DETECTION OF ABNORMAL BEHAVIOR OF THE SYSTEM AND INCREASE THE SECURITY OF CLOUD COMPUTING BASED ON EVOLUTIONARY ALGORITHM

Payam Shojaeian Zanjani¹, Saeed Ebrahimi Nejad Motlagh Tehrani²

¹Faculty of Computing & Informatics, Multimedia University MMU, Cyberjaya, Malaysia
²Amirkabir College of Management and Technology, University of Applied Sciences and Technology UAST, Tehran, Iran

Corresponding Author: Payam Shojaeian Zanjani
Corresponding Author: Email: payam_shojaeian@yahoo.com

https://doi.org/10.26782/jmcms.2019.12.00016

Abstract

In the present era, we have a new method called cloud computing, in which the services are shared over the Internet. There are many organizations that provide cloud processing services. Cloud processing allows users and developers to use these services without interfering with the technical knowledge or control of the technology they require, but on the other hand, day to day, more information of individuals and companies is stored inside clouds, which puts the challenge of data security ahead of users. Information security in virtual environments and new area of cloud computing has always been emphasized as one of the basic infrastructures and essential requirements for ICT-intensive use. Although absolute security is unattainable both in the real environment and in the virtual environment, it is possible to create a level of security that is sufficiently adequate in almost all environmental conditions. In cloud computing, there are many security challenges that must be addressed by cloud service providers to convince users to use this technology. One of the most important issues is ensuring the user's data is inaccurate and unavailable. For the user, the security process used to store data in the cloud is very obscure, long, and vague. In this research, a security approach based on abnormal behavior is designed to detect events that are unusual and abnormal in relation to other system behaviors. The focus of this paper is the use of evolutionary algorithms such as genetics or other new algorithms such as an imperialist competitive algorithm to detect these abnormal behaviors with intelligence agents. In similar studies, various optimization methods such as genetic algorithms, pso have been used. The proposed algorithm can be compared and evaluated with previous methods.

Keywords: abnormal behavior, security, cloud computing, evolutionary algorithm, imperialist competitive algorithm
I. Introduction

In the present century, the progress of science has been remarkable with the expansion and diversification of computing tools. One of the first steps in the development of these technologies was the formation of a computer network with only a few computers connected. These small networks came together to create the Internet, which was shared on the Internet. At that time, there was a need for an exchange of information over the Internet, which created the concept of a global spreadsheet through which information was shared among users [I]. To this end, a new technology called grid computing was developed in which resources were shared remotely, with the aim of increasing processing efficiency and processing power. We are now confronted with a new way called cloud computing, in which services are shared over the Internet. There are many organizations that provide cloud computing services [II]. Cloud computing enables users and developers to use these services without engaging with the technical knowledge or control of the technology infrastructure they need. But on the other hand, more and more information is being stored in the cloud by individuals and companies, which poses a challenge to data security [III]. Information security in virtual environments and a new area called cloud computing has always been emphasized as one of the fundamental infrastructures and requirements in the developmental and inclusive use of ICT. Although absolute security is unattainable both in the real environment and in the cyberspace, it is possible to create a level of security that is sufficient and appropriate in almost all environmental conditions. It is only by providing such a desirable level that customers will with confidence, play their expected role as an effective node of this interactive and synergistic network [IV]. The organization must take security threats and their risks seriously. In the meantime, cloud and cloud space are distinctly more secure than traditional models for the following reasons: the loss of direct control over assets and the potential lack of potential management by the cloud provider, which could be one of the main risks in these called calculations. Security is defined in three ways to maintain the confidentiality, accuracy and availability of data, and therefore there is no difference between cloud computing and other computing models. Organizations, on the other hand, may become overly reliant on one provider and may be particularly challenged in moving data and services within the organization or to another. In fact, using the benefits of cloud computing will create new services and deprive the organization of the speed and agility needed during security events [V]. As mentioned, cloud security is one of the major issues of cloud migration in new systems. Despite the threats in cloud computing, different approaches have been proposed to deal with the threats. Carefully in these routers can be divided into two general categories: Access control and countermeasures and responses. There are many solutions available to deal with threats, but an adequate and acceptable level of data security has yet to be achieved. Intrusion detection systems are used to establish security and prevent the harmful effects of attacks [VI]. Cloud computing is a model for providing user-friendly access over the network to a set of customizable and configurable computing resources such as: networks, servers, storage, applications and services, which can be accessed with the least amount of resource management and Or the need for direct intervention by the service provider to be provided or released promptly. Cloud computing is a model that provides easy,
distributed and inclusive access to configurable, aggregated computing resources. In cloud computing, IT-based capabilities are offered as services that are available without the need for accurate knowledge of infrastructure technologies and minimal management effort. In fact, cloud computing provides the ability to save and save IT resources and increase computing power, so that computing power becomes a permanent accessibility tool [VII]. Because of cloud computing and the increasing volume of data, large-scale data analysis work is needed, because today one of the most critical needs of a cloud server is to provide data analytics to all levels of users, so the need for an efficient database management system is increasingly important for a cloud server. Resource allocation is a big challenge in cloud computing and has a direct relationship with the amount of energy consumed, service providers’ profits and user costs, so there is a lot of work to be done to reduce the number of physical resources used by virtualization and load balancing and the integration of physical resources has been achieved [VIII]. In agent-based resource allocation methods, the consumer and the provider do not communicate directly with each other. If the resources required are in a cloud provider and also available, the allocation is very simple, but if the resources are in a cloud union, the allocation will have to be gathered from different providers, which in complex ways it is needed. Meanwhile, the prices of each resource are dynamically different based on supply and demand. Consideration should be given to retraining the current price of resources from different providers [IX]. In this paper, a security improvement approach is designed based on evolutionary algorithms in which intelligent learning agents are used. In recent years, the use of agents has been observed in many systems of control, error detection, warning systems, network services, etc. [X]. Until now, various techniques such as data mining, statistical modeling and Markov hidden models have been explored to find ways to detect abnormal behavior. Here the abnormal behavior-based security method works by detecting events that appear to be abnormal compared to other normal system behaviors [XI].

