2	Ansam Khraisat et al. [35]	A hybrid IDS (HIDS) combining the C5 decision tree classifier and One Class Support Vector Machine (OC-SVM).	The proposed HIDS is evaluated using the benchmark datasets, namely, Network Security Laboratory Knowledge Discovery in Databases (NSL-KDD) and Australian Defense Force Academy (ADFA) datasets. Studies show that the performance of HIDS is enhanced, compared to SIDS and AIDS in terms of detection rate and low false-alarm rates.
3	Ajith Abraham [36]	Decision trees (DT) and support vector machines (SVM).	Empirical results illustrate that the proposed hybrid systems provide more accurate intrusion detection systems.
4	Ren Hui Gong [37]	Genetic algorithm.	Experimental results show the achievement of acceptable detection rates based on benchmark DARPA data sets on intrusions, while no other complementary techniques or relevant heuristics are applied.
5	Kim et al. [38]	Neural hybrid network, detecting hidden anomaly abuse.	They implemented the IDS classifier based on LSTM-RNN and evaluated the IDS model. By comparing it to other IDS classifier, the

			attacks are well detected by LSTM-RNN classifier.
6	Mazini et al.[39]	Artificial bee colony (ABC) and AdaBoost algorithms.	Demonstrated that all sequential properties (1st, 2nd, 3rd order Markov models) are beneficial, and a combination of them via VLMM leads to accurate prediction. The proposed indicators are information-based metrics, i.e., entropy and log-loss.
7	Muhammad Hilmi Kamarudin et al.[40]	Unified Intrusion Anomaly Detection (UIAD).	Detection time can be drastically reduced, since the new entry traffic can be matched with benign/malicious signatures generated from the previous detection. Moreover, the proposed unified approach can potentially be evaluated online using larger, as well as the latest, encrypted sets of traffic.

Table 2. Comparing conducted methods in the field of security condition knowledge in intrusion detection systems

NO.	Study	Purpose	Outcomes
1	Q. Wu et al. [41]	Dynamic Bayesian network.	The findings reveal that the method can identify the intrusion intention of the intruder from various alarm messages and predict further attacks with good real-time characteristics and inferential capability for undetermined attacks.
2	Hu et al. [42]	Bayesian network.	Both the filter layer and the game layer deal with the same noisy observations in iterative Bayesian inference framework. The key idea of this method can be generalized to other filters such as RLS and Kalman, etc.

Table 2. part 2

NO.	Study	Purpose	Outcomes
3	Dan Shen et al., [43]	Game theory.	The network security system was evaluated and protected from a perspective of data fusion and adaptive control. Game theory, data combining, and data mining are used to gain knowledge about security conditions.
4	Varun Dutt et al., [44]	Sample-based learning.	Based upon model predictions, a defender's prior threat experiences and his or her tolerance to threats are likely to predict detection accuracy; but considering the nature of adversarial behavior is also important.
5	Sushil Jajodia et al., [45]	Localized Encryption and Authentication Protocol (LEAP+).	performance analysis shows that LEAP+ efficient in terms of computational, communication, and storage costs.
6	Shanachie, J. Yang et al., [46]	Markov's length variable models.	Result demonstrate that sequential properties, i.e., the 1st, 2nd, 3rd, order Markov models, are all beneficial, and a combination of them via VLMM leads to the best prediction accuracy. Information theory based metrics, such as entropy and log-loss, are proposed as indicators of the prediction quality.
7	Judson, Dressler et al., [47]	Operational data classes.	Introducing six classes of necessary information (threatening environment, unusual activity, vulnerability, key ground, operational readiness and ongoing operation) effectively activates and empowering commanders and government leaders as a

			symbol of cyberspace to make decision-making process.
8	Moyinoluw, Abidemi, Bode et al., [48]	Bayesian network classification and genetic algorithm.	comparison of the Bayes model with Association Rule Mining model shows efficient performance, and an improved performance with a Genetic Algorithm technique.
9	Wei Yi et al., [49]	Computational cloud-based architecture	To effectively parallel cloud based threat detection that integrates both signature based detection and anomaly based detection.
10	S. Mathew et al. [50]	Classification of attack alerts utilizing Snort	This scheme into a real-time attack detection framework and prototype presented by the authors in previous work and provide some results from testing against multistage attack scenarios. It has been shown that it improves temporary awareness about multistage attacks effectively.

