IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 9, Issue.4, April 2021 E-ISSN: 2347-2693

Survey on an Intrusion Detection Systems Within Cloud Environment

Montather Ghalib ALi[1*], Fadl Mutaher Ba-Alwi[2], Ghaleb H. Al-Gaphari[3]

[1]Department of Computer Science, Faculty of Computer & Information Technology (FCIT), Sana'a, University, Yemen
[2]Department of Information Systems, Faculty of Computer & Information Technology (FCIT), Sana'a, University, Yemen
[3]Department of Computer Science, Faculty of Computer & Information Technology (FCIT), Sana'a, University, Yemen

[*]*Corresponding Author: Corresponding Author: moalgaphari@gmail.com, Tel.: +967-772159089*

DOI: https://doi.org/10.26438/ijcse/v9i4.4155 | Available online at: www.ijcseonline.org

Received: 02/Apr/2021, Accepted: 10/Apr/2021, Published: 30/Apr/2021

***Abstract*—** The decentralized nature of cloud computing paradigms has resulted class computing which prone to cyber-attacks and intrusions. One of major security matters in cloud is conducting intruder detection approaches for detecting and preventing network intrusions. The aim of this research paper is to review and analyze the research domain of collaborative, cooperative and distributed intrusion detection approaches within cloud environment. The research paper focusses on articles related to the keywords: cooperative, distributed, collaborative and their variations in three major databases, namely ScienceDirect, Springer Nature and the Institute of Electrical and Electronics Engineers' Xplore. Such databases are sufficiently cover the literature techniques related to the aforementioned keywords. The collected dataset consists of 23 articles, the largest proportion of them focuses on model's development that leverage collaborative intruder detection approaches, while the rest presents frameworks for intruder detection approaches. This study presents real analyses performed on available work: models, framework limitations and motivations. The study also, specifies the gap of the most state of the art related to cooperative and provides an extensive resource background for researchers who are interested in enhancing the performance of CIDSs within cloud environment. Finally, the paper suggests a new ensemble deep learning based model for improving the performance of proactive multi-cloud cooperative intrusion detection system.

Keywords—Cloud Computing, Cooperative Intrusion Detection System, Distributed Intrusion Detection System, Collaborative Intrusion Detection System.

I. INTRODUCTION

The complex structure of cloud computing systems makes them vulnerable to different kinds of attacks. Hackers have developed new sophisticated techniques and tools which enable them to bring down an entire cloud platform, these tools have become more sophisticated challenge for existing network cloud intrusion detection system (IDSs) [21]. A destructive attack causes new levels of disruption for cloud infrastructures and services [23]. Both of distributed denial of service (DDoS) and denial of service (DoS) attacked cloud infrastructure of different sectors: enterprises, banks and companies. Such attacks raised the estimated average of financial loss to almost 540k per hour [23], this may degrade cloud services performance which impact negatively on cloud confidence within customers community [23]. Therefore, security and privacy sustaining of entire cloud computing has emerged as a major concern for both industry and academia in order to be resistant against different types of security attacks. In this study, many different approaches and techniques have been reviewed and analyzed: distributed intrusion detection system (DIDS), collaborative intrusion detection system (CIDS) and cooperative intrusion detection system (CIDS). Each one of these approaches includes more than one IDS, each IDS works independently and called standalone IDS where CIDSs work in a cooperative manner [22]. The distributed cloud computing (DCC) environments utilized by distributed intrusion detection system. These CIDSs share the logs and alert information with each other. Thus, the administrator needs to be fine-tuned from time to time to configure the type and volume of information shared among the distributed IDS. It facilitates advanced persistent threat analysis, network monitoring, and instant attack analysis of the whole network. It helps the view of the network attack. The CIDSs provide a centralized platform where the attack can be detected right away no matter in whatever network segment it occurs. As it gives an advantage to the administrator for centralized analysis, it also requires proper planning and implementation. Since the whole network infrastructure depends on DIDS, it should have potential power, flexibility, and strength to detect the attack as quickly as possible. DIDS, it should have potential power, flexibility, and strength to detect the threat as quickly as possible without more delay in detection [26]. In fact, Proactive multi-cloud cooperative intrusion detection systems in contexts of cloud computing are very complicated tasks, they may require well informative and representative multi-class datasets. However, the real multi-datasets contain all kinds of attributes with nonlinear behavior and high dimensionality. These attributes not only increase computational complexity of the underlying algorithm but also deteriorate

its performance in terms of making decisions on suspicious intrusion. Thus, some optimal techniques should be employed for selecting an optimal subset of informative attributes, such techniques should concern with datasets dimensionality reduction and effect of non-linear attributes on feature selection. On the one hand, the dimensionality reduction of the dataset can be obtained using a deep learning technique such as Restricted Boltzmann Machine (RBM) which has ability for selecting features, forming clusters at different levels of scale and maintaining consistency of the given feature sets. On the other hand, the effect of non-linear attributes on feature selection can be solved using non-linear estimator such as Unscented Kalman Filtered (UKF). These preprocesses assist in designing a model for enhancing the performance of existing proactive multi-cloud cooperative intrusion detection system. Thus, the main objective of this paper is to illustrate the accomplishments of available researchers, summarize, discuss and compare previous results that reflect the CIDSs requirements, determine evaluation criteria and methods stated by each study, the study also, specify the gap and the limitation in the current state of the art, finally, the paper introduced a new ensemble deep learning based model for improving the performance of proactive multi-cloud cooperative intrusion detection system using an optimal features selector and a filter for non-linear attributes of real time dataset. The rest of this study is organized as follows: Section I introduces briefly different CIDSs and their importance of distributed cloud computing security, section II describes the related work, while section III presented a methodology of the survey, Section IV introduces the CIDSs taxonomy and section V briefly present a summary and discussion.

II. RELATED WORK

Various research efforts existed on CIDSs techniques depending on different approaches of ML, DL, Multi-agent, Mobile-agent and Block-chain in cloud computing environment. CIDSs includes many IDS over different region or host that share alerts between each other to detect collaborative attacks such as DDoS. CIDSs have the abilities of detecting intrusion shared over several networks by aggregating attack evidence across several sub network. Many research studies address the issue of collaborative attacks within cloud computing. They are categorized into signature based, anomaly detection and hybrid techniques. The signature-based technique focused on MACoMal, which assists heterogeneous anti-malware tools to collaborate with each other in order to reach a consensual decision about the maliciousness of a suspicious file [8]. MACoMal consists of two main elements: identification model, and collaborative decision-making scheme. The MACoMal is analyzed with respect to network connectivity and global decision correctness.

The anomaly detection approach was adopted by several research studies [3], they focused on CIDSs within cloud computing that uses data mining methods. In this type the network traffic is collected from edge routers and forwarded to anomaly detection devices using Naïve Bayes classifier. The anomalous data are then transmitted to a central server and then a Random Forest classifier is used for classification on the anomalous data. While other articles paid attention to CIDSs in multi-cloud environment based on DL techniques that efficiently exploits the historical feedback data to provide the ability of proactive decision making. This model used denoising autoencoder as a building block for DL.The CIDS-based denoising autoencoder to learn how to reconstruct original IDSs' feedback given incomplete IDSs' feedback [1]. Moreover, some research studies concentrated on new collaborative anomaly detection framework for detecting known and unknown intrusive activities in cloud computing environments [20]. Such frameworks include capturing logging network data, pre-processing these data to be handled at the decision engine sensor and a new decision engine using the Gaussian Mixture model for identifying abnormal patterns. Some other studies have focussed on ML for Multi-Attacks Detection in Distributed System. They decrease the individual and combination routing attacks. They have used feature selection techniques to determine significant features, along with the best classification method will distinguish between an attack and non-attack. The hybrid approach contains both anomaly detection and signature-based. This hybrid approach was adopted by many researchers in CIDSs [24] where they applied snort and backpropagation neural network classifier which was optimized by optimization algorithm to overcome the weakness of BPN. This hybrid model deployed in front-end and back-end of the cloud to detect external attack and internal attack. In addition, The MAS-DIDS contains two techniques of signature-based and anomaly-based intrusion detection to block both known and unknown attacks within a complex, dynamic and changing environment [5]. finally, HDIDS was presented to combine an anomaly- based detection algorithm and multiple signature-based detection algorithms. The signature-based multiple classifiers ensemble and can detect real time attack based on majority of votes from each classifier. Ensemble output use voting technique which are simplest to implement produce suitable results that Anomaly based classifier has intensive focus over new and unknown attacks in distributed network[25]. Unfortunately, the available research studies still have gaps and limitations in terms of proactive CIDSs models performance and their datasets representation. Thus, it is necessary to introduce an ensemble deep learning model which associate with a real time dataset with simple reasonable representation. This may affect significantly in reducing the limitation in the current state of the art related to CSIDSs and to enhance the performance of proactive CSIDSs.