II. Review of literature

In recent years, the issue of security using agents has been used in many systems. Different methods such as Markov models, different data mining methods, etc. have been used to detect abnormal behavior.

Different approaches to dealing with threats have been presented so far. Carefully in these routers they can be divided into two categories: access control and countermeasures and responses. The mechanism of access control is to ensure the access of authorized users and to prevent unauthorized access to information systems. The response and response event is to find the problems that arise and to find the right response to the problems. There are many solutions available to deal with threats, but an adequate and acceptable level of data security has yet to be achieved. Intrusion detection systems are used to establish security and prevent the harmful effects of attacks [XII].

The paper [XIII] addresses the role of security and trust in cloud computing environments from the perspective of organizations that transfer their personal information to cloud computing providers. Cloud providers need to show that they are trustworthy. Thus, for the widespread use of cloud computing, it has been argued that customers should be able to store their data in the cloud with the same confidence that
they currently store their money and other valuables in the bank. Technological, legal, and behavioral recommendations have been suggested to help further the role of security and trust.

The paper [XIV] highlights the nature, origin, and implications of institutions and organizational change in the field of cloud computing. The purpose of this study is to gain new insights into the mechanisms and forces that brought about institutional change in the cloud industry. Specifically, research examines how the contradictions created at different levels by technology, the formation of dense networks, and the changing relationships and dynamics of power drive organizational change. This article is expected to provide new insights to institutions involved in the development of new and emerging technologies.

The paper [XV] proposes a framework consisting of various techniques and specialized techniques that can effectively provide data protection from start to finish, for example, from cloud owner to user. The data is categorized according to three encryption parameters provided by the user, for example, confidentiality, availability and comprehensiveness. The strategies outlined for data protection utilize various actions, including SSL (Secure Socket Layer) encryption of 128-bit and 256-bit encryption.

It has been suggested in the paper [XVI] that a trusted third party undertakes the task of ensuring specific security features in a cloud environment. The proposed solution encrypts public key infrastructure and infrastructure in particular with SSO and LDAP to ensure authentication, integrity and confidentiality of the data involved and communications. This solution makes a horizontal level of service available to all parties involved in this security mash-up, the necessity of trust being supported.

The paper [XVII] attempts to improve the level of security of the cloud in order to facilitate the customers to understand the current security situation of the cloud computing. Here are some of the popular security models in cloud computing, such as the multi-lease model, the risk accumulation model, the cube model of cloud computing, and the major cloud computing security risks posed by various organizations. Finally, some security strategies are presented from the perspective of construction, operation and security incident to eliminate common security issues in cloud computing.

The paper [XVIII] provides a two-level framework for managing behavior across cloud layers. Here, resource attributes are estimated by analyzing high-level information and predicting user behavior. High-level information patterns are analyzed over a specific time series and then translated into low-level resource features using artificial neural networks.

The paper [XIX] examines the adoption of cloud computing services in government agencies, focusing on key features that influence behavioral intention. The empirical research model is validated by examining the perceptions of users working in public institutions. The modeling results show that users' intentions and behavior are greatly influenced by the perceived characteristics of the cloud with the services provided. These findings enhance the government's use of cloud services to increase user awareness through enhanced capabilities, appeal and security.

In the article [XX], data owners are restricted to controlling IT infrastructures, so they must provide a mechanism to enforce their security policies in order to ensure data privacy and integrity. Following is a security infrastructure to
In [XXI], an incremental encryption scheme based on elliptic curve cryptography is proposed. The main idea is to encrypt data before storing it in the cloud. In the context of encrypted data sharing, it will be re-encrypted without any initial decryption. Then the re-encrypted data will only be available to authorized users in terms of encryption using related authentication tools.