Table 3. Comparing fault tolerance methods in intrusion detection systems

NO.	Study	Purpose	Outcomes
1	Huet & Malik [51]	Virtual multiple machines	The proposed scheme is a good option to be used as a fault tolerance mechanism for real time computing on cloud infrastructure. It has a dynamic behavior of reliability configuration and highly fault tolerant. It does not suffer from domino effect as check pointing is made in the end when all the nodes have produced the result.

Table 3. part2

NO.	Study	Purpose	Outcomes
2	p. Garraghan et al.,[52]	Fault-Tolerant - Federated Cloud platform (FT-FC)	The development of a cloud framework called the FT-FC, which allows itself to quickly create a variety of tolerant systems based on the Byzantine fault and apply them to common clouds, and have produced preliminary results to illustrate the feasibility and potential of this approach. In addition to identifying a number of research problems and challenges that need to be addressed in order to advance this area more.
3	Dr. Lakshmi [53]	Investigating different patterns	The investigation of various types of faults. In contrast, methods for error tolerance such as point research, migration, replication, etc. were investigated.
4	Elham Shamsinezad [54]	Investigating different algorithms and explaining migration methods(Pre-copy and Post-copy)	Results of simulation done by MATLAB software shows that proposed approach leads to overload reduction of server system. Finally, to demonstrate the performance of the proposed approach in terms of transforming time and overload will be assessed and compared with methods of Post-Copy and Yu.
5	Haiying Qi [55]	Neural network	Compared with the existing methods, the proposed method achieved fault tolerant control for time-varying fault, rather than just constant fault. This greatly expands the industrial applications of the developed method to enhance system reliability. The simulation results

			demonstrated that the post-fault is stable and the performance is maintained.

7 RESEARCHES ANALYSIS

Practically, no system does not have full security IDS system has gained an excellent position for intrusion detection in network structure in time and is essential in the networks. Meanwhile, researchers who are looking for different methods to fulfill this need explore and design different types of transmission modes, statistical purposes, data mining, and neural networks systems.

At present, the most crucial issue is to gain knowledge about the network security process, which is influenced by hardware, software, and network users' behavior. A condition believability is acquired by conditional estimation, and high-level information merge. Now the most challenging issue in combining high-level information to achieve knowledge about the future condition and evaluating cyber-attacks effect attacks visualization modeling with four parameters of behavior, opportunity, capability, and will.

Fault tolerance is one of the main concerns in availability guarantee and operating practical programs. To minimize destruction effect on system and running practical programs correctly and successfully, destruction has to he predicted and managed and controlled actively. Fault tolerance methods are, in fact, in charge of predicting these destructions and taking a proper measure before removal.

8 CONCLUSION

As mentioned earlier, guaranteeing existing data security is the most crucial challenge of cloud computing. Nowadays, protecting from cloud performance on the internet considered a big challenge, and many solutions have been employed for data security in cloud computing. As observed in this study, various methods invented to confront probable attacks to comfort cloud servers from their users' personal and organizational data protection. However, these methods are not complete.

On the other hand, cloud computing has been discussed in new communities and organizations. Big companies are moving towards cloud computing environments, sometimes departments leave their costly operations with cloud environments, and in fact, they are outsourcing them. Therefore, cloud environment architecture has to be standard and compatible with trustful rules.

REFERENCES

[1] A. Joshua and F. Ogwueleka, “Cloud Computing with Related Enabling Technologies,” *Int. J. Cloud Comput. Serv. Sci.*, vol. 2, no. 1, pp. 40–49, 2012, doi: 10.11591/closer.v2i1.1720.

[2] V. D. Kale, “Recent Research Trends in Cloud computing,” vol. 6, no. 2, pp. 406–409, 2013.

[3] A. Boukerche *et al.*, “A new solution for the time-space localization problem in wireless sensor network using UAV,” in *Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications - DIVANet ’13*, 2013, pp. 153–160, doi: 10.1145/2512921.2512937.

[4] S. Fleck and W. Straßer, “Smart camera based monitoring system and its application to assisted living,” *Proc. IEEE*, vol. 96, no. 10, pp. 1698–1714, 2008, doi: 10.1109/JPROC.2008.928765.