III. METHODOLOGY

The CIDSs is the most valuable phrase in the scope of this study. Other CIDSs techniques that are not implemented in cloud environment are excluded. All areas are considered related to CIDSs and restricted to the English literature

scope. Moreover, intruder and attacker are used as general categories.

A. Information sources

The target articles were searched for based on the following digital databases:

- The ScienceDirect database provides an entry to journals, technical and science articles.
- The Xplore database of the Institute of Electrical and Electronics Engineers (IEEE) contains technical literature in electrical engineering, electronics, computer science and other related fields.
- The Springer Nature is the largest abstract database of peer reviewed literature (scientific journals and conference proceedings).

B. Study collection

Study collection contains two steps: reading and filtering to search for literature resources. The first step includes reading titles and abstracts to avoid irrelevant research papers and duplicates. The second step covers reading the complete form of the selected manuscripts.

C. Search

This study started in the beginning of January 2021 through the advanced search boxes in WoS, Science-Direct, IEEE Xplore and Springer Nature databases. A compound of different variations of keywords were used, such compound included: 'cooperative',' collaborative', 'distributed', 'intrusion', 'anomaly' and 'attack' to perform this study. These keywords were connected with 'OR' and 'AND' operators. Fig.1 illustrates the query texts used in this study. Journal, chapters and conference articles were considered. the preferences in each search engine to eliminate other types of reports were used. two areas were assumed which consist of the related scientific studies:

- Acceptability measure illustrated in Fig.1 where each article must satisfy such measure. The main aim was to match the study on CIDSs into an overall taxonomy with three sets. Google Scholar used to obtain the initial perception of the background and directions of related papers. If the measure was unjustifiable in the remaining articles after the initial removal of redundant articles, then they were excluded from filtering and reading the papers. An Excel file with a complete list of all the articles from resources with their equivalent initial categories was used for data collection. several full-text readings were obtained then classification of articles was obtained as well.
- Statistical and result information shows that the essential query resulted in 1744 articles in the three databases: 380 in ScinceDirect, 117 in IEEE Xplore and 968 in Springer Nature. This study classifies the research papers which were published during the period 2015 to 2021 into three classes as indicated in Fig.2. After inspection of the titles and abstracts, the number of papers minimized to 76 which covers such classes, meanwhile duplicate articles were 32 out of 76. Then, the full text reading and review excluded 21 papers. Finally, a total of 23 articles remained in the final set given the different topics related to CIDSs technique.

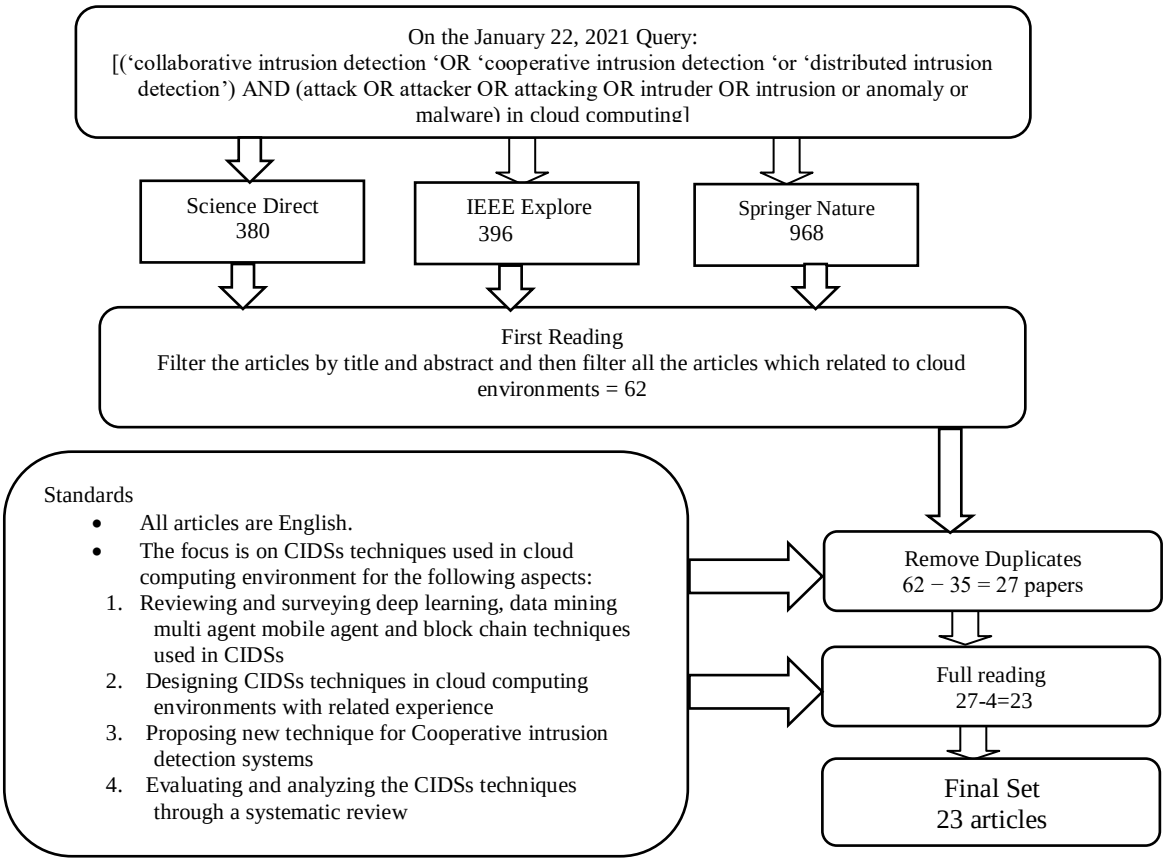

Figure 1 illustrates the query texts used in this study

IV. RESULTS AND FIDING

This section presents important findings of the survey which includes a taxonomy of CIDSs existed in the current state of the art related to the cloud computing environment. Such taxonomy is classified into classes: developed approaches and framework approach. Fig1 illustrates the taxonomy which shows an inclusive improvement in several studies and applications. The first class includes articles associated with development of techniques for CIDSs such as a multiagent systems. The second class includes articles focus on collaborative frameworks for building trustable CIDSs based on data mining techniques and DL. The third class includes articles focuses on the architecture that used as CIDSs in cloud computing. More details on each class as follows:

A. Development methods

This subsection provides a description of the single and the hybrid techniques. It shows 11 subclasses. Such classes cover multiagent system, Naïve Bayes classifier, Denoising Autoencoder, Dendric Cell Mechanism, Binary Segmentation Change and SGD-SVM, Mobile Agent and Blockchain. Each method of this class is based on artificial intelligence concepts and techniques such as data mining, machine learning and deep learning. These methods could be briefly described as follows:

- A distributed intrusion detection system for Cloud environments based on data mining techniques is presented in [3]. The system is designed to be inserted in the edge network components of the cloud provider. This allows intercepting incoming network traffic to the edge network routers of the physical layer within cloud. A time-based sliding window algorithm is used to preprocess the captured network traffic on each cloud router and pass it to an anomaly detection module using Naive Bayes classifier. A set of commodity server nodes based on Hadoop and MapReduce are available for each anomaly detection module to use when the network congestion increases. For each time window, the data of anomaly network traffic on each router are synchronized to a central storage server. Next, an ensemble learning classifiers based on the Random Forest is used to perform a final multi-class classification step for detecting the type of each attack. In addition, the system is implemented in the Google Cloud Platform which use Hadoop and MapReduce to distribute and to scale computations over available clusters.
- An efficient IDS approach [29] which contains a scheme for services provided by cloud computing. The CC provider is required to specify its security such as availability, confidentiality and integrity. Then users of services with similar priority are grouped together and the proper policy will be chosen for each one according to the kind of expected attacks which by experience they are more likely to be prone to. Proper policy means choosing appropriate detection algorithms and also identifying more useful features during detection process. Furthermore, the proposed approach can better adjust to various CC services, and various security attacks.
- Authors in [30] were introduced a distributed IDS that consists of nodes running backpropagation techniques on the cloud platform. This technique has a flexible distributed architecture which could adjust its configuration on the basis of information related to real-time resource usage to avoid overloading any node in the cloud. It provides multiple dimensional results which could be used to not only recognize malicious activities but also find what malicious activities are taking place.
- Adaptive collaboration intrusion detection method presented in [15] for enhancing the safety of a network. A self-adaptive and collaborative intrusion detection model is built by applying the Environments classes, agents, roles, groups, and objects (E-CARGO) model. The objects, roles, agents, and groups are designed by using decision trees (DTs) and support vector machines (SVMs), and adaptive scheduling mechanisms are set up. The KDD CUP 1999 data set is used to verify the effectiveness of the method. The results illustrated the feasibility and efficiency of the proposed collaborative and adaptive intrusion detection method.
- A deep learning approach for proactive multi-cloud cooperative intrusion detection system presented in [1]. Which used stacked denoising autoencoders that enables making decisions about suspicious intrusions even with partial IDS's feedback. This, in turn, accelerates the decision making in real-time environments. Designing a proactive multi-cloud cooperative IDS, which allows us to make decisions about suspicious intrusions proactively without necessity to apply aggregation methods on IDSs feedback. Proposing an approach to extract robust features that yield a better performance in CIDSs.

- A distributed intrusion detection for cloud computing was proposed [2] which includes five components: feature selection, distributed classifier training, distributed attack detection, destination-IP monitoring and aggregation. The feature selection component uses Ant Colony optimization and correlation for selecting the most relevant features in the dataset. The distributed classifier training component is used to train the stochastic gradient descent with port vector machine to achieve distributed detections. The results shown the proposed distributed intrusion detection scheme outperforms existing distributed IDS for clou computing. A real-time working algorithm was proposed to detect DoS in cloud computing based on Dendritic Cell Algorithm [4]. For detecting DoS in Cloud computing environment. The proposed model was tested on ISCX 2012 dataset and the results was promising.
- A multi agent system based distributed IDS(MAS-DIDS) was introduced to identify

  and prevent all anomalies in a cloud environment. This system has a distributed architecture of IDSs that work in collaboration and communicate with each other, in order

to adjust the complexity of cloud networks. Each IDS is composed of a group of dynamic, responsive, and cooperating agents which work together to make the IDS more autonomous and flexible. The MAS-DIDS which combines the two techniques of signature-based and anomaly-based intrusion detection, in order to block both known and unknown attacks within a complex, dynamic and changing environment. Finally, the efficiency and performance of the proposed model are studied in terms of different metrics: detection rate (DR), false positive rate (FPR) and response time [5].

- Swarm intelligence based autonomous distributed denial of service attack was presented in [17] for detecting and preventing DDoS attacks in cloud platform. The model contains four agents: coordination, detection, monitoring and recovery agents. The coordination agent responsible for intercommunication and decision making, the detection agent is activated by monitoring agent for detecting various type of DDoS threats, the monitoring agent keeps watching the entire cloud system while the recovery agent takes the resources allocated for attacker, records IP address and pattern that help in obtaining accurate decision.
- A multi agent approach-based intrusion detection system has been proposed in [18] for collaboration of IDS systems within cloud computing environment. It has used seven agents for both Host and Network which runs independently and communicate with each other to check and identify all malicious in cloud computing.
- A game theoretic-based distributed detection method for virtual machine-to-hypervisor attack in cloud environment was presented a group of mobile agents which act as the sensors of invalid actions and start a noncooperative game wherein players are attackers and intrusion sensors [16]. The attackers are virtual machines leased to users, and the task of detecting the distributed attacks is carried out by intrusion sensors operating along with the hypervisor. The first step is to arrange a noncooperative game, where players take a number of steps representing their behavior on the cloud environment. The detector monitors the behavior of virtual machines and the game continues with creating utility matrix and finding the Nash equilibrium. The location at which Nash point is created and used as a measure to determine whether VM is an attacker or a regular user. To reduce the rate of false alarms, the proposed model is equipped with a threshold which prevents VMs with mostly normal behavior from being blocked after just a few abnormal steps.
- A Distributed Intrusion Detection System using Cloud Computing Infrastructure and Block chain was introduced to making CDIS is robust and reliable for satisfying integrity, consensus, scalability and privacy. The DIDS server performance with a varying load of data shown. There are many other issues like communication delay, the overhead of block chain, cost of implementation [26].
- Different development techniques are summarized in table 1, on the bases of benchmark datasets, intrusion type and evaluation metrics. The top two threat types include DoS, R2L, U2R and probe which contained in KDD99 or NSL-KDD dataset, were used in reference [1],29],[30] accounted for 37%, and both DoS and DDoS which were used in references [2],[4],[19] accounted for 27%. Amongst the reviewed papers 64% associated with detection accuracy,24% of papers were associated with false positive rate ,18% were associated with precision while others associated with different evaluation metrices which described in the same table. Most papers focused on DoS and DDoS because of their important behaviors which can be extremely harmful. The new direction of future research on CIDSs can focus on proactive CIDS.

B. Framework model to adopt as CIDS

This section summarizes and discusses the articles which apply or adopt CIDSs techniques as framework-based in cloud computing environments.

- A cooperative and hyper network intrusion detection system (CH-NIDS) in cloud computing based on Snort and optimized backpropagation neural (BPN) was presented in [24]. The purpose of this framework is to detect networks threats in cloud environment by monitoring the network traffics, while maintaining performance and quality of service. The framework exploits Snort as a signature-based detection to detect known threats, at the same time, it uses BPN for detecting network anomaly. By applying Snort prior to the BPN classifier should detect only unknown attacks, therefore, detection time is reduced. The BPN parameters are optimized to ensure high detection rate, high accuracy, low false positive and low false negative with affordable competitional cost.
- A cloud based cooperative intrusion detection and prevention system(cl-CIDPS). It is an intelligent complete framework that cope with cloud computing circumstances and threats. The cl-CIDPS provides a novel simulation environment to evaluate present and future frameworks without disturbing cloud users. cl-CIDPS is designed to be integrated in a cloud computing environment, supporting the infrastructure layer within the same cloud provider. The system adds several contributions to the rea of IDPS in cloud by proposing an integrated design that consider detection, prevision and login capabilities for applying both signature and anomaly detection. cl-CIDPS was evaluated using a powerful network security simulator tool (Nessi2) which is capable of testing detection unit and communication schemas.
- A Distributed Intrusion Detection System using Mobile Agents in Cloud Computing (DIDMACC) was proposed for detecting the distributed intrusions in cloud [10]. It is used mobile agents to carry intrusion alerts from consumer virtual machines to the management server where correlation takes place. This system can detect the intrusions on virtual machines, identify the vulnerable ports, and can correlate malicious events to detect distributed intrusions in a cloud-based network. Mobile agents are also used to update the signature database at

virtual machines being monitored. Mobile agents are lightweight and flexible software programs that reduce the network load by carrying intrusion-related data and code. DIDMACC provides a scalable and robust intrusion detection system which is a key requirement for cloud networks.