The paper [XXII] noted that lack of proper transparency in the cloud prevents users from using its benefits. It states that the key components of cloud service providers’ responsibility are accessibility, transparency, accountability, assurance and commitment to compensation. It is also stated that there is a need to develop mechanisms to implement security policies to prevent adverse events.

The paper [XXIII] proposes a new trust-based and two-factor collaboration framework based on cloud resource conservation. The uniqueness of the security solutions provided to ensure security and privacy at both the service provider level as well as the user level in a cloud environment is emphasized. Here is updated user activity information and trust documentation to calculate the degree of trust.

The article [XXIV] provides measures to resist the deception of sellers that shoppers can order their applications with very low pre-migration requirements to the cloud platform. Situations between buyers and sellers are modeled as a mathematical model called the eavesdropping and negotiation resistance (ERN) model. Buyers and Sellers Game Strategy analyzes ERN Games with an economic and computational approach based on intelligent agents.

Intelligent agents have been used in other applications in similar studies. For example, an agent-based resource management approach is proposed in [XXV]. In this way, the user does not need to know where the source of the cloud service provider's whereabouts is located and in this way the consumer uses the least expensive resources. The proposed system in this field has three types of factors: consumer agent, intermediary agent (cloud broker) and resource provider. The agent mediates all information about resources and allocates resources to the consumer agent on the part of the provider. The main advantage of this model is that the consumer does not bother to understand the location and cost of the resources. The consumer can get the resources at the lowest cost.

In [XXVI], an integrated scheduling strategy with regard to both resource validity and user satisfaction is proposed. Here, user satisfaction as a target function, resource validation as part of user satisfaction, and optimal scheduling were performed using genetic algorithms. This scheduling strategy is integrated with smart agents and then a multi-agent cloud computing system architecture is presented. The results show that this scheduling strategy improves not only the operating system performance but also the user satisfaction.

III. Cloud computing security

III.1 Cloud Storage Security Requirements

There are three elements involved in data storage and retrieval in the cloud: Client, Server (CSP) and the links between them. In order to provide security, all three elements must have solid security. The client must make sure that he can access his device without permission. While on cloud storage server (CSP), it must ensure that confidentiality, integrity and data availability are maintained. Finally, the
connection between the client and the server must be made through a secure channel, meaning that data transmission must be kept confidential throughout the transfer between the server and the client.

**III.i.a. The most important security risk categories**

The security risk of using cloud companions should be taken into account, and the risks associated with using cloud companions should be compared with those of traditional solutions, such as desktop-based models, and then the need-based approach.

**III.i.a.1 Politics and Organization**

A) **Lock in lock**

It is possible to lock data in a specific CSP. There is no specific standard in data formats or in the service of interfaces that guarantee data. In addition, this is a very high risk for a company as it may lead to the following vulnerabilities: lack of standard technology and solutions, poor provider selection, lack of redundancy, and inadequacy and transparency in terms of use, this impact on company reputation, sensitive personal information and service delivery. In addition, it can lead to business failure [XXV].

B) **Loss of sovereignty**

When using cloud infrastructure, the customer can have control over certain parts, which may compromise the cloud provider's security and lead to loss of control. This loss of government and control strongly affects the strategy of the organization and its goals. In addition, it compromises compliance with security requirements, resulting in confidentiality, data availability, and performance degradation and quality of service.

C) **End or failure of the cloud**

In any IT marketplace, given the competitive environment, inappropriate business plans and lack of financial support may force some cloud providers to quit or decline services. In other words, some cloud companion services may shortly be terminated for any of the reasons outlined above and may be terminated as a medium risk leading to loss or deterioration of performance. Service delivery and quality of service as well as loss of investor are expressed [XXV].

**III.i.a.2 Technical risk**

A) **Management of the compromise interface**

Since the client has access to the public cloud interfaces over the Internet, he has access to a large pool of resources, which in turn increases the risk and vulnerability, such as script attacks. In addition, back-end technology enables account theft and account compromise. The management interface also includes client interfaces that control a number of virtual machines and CP interfaces and enable the operation of the overall cloud system [XXV].

B) **Denial of Service (Dos)**

An attacker may have trouble accessing customer-protected resources through public channels. Cloud system protection against DOS attacks depends on the capabilities and configurations of the provider's cloud technology [XXV].
C) Loss of encryption keys
Poor key management may lead to the disclosure of secret SSL keys, file encryption, client private keys or passwords to malicious persons and losing that key and unauthorized use for authentication and digital signature.

D) Non-separation
The two main features are multi-tenant cloud and resource sharing. These two features make it possible for the computing, storage, and network capacity needed to be shared among multiple users. On the other hand, it leads to the creation of a class of risks, which include the failure of the storage separation mechanism, memory, routing, and even the reputation of the different tenants sharing the infrastructure [XXV].