[5] W. Schriebl, T. Winkler, A. Starzacher, and B. Rinner, “A pervasive smart camera network architecture applied for multi-camera object classification,” in *2009 Third ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC)*, 2009, pp. 1–8, doi: 10.1109/ICDSC.2009.5289377.

[6] B. Rinner, T. Winkler, M. Quaritsch, B. Rinner, W. Schriebl, and W. Wolf, *The evolution from single to pervasive smart cameras Epigenetic regulation of stress induced drug tolerance View project VECTO-Vehicle Energy Consumption Calculation Tool View project THE EVOLUTION FROM SINGLE TO PERVASIVE SMART CAMERAS*. 2008.

[7] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, “Wireless multimedia sensor networks: applications and testbeds,” in *Proceedings of the IEEE*, 2008, vol. 96, no. 10, pp. 1588–1605, doi: 10.1109/JPROC.2008.928756.

[8] M. Quaritsch, B. Rinner, and B. Strobl, “Improved agent-oriented middleware for distributed smart cameras,” *2007 1st ACM/IEEE Int. Conf. Distrib. Smart Cameras, ICDSC*, no. May 2014, pp. 297–304, 2007, doi: 10.1109/ICDSC.2007.4357537.

[9] P. Chen *et al.*, “Citric: A low-bandwidth wireless camera network platform,” in *2008 2nd ACM/IEEE International Conference on Distributed Smart Cameras, ICDSC 2008*, 2008, doi: 10.1109/ICDSC.2008.4635675.

[10] A. Doblander, A. Zoufal, and B. Rinner, "A novel software framework for embedded multiprocessor smart cameras," *ACM Trans. Embed. Comput. Syst.*, vol. 8, no. 3, pp. 1–30, Apr. 2009, doi: 10.1145/1509288.1509296.

[11] P. Saastamoinen, S. Huttunen, V. Takala, M. Heikkilä, and J. Heikkilä, "Scallop: An open peer-to-peer framework for distributed sensor networks," in *2008 2nd ACM/IEEE International Conference on Distributed Smart Cameras, ICDSC 2008*, 2008, doi: 10.1109/ICDSC.2008.4635712.

[12] S. A. M. Sharif and V. Jeoti, "Video wireless sensor network: Co-operative vision based localization method," in *Proceedings - 2nd Asia International Conference on Modelling and Simulation, AMS 2008*, 2008, pp. 570–573, doi: 10.1109/AMS.2008.77.

[13] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, "The evolution of MAC protocols in wireless sensor networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 101–120, 2013, doi: 10.1109/SURV.2012.040412.00105.

[14] W. Feng, Q. Zhang, G. Hu, and J. X. Huang, "Mining network data for intrusion detection through combining SVMs with ant colony networks," *Futur. Gener. Comput. Syst.*, vol. 37, pp. 127–140, 2014, doi: 10.1016/j.future.2013.06.027.

[15] V. Jecheva and E. Nikolova, "Some clustering-based methodology applications to anomaly intrusion detection systems," *Int. J. Secur. its Appl.*, vol. 10, no. 1, pp. 215–228, 2016, doi: 10.14257/ijsia.2016.10.1.20.

[16] Y. Mehmood, M. A. Shibli, U. Habiba, and R. Masood, "Intrusion detection system in cloud computing: Challenges and opportunities," in *Conference Proceedings - 2013 2nd National Conference on Information Assurance, NCIA 2013*, 2013, pp. 59–66, doi: 10.1109/NCIA.2013.6725325.

[17] J. Jaiganesh, S. Mangayarkarasi, and P. Sumathi, "Intrusion Detection Systems: A Survey and Analysis of Classification Techniques," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 4, pp. 1629–1635, 2013.

[18] S. R. Snapp, S. E. Smaha, D. M. Teal, and T. Grance, "The DIDS (Distributed Intrusion Detection System) Prototype," *Proc. Summer USENIX Conf.*, pp. 227–233, 1992.

[19] J. Nikolai and Y. Wang, "Hypervisor-based cloud intrusion detection system," in *2014 International Conference on Computing, Networking and Communications, ICNC 2014*, 2014, pp. 989–993, doi: 10.1109/ICCNC.2014.6785472.