- Multi-cloud cooperative intrusion detection system was presented [13]. It enables IDSs to distributely form trustworthy ISDSs communities by advancing a trust based Hedonic collational game. This game framework allows IDSs to increase their individual detection accuracy in presence of untrusted IDSs and formulate fairness assurance mechanism as Stackelberg game between the well behaving IDSs and the selfish ones that frequently send consolation request to other IDSs.
- A collaborative cloud-based application-level intrusion detection and prevention has been proposed [11]. More specifically, it has been designed as a collaborative intrusion detection architecture made of three levels: the organization level, the domain level and the overarching root level. This hierarchical architecture combined with streaming and clustering offers very good privacy, scalability, accuracy and resilience tradeoffs. Moreover, the adoption of the cloud as a cost-effective and elastic platform allows someone to handle big data generated by millions of applications as alarm streams. Also specify a lightweight Application alarm message exchange format (A2MEF) to support collaboration among the different stakeholders. Finally, design a reputation-based alarm correlation algorithm that manages the iterative and bidirectional relationship between the reputation of involved parties and the accuracy of their reported alarms.
- A DIDS model that solves data storage problem and combines multiple heterogenous sources of alert data on cloud computing and big data techniques [6]. It combines three intrusion detection datasets NSLKDD, MAWILab and DARPA'99 to have a variety of intrusions, also to have only one homogenous dataset and finally make a realistic intrusion detection rate. Databricks tool was used as a unified cloud environment, while Databricks file system (DBFS) was used for loading the datasets on. A ML pipeline model was used for loading, processing combinable dataset. Then Naive Bayesian machine-learning algorithm was used for training the dataset to obtain classification rate of each attack type.
- A deep blockchain framework was designed for a collaborative intrusion detection system that achieves data security and privacy in cloud networks [28]. The framework includes A privacy-preserving technique which is based on blockchain and smart contracts for enabling immutable data exchange, migration between multi-cloud services, accomplishment consensus and data protection to cloud elements. It also includes an intrusion detection method which depends on BiLSTM deep learning algorithm for discovering cyber-attacks from network data migration in cloud systems. The framework was assessed using the network datasets UNSW-BN15 and BoT-IoT. The system's performance is compared with several intrusion detection techniques to determine its effectiveness while deploying it to cloud.
- A DIDS based on hybrid gene expression programming and cloud computing was proposed [27]. This model includes attribution reduction of noise data based on rough set and global intrusion model based on non-linear least squares are applied to improve the efficiency and accuracy of intrusion detection. At the same time the MapReduce programming framework of cloud computing is adopted and the parallelization of the proposed model is performed to enhance its ability to manage massive and high dimensional data. The proposed model shown obvious advantages in terms of false attack rate, detection accuracy rate and average time consumed. it also shown excel ant parallel performance.
- A framework for data security in cloud computing using CIDS was presented for private cloud environment. The benefit of this model enables the end users to get comprehensive information in the event of the distributed attack on cloud [9].

C. Study/test

This section classifies the research papers into subclasses: attacks and malware. The attacks subclass presents articles that studied or tested classifying techniques as an intrusion attack detector. It classifies the research papers on the basis of the type of dataset used, while the malware subclass focuses on research papers that studied or tested classifying techniques as a malware detector. The attack subclass classifies the research papers on the basis of the type of the dataset used in the experiment as follows:

- KDD CUP 99 Dataset

This dataset consists of four classes of attacks called, Probe, DoS, R2L and U2R, and normal network connection. Each record category has 41 features partitioned into seven characters and 34 numerical features. The authors of [1] used DL based on Denoising Autoencoder (DA), which is used as a building block to construct a deep neural network. The power of DA lies in its ability to learn how to reconstruct IDSs' feedback from partial feedback. Once the dataset was created, it was used to train the model. Then, the ability of the proposed model in making decisions about suspicious intrusions was tested, even in the presence of partial/incomplete feedback. Experimental results shown that model can achieve detection accuracy up to 95%.

- NSL-KDD Dataset

The NSL-KDD dataset is divided into five categories: Probe, DoS, R2L, U2R and normal. Three groups of feature attributes, namely content, basic and traffic features, exist in the NSL-KDD dataset. this scheme (D-CIDS) as shown that the proposed A-D-CIDS achieved an accuracy of 99.6%, a detection rate of 99.7% and a false positive rate of 0.03% [6].

- CIDDS-001 Dataset

CIDDS-001 dataset is unidirectional NetFlow data with fourteen features, it contains traffic data from two servers which are OpenStack and External server. The dataset is generated by emulating small business environment which consist of OpenStack environment having internal servers

(web, file, backup and mail) and an External Server (file synchronization and web server). It is deployed on the internet to capture real and up-to-date traffic from the internet. This dataset includes three logs files (attack logs, client configurations and client logs) and traffic data from two servers where each server traffic consists of four week captured traffic data. This dataset consists of large number of traffic instances out of which 153026 instances from External Server and 172839 instances from OpenStack Server. Several experiments were performed on the CIDDS-001dataset, where the data set is split into 60% for training and 40% for testing. In order to simulate the intrusions in the cloud platform a 5 minutes time-based window sampling method is applied to the test set. The traffic records of each time window are divided subsequently to 4 parts, where each record go to a single router. At each one of the routers sides the pre-processing tasks and the anomaly detection are performed. Then the Random Forest ensemble learning is used to detect types of each intrusion. The obtained results of the entire proposed IDS are compared with a standard Random Forest ensemble classifier using the CIDDS-001dataset. The simulation of the proposed model achieved 94.3% at the third router, it also, achieved an accuracy of 89%,92.7% and 91.4% for respectively router 1, router 2 and router 4.

- Miraged dataset

Authors in [6] merged three different datasets to create a composable dataset which are DARPA99, MAWILAB and NSLKDD. The merged dataset consists 1197017 instances with nine classes. The purpose of this dataset is to evaluate intrusion detection systems. The Naïve Bayes algorithm was implemented on the merged dataset. The main achievements shown good performance especially when dealing with intrusions carrying high records number.

- UNB-ISCX-IDS 2012

It is a dataset for DDoS detection attacks, it contains of seven days of recorded network traffics where three days contain only normal activities while the remaining contain multiple five types of attacks. Authors in [4] has used all dataset contains only HTTP distributed of service attacks which contains 9 648000 number of packets with 20 features. The CDoSD has produced a slightly high detection rate and low false alarm rate 94.4% and 5.04% respectively.

- Malware:

The malware subclass focuses on research papers that studied or tested classifying techniques as a malware detector. It classifies articles on the basis of whether the dataset used in the studies is a benchmark or in real time as follows:

- Dataset Benchmark

Distributed Malware Detection based on Binary File Features in Cloud Computing environment presented in [12]. These methods pose at two major challenges. First, these approaches are subjected to a growing array of countermeasures that increase the cost of capturing these malware binary executable file features. Further, feature extraction requires a time investment per binary file that does not scale well to the daily volume of malware instances being reported by those who diligently collect malware. In order to address the first challenge, this article proposed a binary-to-image projection algorithm based on a new type of feature extraction for the malware. To handle the second challenge, the technique's scalability is demonstrated through an implementation for the distributed (Key, Value) abstraction in cloud computing environment.

A Multi-Agent Based Collaborative Mechanism for Anti-Malware Assistance proposed in [8] assists heterogeneous anti-malware tools to collaborate with each other in order to reach a consensual decision about the maliciousness of a suspicious file. MACoMal consists of two main elements: (1) an executable file identification model, and (2) a collaborative decision-making scheme. MACoMal is analyzed with respect to network connectivity and global decision correctness. By leveraging a multi-agent simulation tool and a set of real malware samples.

The authors of [17] presented multi agent depend on DDoS attack detection and prevention system with swarm intelligence gives better performance than the Hidden Markov Models and Cooperative Reinforcement Learning (HMM-CRL) for HMM-CRL and hop-count filtering (HCF). The proposed system in the cloud platform can prevent against various kinds of DDoS attacks with the accuracy of the 98%. These multi agents Coordination agents, Detection agents, Monitoring agents and Recovery agents are coordinated with the particle swarm optimization, which improves the communication stronger and lossless. So, the day-today issue in accessing the cloud service is made easier.

- Real-time Benchmark

The authors of [16] presented a two-stage IDS, which consisted of an anomaly and a signature detection module. These modules are run in real time and may be required for the commands to be given to a robot to enable it to function properly. The first module detected anomalous behaviour by analysing deviations that occur from expected behaviour. The second module aimed to detect misuse by identifying known signatures of malicious activities. A DNN was utilized as the trained anomaly detection module to detect commands that deviate from expected behaviour.