III.ii. Intrusion detection

Detecting attempts to unauthorized and illegal access to the network and reducing its efficiency is called intrusion detection. Intrusion detection systems are classified into three types of combination-based IDS, network-based IDS, and host-based IDS.

An intrusion detection model using the moving factor Tabatabaei and Bakar is presented which provides specific features in this area. The advantage of this method is to achieve greater scalability, asynchronous and non-dependent execution, dynamic adaptation, operation in heterogeneous environments, having strong and fault-tolerant behavior, overcoming network delays, reducing network load and thus reducing operating costs [XXVI].

A method called IDSaaS has been used in the intrusion detection system as a public cloud service. The goal of IDSaaS is to provide the security of supercomputing infrastructures by providing intrusion detection technology that is portable and user controlled. IDSaaS is a network-based IDS and signature-based cloud model in general. IDSaaS is portable, controllable and demand-based [XXVII].

In [XXVIII], an agent-based model is proposed that keeps user data secure in the cloud environment. In this paper, different implicit algorithms are provided for a secure system, thus identifying attacks and preventing intrusion.

Cloud computing in government agencies has been studied focusing on key features of service acceptance. This study is based on the technology adoption model with a combination of factors such as availability, accessibility, security and reliability. The empirical research model is validated by examining the perceptions of users working in public institutions. Modeling results show that users' intentions and behavior are largely influenced by the perceived characteristics of the cloud with the services provided. These findings enhance the government's use of cloud services to increase user awareness by enhancing capabilities, appealing and providing security [XXIX].

Security and trust in cloud computing environments have been studied from the perspective of organizations that transfer their personal information to cloud computing providers. Cloud providers need to show that they are trustworthy. Therefore, for the widespread use of cloud computing, it has been argued that customers should be able to store their data in the cloud with the same confidence that
they currently store their money and other valuables in the bank. Technological, legal, and behavioral recommendations have been suggested to help further the role of security and trust [XXX].

III.iii. Anomaly detection

Anomalous (or behavioral) identification focuses on identifying events that appear to be abnormal with respect to normal system behavior. Various techniques, including data mining and statistical modeling and Markov models have been discovered as different ways of achieving the anomaly detection problem. The anomaly-based approach includes a set of data that relates to legitimate user behavior over a period of time and then performs statistical tests on the observed behavior to determine if it is legal behavior. The advantage of this method is that it detects attacks that have not been detected before. The key element to using this method is to generate law so that it has fewer alerts for unknown attacks as well as known attacks. The Dot team has developed an anomaly-based solution to prevent intrusion into real-time systems that analyzes protocol-based attack and multidimensional traffic. However, optimization is done to reduce the number of IPS. Zheng's team has introduced a light-weight intrusion detection system to effectively detect intrusions into the real-time system. Cloud anomaly detection techniques have been used to detect unknown attacks at different levels [XXXI, XXXII]. In the cloud, a large number of events (network level or system level) occur that permits intrusion monitoring and control using anomaly detection techniques. Garfinkel, Rosenblum, Vieira Group, Dastjerdi Group, and Guan, have proposed anomaly detection techniques that detect intrusions into different layers of the cloud [XXXIII-XXXVI]. The ability ofsoft computing techniques to deal with partially correct and uncertain data makes them attractive as they apply to intrusion detection. There are several soft computing techniques such as artificial neural network, fuzzy logic, association rule mining, support vector machine, genetic algorithm, etc. It can improve the accuracy and efficiency of signature-based IDS or IDS-based IDS.

III.iv. Evolutionary Algorithms

A subset of artificial intelligence is concerned with evolutionary algorithms. This set of methods includes search algorithms in which the search begins at several points in the answer space. Evolutionary algorithms are fundamentally different from other conventional search and optimization techniques. Some of these differences are:

Evolutionary algorithms: 1) they do not search for just one single point, but look at a population of points in parallel. 2) they do not require implicit information and other complementary knowledge; only the relevant function and competence affect the search directions. 3) use possible changing rules, not specific ones. 4) it is generally straightforward to use, since there are no restrictions on defining the objective function. 5) obtain a large number of acceptable responses and the end-user is the choice; in cases where the problem does not include a single answer, such as a family of beam-optimal
responses, similar to that of multi-objective optimization and scheduling problems of existence has it. Evolutionary algorithms are inherently efficient for identifying these multiple responses simultaneously. Evolutionary algorithms are: bee colony algorithm, ant colony optimization method, genetic algorithm and imperialist competitive algorithm. The method used in this research is imperialist competitive algorithm, which is explained in more detail below.