[20] K. K. Basu, "Organisational culture and leadership in ERP implementation," *Int. J. Strateg. Chang. Manag.*, vol. 6, no. 3/4, p. 292, 2015, doi: 10.1504/IJSCM.2015.075919.

[21] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, no. April, pp. 27–33, 2010, doi: 10.1109/AINA.2010.187.

[22] N. Azizi, J. Karimpour, and F. Seifi, "HCTE: Hierarchical Clustering based routing algorithm with applying the Two cluster heads in each cluster for Energy balancing in WSN," *Int. J. Comput. Sci. Issues*, vol. 9, no. 1, pp. 57–61, 2012.

[23] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60. pp. 19–31, 2016, doi: 10.1016/j.jnca.2015.11.016.

[24] S. Vijayarani and R. Kalaivani, "Intrusion Detection System – A Survey," *Int. J. Bus. Intelligents*, vol. 004, no. 002, pp. 57–61, 2015, doi: 10.20894/ijbi.105.004.002.001.

[25] J. Singh and M. J. Nene, "A Survey on Machine Learning Techniques for Intrusion Detection Systems," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 11, pp. 4349–4355, 2013.

[26] N. Farah, M. Avishek, F. Muhammad, A. Rahman, M. Rafni, and D. Md., "Application of Machine Learning Approaches in Intrusion Detection System: A Survey," *Int. J. Adv. Res. Artif. Intell.*, vol. 4, no. 3, 2015, doi: 10.14569/ijarai.2015.040302.

[27] V. K. Kshirsagar, S. M. Tidke, and S. Vishnu, "Intrusion Detection System using Genetic Algorithm and Data Mining : An Overview," *Int. J. Comput. Sci. Informatics*, vol. 1, no. 4, pp. 91–95, 2012.

[28] M. M. Hassan, "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 1, no. 7, pp. 1435–1445, 2013.

[29] A. Rehman and T. Saba, "Evaluation of artificial intelligent techniques to secure information in enterprises," *Artif. Intell. Rev.*, vol. 42, no. 4, pp. 1029–1044, 2014, doi: 10.1007/s10462-012-9372-9.

[30] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.

[31] M. Kumar, M. Hanumanthappa, and T. V. S. Kumar, "Intrusion Detection System using decision tree algorithm," in *International Conference on Communication Technology*

Proceedings, *ICCT*, 2012, pp. 629–634, doi: 10.1109/ICCT.2012.6511281.

[32] H. Altwaijry and S. Algarny, "Bayesian based intrusion detection system," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 24, no. 1, pp. 1–6, 2012, doi: 10.1016/j.jksuci.2011.10.001.

[33] M. N. Mohammed and N. Sulaiman, "Intrusion Detection System Based on SVM for WLAN," *Procedia Technol.*, vol. 1, pp. 313–317, 2012, doi: 10.1016/j.protcy.2012.02.066.

[34] D. Barbará, J. Couto, S. Jajodia, and N. Wu, "ADAM: A testbed for exploring the use of data mining in intrusion detection," *SIGMOD Rec.*, vol. 30, no. 4, pp. 15–24, 2001, doi: 10.1145/604264.604268.

[35] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine," *Electronics*, vol. 9, no. 1, p. 173, Jan. 2020, doi: 10.3390/electronics9010173.

[36] S. Peddabachigari, A. Abraham, C. Grosan, and J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems," *J. Netw. Comput. Appl.*, vol. 30, no. 1, pp. 114–132, 2007, doi: 10.1016/j.jnca.2005.06.003.

[37] R. H. Gong, M. Zulkernine, and P. Abolmaesumi, "A software implementation of a genetic algorithm based approach to network intrusion detection," *Proc. - Sixth Int. Conf. Softw. Eng., Artif. Intell. Netw. Parallel/Distributed Comput. First ACIS Int. Work. Self-Assembling Wirel. Netw., SNPD/SAWN 2005*, vol. 2005, no. June 2005, pp. 246–253, 2005, doi: 10.1109/SNPD-SAWN.2005.9.

[38] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," in *2016 International Conference on Platform Technology and Service (PlatCon)*, 2016, no. September 2017, pp. 1–5, doi: 10.1109/PlatCon.2016.7456805.