Table 2 provides the evaluation metrics, which are crucial components of every research, used in the related work. These metrics can vary in every research based on the development above. The table lists the metrics used to evaluate CIDSs techniques which are accuracy, precision, recall, F1-score (F-measure), error rate, detection rate, area under the curve, false positive rate, false negative rate, number of packets, training time, false detection rate, running time, true positive rate, true positive, false positive, true negative, false negative and dataset. It obvious that most of the metrics focus on accuracy given the challenges in obtaining a high accuracy rate with a low training time and a low false positive rate.

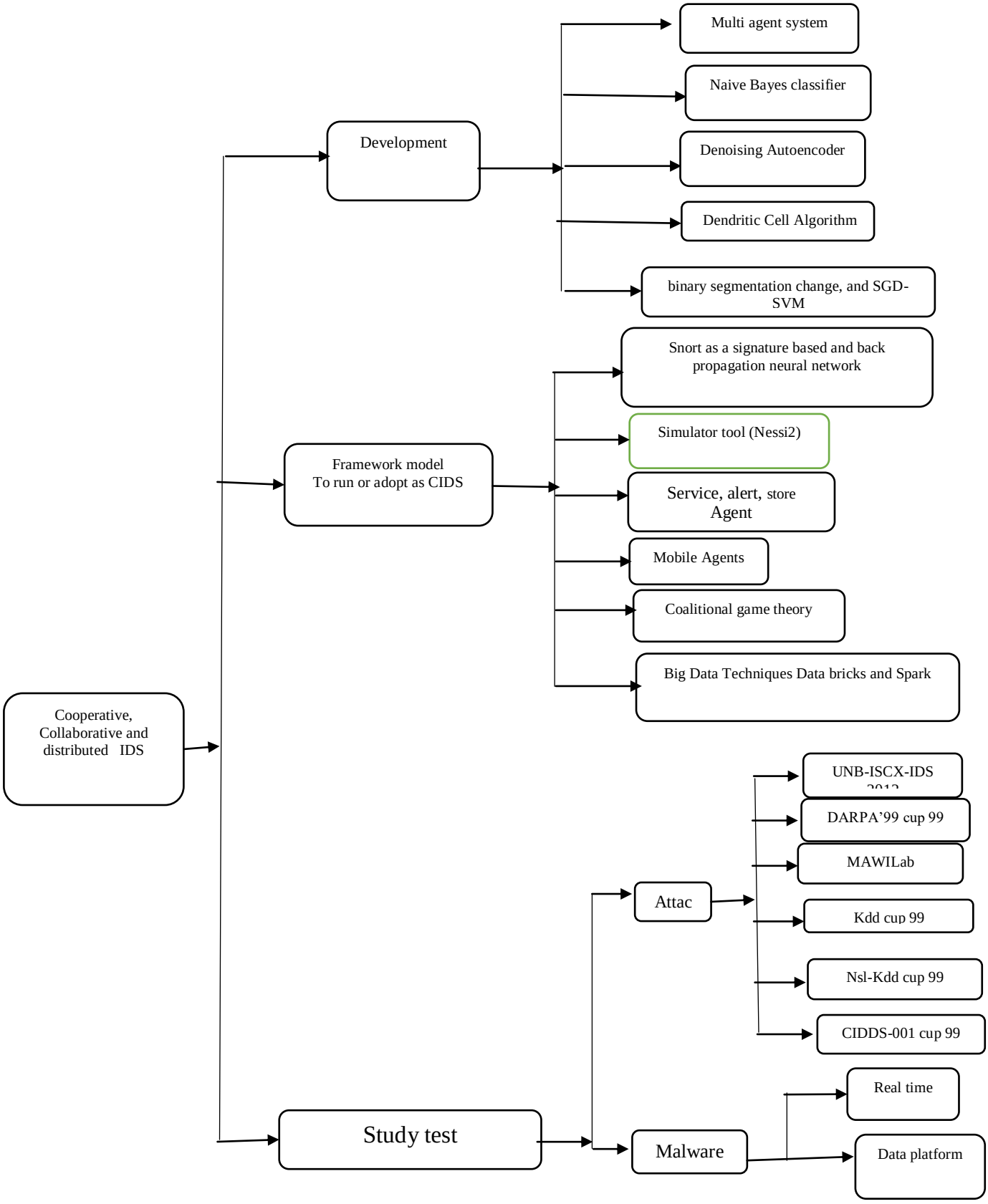

Figure 2 Taxonomy of the literature of CIDSs based on cloud computing

Table 1 development technique analysis

Technique	References	Benchmark data type	Type of intrusion	Evaluation metrics
Binary segmentation change, and SGD-SVM	[2]	Dataset	DDoS	Accuracy, detection rate and false positive rate.
Dendritic Cell Mechanism based approach	[4]	Dataset	DoS	Detection Rate, False Negative False Positive and True Positive
Multi agent system	[17]		DDoS	Attack recovery time, Attack detection time, False attack detection alert, and Accuracy
Denoising Autoencoder	[1]	Dataset	DoS, R2L, U2R and probe	accuracy, and detection rate
Multi agent system	[5]	Dataset	Probing, DoS and R2L	Detection rate and a false alarm rate
Naive Bayes and CRT classifiers	[29]	Dataset	DoS, R2L, U2R and probe	Accuracy and Time of processing
Coalitional game theory	[16]	Dataset	VM side channel, VM escape and Rootkit attacks.	Accuracy and, False attack detection alert
Block chain	[26]	Real dataset		Cost of implementation, communication delay, and the overhead of blockchain
Naive Bayes classifier	[3]	Dataset	DoS, PortScan , PingScan and BruteForce	Accuracy: False Positive Rate (FPR, Running time ROC and AUC curves: Receiver Operator Characteristic (ROC) and Area Under ROC (AUC) curves
Neural networ	[30]	Data set	DoS, R2L, U2R and probe	Accuracy and Time of processing
SVM and DT	[15]	Dataset	TCP, UDP, ICMP intrusion	Accuracy and Time, space of processing

V. DISCUSSION

This section describes and highlights the three aspects namely challenges, motivations, and substantial analysis.

A. Open challenges

These challenges are divided into sub classes shown in Figure 2 which are explained as follows:

- Challenges related to nature of cloud dataset diversity:

There are many challenges take place while the development of success and adaptable CIDSs to unknown features attacks. The first important challenge is an optimal feature selection: the existing dataset of cloud for anomaly detection is irritating. Assuming, intrusion behaviours are constantly changeable and previously selecting features for one class of intrusion may operate ineffectively for another class of intrusion. The second challenge occurs in real life scenarios applications and services in cloud environment may have multi-class datasets [14]. Furthermore, the non-linear manner among the dataset attributes present additional challenges for nodes behaviour recognition. Additionally, labelled traffic datasets inaccessibility by CIDSs presents another challenge. The datasets, which are used to train the models for classification and detection, are characterized by imbalance and a diverse nature.

- Challenges related to data processing:

The use of new cloud techniques enables the reduction of imperfection false rate and thus produces huge amount of network data. The CIDS process is irritating and confusing in terms of accessing and handling the preparation of high volumes of information from un-trustable network methods. Current CIDS have used to handle big data and false negative rate. However new types of intrusion and low false positive rates which may not meet the current requirements of cloud security are being found. Existing problems in CIDSs that use long training periods, some ML techniques and large amounts of data easily get involved in local optima and include redundant information. High dimensional intrusion data and complex attack types cause problems to CIDSs.

- Challenges related to attack information sharing among the distributed IDSs

The main limitation of these CIDSs occur as a result of their complex structure of computing which distributed on large geographic areas. This challenge occurs when sharing attack information among the detection units or distributed IDSs in order to reduce the high rate of false alarm that may result from the inappropriate timing of the transmission of attack information [2].

- Challenges related to delays in making a final decision

There are substantial delays associated with the use of available CIDSs. These delays are mostly occurred as a result of the computation complexity of applying the aggregation algorithms. Such technique depends on many factors: number of consulted IDSs, the IDSs expertise, trust levels, IDSs connections, Internet speeds, busy IDSs and

compromised IDSs. As a result of these delay no guarantee that feedback will be obtained simultaneously. Therefore, decisions on whether or not to rise an alarm about expected intrusions might be significantly delayed because of the missing feedback of a single IDS. subsequently, the decisions generated by the CIDS are ineffective in a real-time setting, making it unbearable [3].