**Imperialist Competitive Algorithm**

The imperialist competitive algorithm is a method of finding the optimal answer to various optimization problems. The imperialist competitive algorithm has many advantages over other nature-inspired methods. Including: new idea: it is based on human social behavior that is smarter than his biological behavior. High convergence speed: ability to optimize functions with a large number of variables. The basic foundations of this algorithm are the politics of matching, competition and revolution. In fact, this algorithm looks at the optimization solutions in the form of countries and tries to improve these solutions gradually and over the course of an iterative process and ultimately to obtain the optimal solution of the problem [XXXVII].

**Parameters**

1. Initial Population: Some of these countries will be created as the initial population. $N_{country}$ of initial country
2. Choice: $N_{imp}$ must be selected as the imperialist of the best members of this population (countries with the least amount of cost function).
3. Remnants: $N_{col}$ the remaining states are colonies that each belong to a system.
4. Dividing colonies: each imperialist is assigned a number of colonies proportional to its power. To do so, at the expense of all the imperialists, the cost of normalizing them is as follows.

\[ C_n = \max_i \{c_i\} - c_n \]  \hspace{1cm} (1)

Where $c_n$ is the nth imperialist cost, $\max_i \{c_i\}$ is the highest cost between the imperialists and $C_n$ the normalized cost of this imperialist. The imperialist is more expensive and weaker imperialist have less normalization cost.

Calculate the relative power of normalization Each imperialist is divided between the imperialist sites at the cost of normalization and division of the colonial countries.

\[ P_n = \frac{c_n}{\sum_{i=1}^{N_{imp}} c_i} \]  \hspace{1cm} (2)

The proportion of colonies ruled by an imperialist is regarded as the normalized power of an imperialist. Thus the initial number of colonies of an
imperialist would be:

\[ N. C_n = \text{round}\{P_n \cdot (N_{col})\} \]

\(N. C_n\): The initial number of colonies of a system
\(N_{col}\): The number of colonial countries in the population of early states
\text{Round}: The closest integer to a decimal number

Considering the N.C. for each system, these randomly selected initial colonial states will be given the \(n\)th imperialist. With the initial state of all systems, the colonial competition algorithm begins. The process of evolution is in a loop that continues until a stopping condition is met. The larger systems have more colonies, depending on the shape of the initial systems. In this form, the imperialist No. 1 has created the strongest system and has the largest number of colonies.

![Figure 1: how the initial population (systems) formed [37]](image)

### III.v. Assimilation

In order to analyze the culture and social structure of the colonies, a centralized culture of assimilation is performed. The efforts of the colonial states to increase their influence by pursuing a policy of assimilation into the colonies by applying the policy of assimilation include the attempt to change and bring the colony into alignment with various socio-political dimensions. The modeling of this phase of the colonization process in the optimization algorithm is carried out as the colonies move toward the imperialist state.
The colonial state is absorbed by the imperialist state along the cultural and linguistic axes of the colony's x unit in the colonial line to move to the colonel and move to a new position. 

\[ X \sim \mathcal{U}(0, \beta \times d) \]  

- \( d \): The distance between the colonizer and colony
- \( X \): Random number with uniform distribution
- \( \beta \): Constant number greater than one and close to 2

Coefficient \( \beta > 1 \) to approach the colonial country from different directions as it moves towards the colonial state. It is worth pointing out that despite the pursuit of colonial drawer seriously for the policy of assimilation, events do not fully follow their policy and there are deviations from the result.

### III.vi. Position replacement

The policy of assimilation does not produce good results for the country of the colony. But sometimes this policy, while destroying the social and political structures of the colonial state, in some cases also had positive results for them. Some countries gained some form of public self-esteem as a result of this policy, and after some time the same educated colonialists began to lead their nation to the grip of colonialism. In modeling this historical event in the ICA algorithm, it is worked out that some of these colonies may be in a better position than the imperialist during the movements of the colonies towards the colonial state. In this case, the colonial state and the colonizer state have replaced each other and the algorithm has continued with the colonial state in the new position, this time it is the new imperialist state that begins to apply the policy of assimilation to its colonies. In this way, the best colony of the system, less costly than the imperialist it is shown in darker color.
III.vii. Cost function

The cost function of a system, given that the power of a system as a total power of the colonial state is expressed as a percentage of the total power of its colonies, is as follows:

\[ T.C_n = \text{Cost(Imperialist}_n) + \xi \text{mean}\{\text{Cost(colonies of empire}_n)\} \]

\( T.C_n \): Total cost of \( n \)th system  
\( \xi \): Positive number (integer between zero and one near zero) - small consideration of \( \xi \) causes the total cost of the system to be approximately equal to the cost of its central government, and the increase in \( \xi \) also increases the cost effect of a system's colonies on determine its total cost.