[39] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 31, no. 4, pp. 541–553, Oct. 2019, doi: 10.1016/j.jksuci.2018.03.011.

[40] M. H. Kamarudin, C. Maple, T. Watson, and N. S. Safa, "A New Unified Intrusion Anomaly Detection in Identifying Unseen Web Attacks," *Secur. Commun. Networks*, vol. 2017, pp. 1–18, 2017, doi: 10.1155/2017/2539034.

[41] Q. Wu, R. Zheng, G. Li, and J. Zhang, "Intrusion intention identification methods based on dynamic Bayesian networks," *Procedia Eng.*, vol. 15, pp. 3433–3438, 2011, doi: 10.1016/j.proeng.2011.08.643.

[42] M. Zhai, H. Feng, T. Yang, and B. Hu, "Recursive filters with Bayesian quadratic network game fusion," in *2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2015, pp. 463–467, doi: 10.1109/GlobalSIP.2015.7418238.

[43] D. Shen, G. Chen, J. B. Cruz, Jr., L. Haynes, M. Kruger, and E. Blasch, "A Markov game theoretic data fusion approach for cyber situational awareness," *Multisensor, Multisource Inf. Fusion Archit. Algorithms, Appl. 2007*, vol. 6571, no. 65710, p. 65710F, 2007, doi: 10.1117/12.720090.

[44] V. Dutt, Y. S. Ahn, and C. Gonzalez, "Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory," *Hum. Factors*, vol. 55, no. 3, pp. 605–618, 2013, doi: 10.1177/0018720812464045.

[45] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 2, no. 4, pp. 62–72, 2003.

[46] S. J. Yang and D. Fava, "Characterizing Cyber Attacks through Variable Length Markov Models," pp. 1–10.

[47] J. Dressler, C. L. Bowen, W. Moody, and J. Koepke, "Operational data classes for establishing situational awareness in cyberspace," *Int. Conf. Cyber Conflict, CYCON*, vol. 2014, pp. 175–186, 2014, doi: 10.1109/CYCON.2014.6916402.

[48] B. M. Abidemi, A. B. Kayode, T. A. Favour-Bethy, and I. Otasowie, "A bayesian network model for risk management in cyber situation," *Lect. Notes Eng. Comput. Sci.*, vol. 1, pp. 434–441, 2014.

[49] W. Yu, G. Xu, Z. Chen, and P. Moulema, "A cloud computing based architecture for cyber security situation awareness," in *2013 IEEE Conference on Communications and Network Security, CNS 2013*, 2013, pp. 488–492, doi: 10.1109/CNS.2013.6682765.

[50] S. Mathew, D. Britt, R. Giomundo, S. Upadhyaya, M. Sudit, and A. Stotz, "Real-time multistage attack awareness through enhanced intrusion alert clustering," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2005, pp. 1–6, 2005, doi: 10.1109/MILCOM.2005.1605934.

[51] S. Malik and F. Huet, "Adaptive Fault Tolerance in Real Time Cloud Computing," in *2011 IEEE World Congress on Services*, 2011, pp. 280–287, doi: 10.1109/SERVICES.2011.108.

[52] P. Garraghan, P. Townend, and J. Xu, "Universities of Leeds , Sheffield and York Byzantine Fault-Tolerance in Federated Cloud Computing," pp. 280–285, 2011.

[53] L. P. Saikia and Y. L. Devi, "Fault tolererance techniques and algorithms in cloud system," *Int. J. Comput. Sci. Commun. Networks*, vol. 4, no. 1, pp. 1–8, 2014.

[54] E. Shamsinezhad, A. Shahbahrami, A. Hedayati, A. K. Zadeh, and H. Banirostam, "Presentation Methods for Task Migration in Cloud Computing by Combination of Yu Router and Post-Copy," vol. 10, no. 4, pp. 98–102, 2013.

[55] H. Qi, Y. Shi, S. Li, Y. Tian, D.-L. Yu, and J. B. Gomm, "Fault tolerant control for nonlinear systems using sliding mode and adaptive neural network estimator," *Soft Comput.*, vol. 8, Dec. 2019, doi: 10.1007/s00500-019-04618-8.