- Challenges related to cloud network attackscloud networks, along with the Internet support and create new business avenues. This scenario makes cloud increasingly vulnerable to hacking. The volume of alerts that require the review of human analysts is a significant problem in cloud intrusion detection. Attack challenges are divided into three classes: growing attack diversity, growing number of hackings and recognition difficulty [20].

- Challenges related to distributed network traffic growth:

current CIDSs paradigm is challenging to develop a given massive cloud network traffic capacities and difficult decision boundaries and highly divers data distribution. TCP-IP model of the Internet lack the necessary features for traffic analysis. To date, most protocol classification systems depend on different parameters, such as static headers, IP addresses and port numbers [20].

- Challenges related to data processing:

The use of new cloud techniques enables the reduction of imperfection false rate and thus produces huge amount of network data. The CIDS process is irritating and confusing in terms of accessing and handling the preparation of high volumes of information from un-trustable network methods. Current CIDS have used to handle big data and false negative rate. However new types of intrusion and low false positive rates which may not meet the current requirements of cloud security are being found. Existing problems in CIDSs that use long training periods, some ML techniques and large amounts of data easily get involved in local optima and include redundant information. High dimensional intrusion data and complex attack types cause problems to CIDSs.

- Challenges related to attack information sharing among the distributed IDSs

The main limitation of these CIDSs occur as a result of their complex structure of computing which distributed on large geographic areas. This challenge occurs when sharing attack information among the detection units or distributed IDSs in order to reduce the high rate of false alarm that may result from the inappropriate timing of the transmission of attack information [2].

- Challenges related to delays in making a final decision

There are substantial delays associated with the use of available CIDSs. These delays are mostly occurred as a result of the computation complexity of applying the aggregation algorithms. Such technique depends on many factors: number of consulted IDSs, the IDSs expertise, trust levels, IDSs connections, Internet speeds, busy IDSs and compromised IDSs. As a result of these delay no guarantee that feedback will be obtained simultaneously. Therefore, decisions on whether or not to rise an alarm about expected intrusions might be significantly delayed because of the missing feedback of a single IDS. subsequently, the decisions generated by the CIDS are ineffective in a real-time setting, making it unbearable [3].

- Challenges related to cloud network attacks

cloud networks, along with the Internet support and create new business avenues. This scenario makes cloud increasingly vulnerable to hacking. The volume of alerts that require the review of human analysts is a significant problem in cloud intrusion detection. Attack challenges are divided into three classes: growing attack diversity, growing number of hackings and recognition difficulty [20].

- Challenges related to distributed network traffic growth

current CIDSs paradigm is challenging to develop a given massive cloud network traffic capacities and difficult decision boundaries and highly divers data distribution. TCP-IP model of the Internet lack the necessary features for traffic analysis. To date, most protocol classification systems depend on different parameters, such as static headers, IP addresses and port numbers [20].

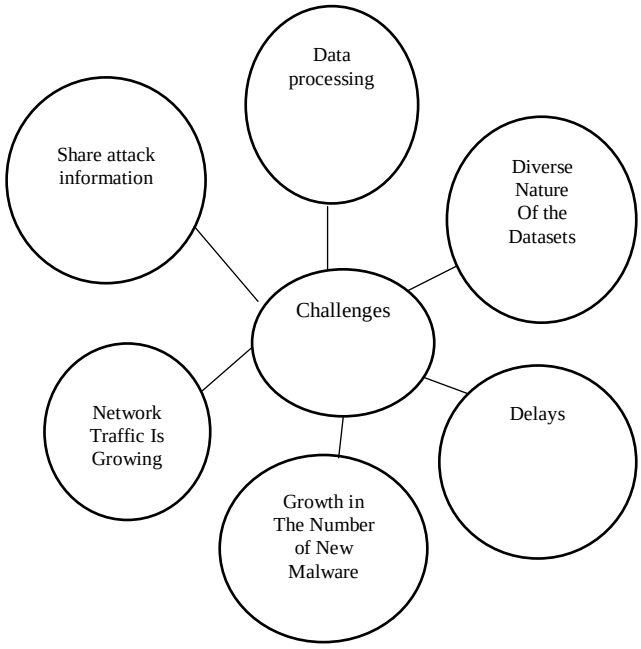

Figure 3 Opens Challenges Subclasses

Table 2 Evaluation metrics

References	acc.	prec.	rec.	f1	er	dr	auc	fpr	tpr	fnr	fdr	nop	tt	rt	ca	tp	fp	tn	fn	ds
[1]	___					__														
[2]	__					__		__												
[3]	__						__	__						__						
[4]						__		__	__	__										
[5]						__		__												
[16]	__										_ _									
[17]	__										__			__						
[29]	__														__	__				
[26]														__						
[30]	__					__							__							
[15]	__																			
total	7					4	1	4	1	1	2		1	3	1	1				

B. Motivations

The motivations are partitioned into four types as follows (Figure. 4).

- Motivation related to response time

Response time has main effect in preventing an attack and blocking an attacker from obtaining access to denied services. Most technologies have been conducted to minimize response time or block the attack at zero hour. These technologies cover CIDSs and prevention systems. The security industry has been exploited in manipulating security threats against cloud associations. CIDSs are security techniques that intelligently observe cloud systems and quickly exploit suitable measures in real time in response to a detected intrusion [5][10][27].

- Motivation related to improving security cloud weakness increases when new digital devices are connected. Hackers could also target cloud to leak information for illegal gains or steal data, such as industrial secrets and personal information. The cloud security is becoming increasingly complicated and attack techniques for hacking cloud continue to develop accordingly and then evolve. Thus, enhancing the accuracy rate of classifiers to effectively identify and detect intrusive behavior is the main motivation of intrusion detection [7][12][24][30].

- Motivation related to developing a powerful detection technique

Cloud has recently obtained considerable attention for security concerns. Various techniques have been presented to detect and fight these security threats [14]. Amongst these studies, signature-based CIDSs have gone through extensive adoption and commercial success. However, they remain ineffective in detecting newly invented threats. The limitation of this type of intrusion detections become the key motivation of using new techniques such as DNN models for CIDSs [1]. The DL is confirmed to be applicable for general and other applications. available antiviruses aim to detect and fix an infected device, but they still need to realize improved security and develop new techniques for new threats [5]. A powerful detection mechanism can be obtained through an improved detection technology. With the development of science and technology, cloud have been increasingly and extensively used. But their distributed nature makes them prone to various invasions. Thus, the security research of cloud computing and other networking is important issue [1],[5],[10],[23],[27].

An intrusion detection technology is a mean to enhance cloud computing security as an active security mechanism. Thus, Effective CIDSs should be designed and implemented to efficiently and intelligently detect attacking attempts in incoming network traffic energy[8][18].

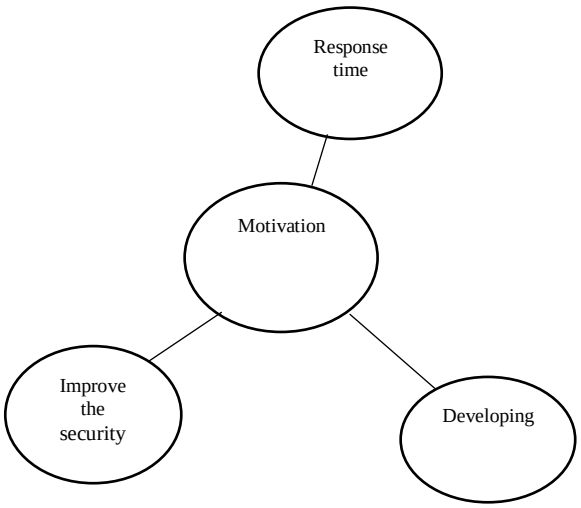

Figure 4 Motivation Partitions

C. Significant Analysis

This section describes the significant analysis performed on the related work. This analysis is divided into 4 parts, as occurred in Fig. 5 The statistics of each division are provided in the related work with the percentage from the total number of related articles as shown in the following subsections