III.viii. Competition

Like other evolutionary algorithms, there is a process of elimination and survival in this algorithm. Over time, weak systems lose their colonies and stronger systems take over and increase their power. To model this fact, we assume that the eliminating system is the weakest system available. Thus, in the iteration of the algorithm, we remove one or more of the weakest colonies from the weakest system and create a competition among all the systems to acquire these colonies. These colonies will not necessarily be conquered by the strongest system, but stronger systems are more likely to be conquered.
III.ix. System Survival

During imperialist rivalries, weakly, weak systems gradually collapse and their colonies fall into stronger systems. Different conditions can be considered for a system crash. In the ICA algorithm, a system is considered to be eliminated when it has lost its colonies.

Figure 4: General scheme of imperialist competitive [XXXVII]

III.x. Termination of the algorithm

The algorithm continues until a convergence condition is met or until the total number of iterations is completed. After a while, all systems will collapse and we will have only one system and the rest of the countries will be under the control of this single system. In this ideal new world, all colonies are governed by a single system, and the colonies' positions and costs are equal to those of the imperialist state. In this
new world, there is no difference, not only between the colonies but between the colonies and the imperialist state. In other words, all countries are at the same time colonial. In such a situation the imperialist competition is over and one of the conditions of the algorithmic agreement is stopped.

III.xi. Proposed method

In this paper, we intend to present a method for detecting abnormal system behaviors and increasing security in cloud based algorithms based on evolutionary algorithm using intelligent learning agents. In recent years, the use of agents has been observed in many systems of control, error detection, warning systems, network services and more. It is architecturally very close to the immune system. The distributed network system consists of a large number of data centers and intelligent learning agents that move through the data center. Learning is one of the important capabilities of smart agents, so in many cases an intelligent agent is expected to be able to learn and improve its performance based on its results, in addition to other capabilities. On the other hand, in many cases, a system where learning is possible is often regarded as an intelligent system. Thus, agent learning is one of the characteristics that need special attention. Learning methods in intelligent agents are presented using machine learning methods and their adaptation to operating conditions and multi-agent systems. The learning process in intelligent agents can be attributed to agent change so that these changes bring the agent's knowledge closer to the feedback information it receives from the environment, and ultimately improve the agent's general performance. The imperialist competitive algorithm is used here to apply the learning to the agents.

III.xii. Scenario

The following scenario is used to evaluate the performance of the proposed system. At first it is assumed that no intrusion has occurred on the network. Then the intrusion occurs and spreads to the same data center and its neighboring data center. In the first case the network is secure and no intrusion has occurred. In this case the simulations are performed and the response time in the data centers is specified. In the latter case, the intrusion is spread across the data center and its neighboring data center. In this case, all servers inside the data center as well as the main server in the neighboring data center will be affected.

Figure 6: Detection system of user’s abnormal behavior in cloud environment
The dataset used in this article is the NSL-KDD dataset. This dataset is a new dataset for evaluating research in a network intrusion detection system. In general, the kdd dataset has several classes that can be detected by examining the influence of cloud computing. In order to evaluate the influence, the existing requests are first divided into two classes of allowed and unauthorized, and the system can decide on the desired request according to the class of requests. The reason for using this dataset is that it is easily accessible and can be downloaded from various sites without any charge. Secondly, it has various features that allow the intrusion detection process to be performed with reasonable accuracy. This dataset consists of selected records from the complete KDD 99 dataset. The NSL-KDD dataset contains forty-one attributes that have thirty-four numerical attributes and seven symbolic or discrete attributes. The NSL-KDD training set contains data on more than twenty-two types of attacks. Table 1 describes the features of the NSL-KDD dataset.

Table 1: describes the features of the KDD dataset

| No | Name               | Description                                              |
|----|--------------------|----------------------------------------------------------|
| 1  | Duration           | Connection time or duration                              |
| 2  | Protocol_type      | Type of protocol                                         |
| 3  | Service            | Destination service                                      |
| 4  | Flag               | Connection flag status                                   |
| 5  | Src_byte           | The number of bytes of data from source to destination   |
| 6  | dst_byte           | The number of bytes of data from destination to source   |
| 7  | Land               | If the connection from / to the host / port is the same, the value is one, otherwise it is zero |
| 8  | Wrong_fragment     | The number of incorrect fragment                         |
| 9  | Urgent             | The number of urgent packets                             |
| 10 | Hot                | The number of hot indicators                             |
| 11 | Num_failed_logins  | Number of problematic login                              |
| 12 | Logged_in          | If the login is successful, the value is one and in the other cases zero |
| 13 | Num_compromised    | Number of conditions compromised                          |
| 14 | Root_shell         | If you have access to the root, the value is one, and in the other cases it is zero |
| 15 | Su_attempted       | If the su root command is given, the value is one and in the other cases zero |
| 16 | Num_root           | Number of root accesses                                  |
| 17 | Num_file_creation  | Number of file creation operations                        |
|   | Key            | Description                                                                 |
|---|----------------|-----------------------------------------------------------------------------|
| 18| Num_shells     | Number of shell prompt                                                       |
| 19| Num_access_files | Number of access operations to control file                                    |
| 20| Num_outbound_cmds | The number of remote commands in a ftp session                                |
| 21| Is_host_login  | If the login is through a hot list the value is one and in the other cases the value is zero |
| 22| Is_guest_login | If the login is done by a guest, the value is one and in the other cases the value is zero |
| 23| Count          | Number of similar connections to host in the last two seconds                |
| 24| Srv_count      | Number of similar connections to the same service in the last two seconds    |
| 25| Serror_rate    | Percentage of connections that have a SYN error                              |
| 26| Srv_serror_rate | Percentage of connections that have a SYN error                              |
| 27| Rerror_rate    | Percentage of connections that have a REJ error                              |
| 28| Srv_rerror_rate | Percentage of connections that have a REJ error                              |
| 29| Same_srv_rate  | Percentage of connection to similar services                                 |
| 30| Diff_srv_rate  | Percentage of connection to dissimilar services                              |
| 31| Srv_diff_host_rate | Percentage of connection to different hosts                                  |
| 32| Dst_host_count | Number of connections with the same destination                              |
| 33| Dst_host_srv_count | The number of connections to the same destination using the same service    |
| 34| Dst_host_same_srv_rate | Percentage of connections to the same destination using the same service |
| 35| Dst_host_diff_srv_rate | Percentage of different services on the host                                |
| 36| Dst_host_same_src_port_rate | Percentage of connectivity to hosts that have the same source port          |
| 37| Dst_host_srv_diff_host_rate | Percentage of connection to a service from different hosts                 |
| 38| Dst_host_serror_rate | Percentage of connection to host that has error S0                           |
| 39| Dst_host_srv_serror_rate | Percentage of connection to host and                                        |
IV. Results

There are various criteria for evaluating the proposed algorithm that can be used to evaluate the benefits of the proposed method. The most important criterion that can be used to evaluate the proposed algorithm is the percentage of error in detecting intrusion in the cloud, which is closer to zero, indicating the efficiency and optimization of the algorithm used. Another parameter that can be used to evaluate the proposed algorithm is the execution time or the time spent on executing the algorithm. Obviously, lower runtime means faster speeds are an essential feature of computer systems. It should be noted that in all available measurements, the unit of time is seconds. Figure 7 shows the results of comparing the error rate of the proposed algorithm with some other methods available in the field. The proposed algorithm performs better than some other methods in the field. Figure 8 also compares the execution time of the proposed algorithm with the execution time of some other methods. The algorithms are run using a computer with a PENTIUM IV processor to calculate the assumed runtime. It has 4 GB of memory and runs on Windows 8 operating system.

![Error Rate Comparison](image.png)

Figure 7: compares the error rate of the proposed algorithm with some other methods
Figure 8: shows the execution time of the proposed algorithm with the execution time of some other methods

V. Conclusion

In this paper, intrusion detection in cloud computing with evolutionary algorithms is investigated and its results compared with some other methods available in this field. Evaluation of the results of the proposed algorithm of this paper shows that the proposed algorithm yields better results and can detect cloud infiltration process in less time and with greater accuracy.
References

I. A. Vakili, N.J. Navimipour. Comprehensive and systematic review of the service composition mechanisms in the cloud environments. J. Netw. Comput. Appl., 81 pp. 24-36, 2017.

II. B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," Computer Networks, vol. 81, pp. 308-319, 2015.

III. Beiter, Michael, et al. "End-to-end policy based encryption techniques for multi-party data management." Computer Standards & Interfaces, 36.4 689-703, 2014.

IV. Bose, Ranjit, Xin Luo, and Yuan Liu. "The Roles of Security and Trust: Comparing Cloud Computing and Banking." Procedia-Social and Behavioral Sciences, 73: 30-34, 2013.

V. Che, Jianhua, et al. "Study on the security models and strategies of cloud computing." Procedia Engineering, 23: 586-593, 2011.

VI. Dastjerdi, Amir Vahid, Kamalrulnizam Abu Bakar, and Sayed Gholam Hassan Tabatabaei. "Distributed intrusion detection in clouds using mobile agents." Advanced Engineering Computing and Applications in Sciences, 2009. ADVCOMPO9. Third International Conference on. IEEE, 2009.

VII. Govinda, K., and E. Sathiyamoorthy. "Agent Based Security for Cloud Computing using Obfuscation." Procedia Engineering 38 (2012): 125-129.

VIII. Jalal Nouri,D., Saniee Abadeh, M.&Ghareh Mohammadi, F. HYEI: A New Hybrid Evolutionary Imperialist Competitive Algorithm for Fuzzy Knowledge Discovery. Advances in Fuzzy Systems. vol. 14, no. 11, 387-395, 2014.

IX. Jin, Hai, et al. "A guest-transparent file integrity monitoring method in virtualization environment." Computers & Mathematics with Applications, 60, 2: 256-266, 2010.