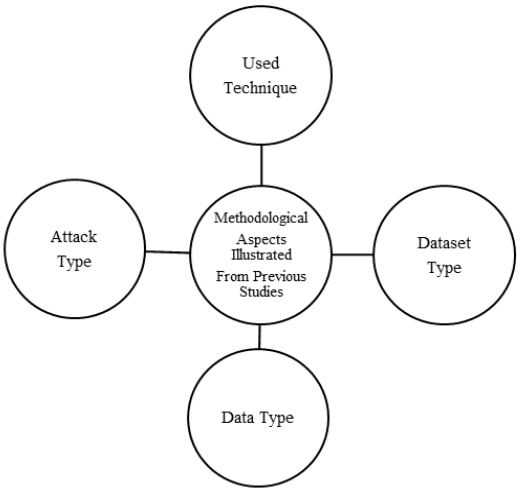

Figure 5 Techniques Types applied in articles

D. Used techniques

data mining are databases, statistics, whereas machine learning involves the algorithm that improves automatically through experience based on data. machine learning is most important technique in the field of data mining. Multiple-agent communication technologies can be used for management and organization of cloud and fog computing. Moreover, Blockchain technique is a structure that saves transactional records in a network connected through peer-to-peer devices. The deep learning techniques are subfields of machine learning (ML) techniques which are important part for building deep learning based CIDSs. Authors of the related articles have generated CIDSs using single or hybrid methods Fig.6 illustrates the techniques and the number of articles that address such techniques. The multi agent was the most commonly used technique to build a CIDSs system with 4/23 articles while each one of SVM and block chain was adopted in 2/23 articles. Naive Bayes classifier, Dendritic Cell, mobile agent, and SDA, had the lowest proportions, with 1/3 reference articles.

E. Benchmark data type

Benchmark data type is categorized into dataset and real time on the basis of the utilization of the proposed model in the related work. In the first category, the proposed models have used dataset to test the trained application. Fig.6 shows that 19/23 articles applied a dataset. In the second category, the proposed models have real time used to test and trained application, also, Fig. 6 illustrates that 4/23 articles applied real time in the related work, in more details:

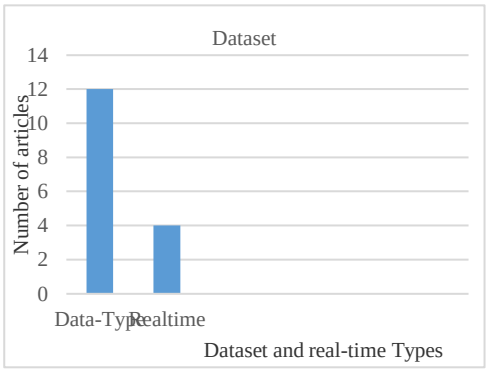

Figure 6 Datasets and real time applied in research papers

Fig.7 shows 6 types of datasets were used in the related research papers. The KDD Cup 99 dataset ranked first with 8/19 research papers of the related work. While the was a generated/collected dataset ranked second with 4/19 articles. In third position was a UNSW-NB15 dataset with 2/19 research papers. In fourth position was a computer malware dataset with 3/19 research papers. The fifth position was combinable of three datasets, namely MAWILab, DARAPA'99 and NSL-KDD ranked with 1/19 research papers. Finally, each one of the following three datasets NSL-KDD, ISCX-2012 and CIDDS-001 ranked with 1/19.

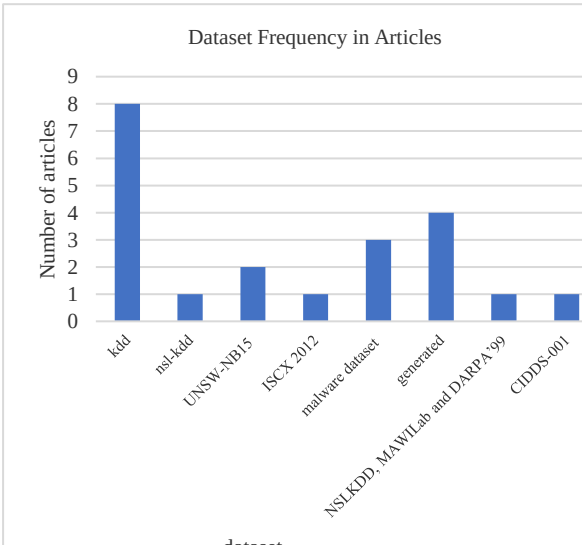

Figure 7 Datasets along with number of articles

F. Attack categories

The related research papers include 8 attacks as illustrated in Fig.8. The first type is a group of attacks includes: Probe, U2R and R2L which were applied by the authors of 5/23 research papers given the usage of the NSL-KDD and KDD cup 99 datasets. The second type is another group of attacks includes:(DoS, PortScan, PingScan and Brute Force which applied by the authors of 2/23. The third type is a malware threat with 3/23 articles. The fourth type consists

of network attacks with 1/23articles. The fifth DDoS attack with 2/23 articles. The sixth type VM side channel, V Manscape and rootkit attacks 1/23 the seventh type is composed of DoS attacks with 1/23 article each. The eighth is PMFA which used 1/23.

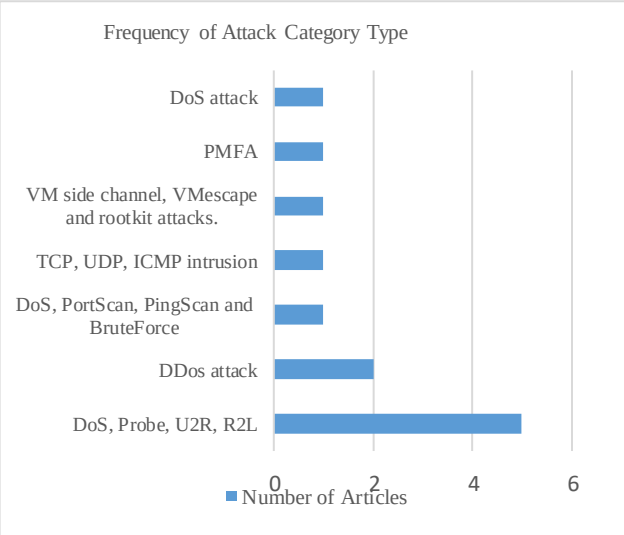

Figure 8 Number of articles along with attack frequency

A. Year of study

The year of study of the related work is a crucial aspect as shown in Fig.9. The interest in CIDSs but it was inapplicable due to the limited processing speed of the computers at that time and the high cost of supercomputers. Many factors emerged in the last 6 years because most developed components have accessible massive to cloud computing and labelled datasets. In 2015, the interest in ML techniques to CIDSs began, and 4/23 articles were introduced. In 2016, interest in this area with 2/23 articles. In 2017, DL attracted further interest with 5/23 articles. In 2018 increased in this area 6/23 The current. In 2019 in this field, we get 4/23. In 2020 in this field 6/23.

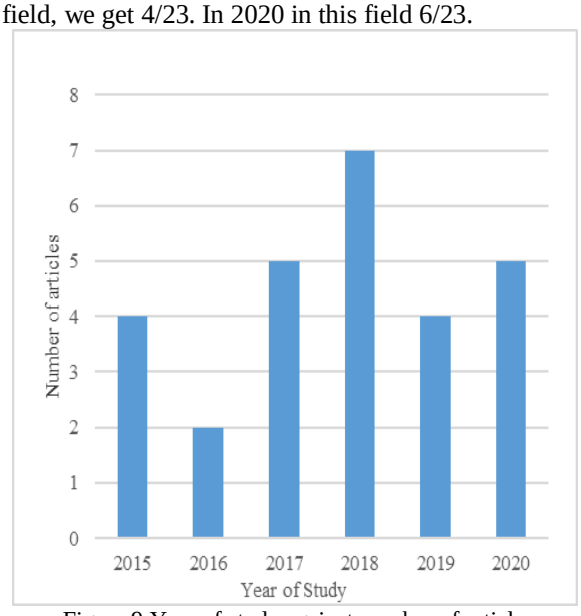

Figure 9 Year of study against number of articles

Unfortunately, the available research studies still have gaps and limitations in terms of proactive CIDSs models performance and their datasets representation. Proactive multi-cloud cooperative intrusion detection systems in contexts of cloud computing are very complicated tasks, they may require well informative and representative multi-class datasets. However, the real multi-datasets contain all kinds of attributes with nonlinear behavior and high dimensionality. These attributes not only increase computational complexity of the underlying algorithm but also deteriorate its performance in terms of making decisions on suspicious intrusion. Thus, some optimal techniques should be employed for selecting an optimal subset of informative attributes, such techniques should concern with datasets dimensionality reduction and effect of non-linear attributes on feature selection. On the one hand, the dimensionality reduction of the dataset can be obtained using a deep learning technique such as Restricted Boltzmann Machine (RBM) which has ability for selecting features, forming clusters at different levels of scale and maintaining consistency of the given feature sets. On the other hand, the effect of non-linear attributes on feature selection can be solved using non-linear estimator such as Unscented Kalman Filtered (UKF). These preprocesses assist in designing a model for enhancing the performance of existing proactive multi-cloud cooperative intrusion detection system.Thus, it is necessary to introduce an ensemble deep learning model which associate with a real time dataset with simple reasonable representation. This may reduce the limitation in the current state of the art related to CSIDSs and to enhance the performance of proactive CSIDSs.