X. K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection techniques in grid and cloud computing environment," IT Professional, IEEE Computer Society, vol. 12, pp. 38-43, 2010.

XI. Kim, Junghan, Inhyuk Kim, and Young Ik Eom. "Nopfit: File system integrity tool for virtual machine using multi-byte nop injection." Computational Science and Its Applications (ICCSA), 2010 International Conference on. IEEE, 2010.

XII. Kong, Jinzhu, AdjointVM: a new intrusion detection model for cloud computing. Elsevier, 2011.

XIII. Kousiouris, George, et al. "Dynamic, behavioral-based estimation of resource provisioning based on high-level application terms in Cloud platforms." Future Generation Computer Systems, 32: 27-40, 2014.

XIV. Kshetri, Nir. "Privacy and security issues in cloud computing: The role of institutions and institutional evolution." Telecommunications Policy, 37, 4: 372-386, 2013.

XV. Lai, Yung-Liang. "Analyzing strategies of mobile agents on malicious cloud platform with Agent-Based Computational Economic Approach." Expert Systems with Applications, 40, 7: 2615-2620, 2013.
XVI. Lo, Chi-Chun, Chun-Chieh Huang, and Joy Ku. "A cooperative intrusion detection system framework for cloud computing networks." Parallel processing workshops (ICPPW), 2010 39th international conference on. IEEE, 2010.

XVII. M. Haresh, S. Kalady, and V. Govindan, "Agent based dynamic resource allocation on federated clouds," in Recent Advances in Intelligent Computational Systems (RAICS), IEEE, 2011, pp. 111-114, 2011.

XVIII. M. Tang, X. Dai, J. Liu, J. Chen. Towards a trust evaluation middleware for cloud service selection. Future Gener. Comput. Syst., 74, pp. 302-312, 2017.

XIX. Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr.A. D. Gawande, Intrusion Detection System for Cloud Computing. International Journal of Scientific & Technology Research, 2012.

XX. N. Dot. Anomaly Detection via Online Over-Sampling Principal Component Analysis| FTJ1314, 2015.

XXI. N. Ghadiri, A. Baraani-Dastjerdi, N. Ghasem-Aghaei, and M. A. Nematbakhsh, "Optimizing the performance and robustness of type-2 fuzzy group nearest-neighbor queries," Mobile Information Systems, vol. 7, pp. 123-145, 2011.

XXII. Pearson Siani. Toward accountability in the cloud. EEE Internet Comput;15(4):64–99, 2011.

XXIII. R. Roustaei and F. Yousefi Fakhr. A Hybrid Meta-Heuristic Algorithm based on Imperialist Competition Algorithm. Journal of Aland Data Mining Vol 6, No 1, 59-67, 2018.

XXIV. Rasheed, Hassan. "Data and infrastructure security auditing in cloud computing environments." International Journal of Information Management 34.3: 364-368, 2014.

XXV. Rong Chunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011), 2011.

XXVI. Shin, Dong-Hee. "User centric cloud service model in public sectors: policy implications of cloud services." Government Information Quarterly 30.2:194-203, 2013.

XXVII. Sood, Sandeep K. "A combined approach to ensure data security in cloud computing." Journal of Network and Computer Applications 35.6, 1831-1838, 2012.

XXVIII. T. Garfinkel and M. Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection," in Ndss, pp. 191-206, 2003.

XXIX. Tarigonda, Siva, A. Ganesh, and Srinivasulu Asadi. "Providing Data Security in Cloud Computing using Novel and Mixed Agent based Approach." International Journal of Computer Applications 112.6, 2015.

XXX. Tianfield, Huaglory. "Cloud computing architectures." Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on. IEEE, 2011.

XXXI. Turki Alharkan, Patrick Martin, IDSaaS: Intrusion Detection System as a Service in Public Clouds. IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012.
XXXII. Waqar, Adeela, et al. "A framework for preservation of cloud users’ data privacy using dynamic reconstruction of metadata." Journal of Network and Computer Applications 36.1, 235-248, 2013.

XXXIII. Y. Wang, J. Wei. Toward protecting control flow confidentiality in cloud-based computation. Comput. Secur., 52, pp. 106-127, 2015.

XXXIV. Z. Cai, X. Guan, P. Shao, Q. Peng, and G. Sun, "A rough set theory based method for anomaly intrusion detection in computer network systems," Expert Systems, vol. 20, pp. 251-259, 2003.

XXXV. Zhang, Xuyun, et al. "An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud." Journal of Computer and System Sciences 79.5: 542-555, 2013.

XXXVI. Zhao Gansen, Rong Chunming, Li Jin, Zhang Feng, Tang Yong. Trusted data sharing over untrusted cloud storage providers. In: Proceedings of the 2nd IEEE international conference on cloud computing technology and science (CloudCom 2010), 2010.

XXXVII. Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer Systems, 28, 3: 583-592, 2012.