VI. CONCLUSION

This research study reviewed with analysis the current state of the art in CIDSs within cloud computing environment. It concentrated on articles related to the keywords: cooperative, distributed, collaborative, learning and their variations in three major databases. Datasets, ML, Dl and other related techniques were discussed, compared, hence, coherent taxonomy of such techniques was derived, it has specified three main classes: development, framework and datasets. In addition, a methodology of a literature review of related papers was chosen based on the terms mentioned above, then each class of the taxonomy was explained and discussed. The motivations, challenges, and significant analysis of the related research papers were considered, then the result of the analysis was used to depict new directions in deep learning based CIDSs and the accuracy of proactive CIDSs techniques were suggested to point out the gap and the limitation in coming research works that concerned on deep learning based CIDSs models which obtained a higher accuracy rate than the other models applied. On the bases of this survey, a deep based model for improving performance of proactive multi-cloud cooperative intrusion detection system was proposed to meet the requirements for detecting DDoS attacks with a high accuracy rate.

REFERENCES

[1] Adel Abusitta, Martine Bellaiche ∗, Michel Dagenais, Talal Halabi, "*A deep learning approach for proactive multi-cloud cooperative intrusion detection system*", Future Generation Computer Systems, **vol. 98 ,pp. 308–318 2019.**

[2] Nurudeen Mahmud Ibrahim, Universiti Teknologi Johor Bahru, Malaysia Anazida Zainal "*A Distributed Intrusion Detection Scheme for Cloud Computing*", International Journal of Distributed Systems and Technologies ,**vol.11 • Issue 1 pp. 68-82• January-March 2020**

[3] Mohamed Idhammada,_, Karim Afdela, Mustapha Belouchb "*Distributed Intrusion Detection System for Cloud Environments based on Data Mining technique*", Procedia Computer Science ,**vol.127 ,pp. 35–41 ,(2018)**

[4] Azuan Ahmad1, Mohd Nazri Kama2, Azri Azmi2, and Norbik Bashah Idris3 "Collaborative Cloud IDS in Detecting Denial of Service by Dendritic Cell Mechanism", International Journal of Electrical and Electronic Engineering & Telecommunications **Vol. 8, No. 4, July 2019**

[5] Omar Achbarou(&), My Ahmed El Kiram, Outmane Bourkoukou, and Salim Elbouanani "Multi-agent System-Based Distributed Intrusion Detection System for a Cloud Computing", International Conference on Model and Data Engineering MEDI 2018: New Trends in Model and Data Engineering , (CCIS, volume 929), **pp. 98–107, 2018**

[6] Rim Ben Fekih1(&) and Farah Jemili2 "Distributed Architecture of an Intrusion Detection System Based on Cloud Computing and Big Data Techniques", International conference on the Sciences of Electronics, Technologies of Information and Telecommunications

[7] SETIT 2018: Proceedings of the 8th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT'18), **Vol.1 pp 192-20.**

[8] A.A. Ujeniya1*, R.D. Pawar2 , S.A. Sonawane3 , S.B. Shingade4 , S.R. Khonde5, "Hybrid Distributed Intrusion Detection System", International Journal of Computer Sciences and Engineering pp .232-237 **Vol..6, Issue.12, Dec 2018**

[9] Mohamed Belaoued1, Abdelouahid Derhab 2, Smaine Mazouzi 3, And Farrukh Aslam Khan 2 "MACoMal: A Multi-Agent Based Collaborative Mechanism for Anti-Malware", SpecialL Section on Emerging Approaches To Cyber Security, Journal of IEEE Access , VOLUME 8, 2020, **Issue.10, pp.66-75, 2012**. doi: 10.1109/ACCESS.2020.2966321

[10] Upasana Nagar, Priyadarsi Nanda, Xiangjian He , Zhiyuan(Thomas) Tan "A framework for data security in cloud using collaborative intrusion detection scheme", Proceedings of the 10th International Conference on Security of Information and Networks Pages 188–193(2017)

[11] Yasir Mehmood; Muhammad Awais Shibli; Ayesha Kanwal; Rahat Masood, "Distributed intrusion detection system using mobile agents in cloud computing environment", in: 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan,**2015**

[12] Hassani Mohamed; Lebbat Adil; Tallal Saida; Medromi Hicham, "A collaborative intrusion detection and Prevention System in Cloud Computing" , Pointe aux Piments, Mauritius,**2013**

[13] Xiaoguang Han1 , Jigang Sun2 , Wu Qu3, 4*, Xuanxia Yao1, "Distributed malware detection based on binary file features in cloud computing environment", in 2014The 26th Chinese Control and Decision Conference (2014 CCDC), Changsha, China, **pp.438-488**

[14] Adel Abusitta, Martine Bellaiche & Michel Dagenais ,"Multi-cloud cooperative intrusion detection system: trust and fairness assurance Annals of Telecommunications, **vol. 74, pp.637–653(2019)**

[15] A. M. Aleesa1 , B. B. Zaidan2 ,A. A. Zaidan2 Nan M. Sahar1, "Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions" , Neural Computing and Applications **vol. 32, pp.9827–9858(2020)**

[16] Shaohua Teng; Naiqi Wu; Haibin Zhu; Luyao Teng; Wei Zhang, "SVM-DT-based adaptive and collaborative intrusion detection, IEEE/CAA Journal of Automatica Sinica ,**Vol: 5, pp: 108 – 118, Issue: 1, Jan. 2018**

[17] Amin Nezarat1 · Yaser Shams2"A game theoretic-based distributed detection method for VM-to-hypervisor attacks in cloud environment", The Journal of Supercomputing **vol: 73, pp 4407–4427,2017**

[18] R. Kesavamoorthy & K. Ruba Soundar , "Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system", Cluster Computing, **vol 22, pp 9469–9476(2019)**

[19] Omar Achbarou, My Ahmed El Kiram and Salim Elbouanani, "Cloud Security: A Multi Agent Approach Based Intrusion Detection System", Indian Journal of Science and Technology, , **Vol: 10, Issue: 18, pp: 1-6 2017**

[20] Weizhi Meng, Wenjuan Li, Laurence T,Yang & Peng Li , "Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain", International Journal of Information Security **volume 19, pages279–290(2020)**

[21] Nour Moustafa, Gideon Creech, Elena Sitnikova, Marwa Keshk "Collaborative Anomaly Detection Framework for handling Big Data of Cloud Computing", International Journal of Scientific Research in Network Security and Communication, **Vol.1, No.5, pp.1-4, 2013.**

[22] Zouhair Chiba,Noreddine Abghour,Khalid Moussaid,Amina El omri,Mohamed Rida, "Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms", Computers & Security,**Vol 86, pp, 291-317,2019**

[23] Murat Özalp, Cihan Karakuzu, Ahmet Zengin,, "Distributed Intrusion Detection Systems: A Survey", Academic Perspective Procedia, **Vol, 2, Issue 3, Pp, 400-407,2019**

[24] Sahil Garg a,b,∗, Kuljeet Kaur a,b, Shalini Batra b, Gagangeet Singh Aujla c,d, Graham Morgan c, Neeraj Kumar b, Albert Y. Zomaya e, Rajiv Ranjan c, "En-ABC: An ensemble artificial bee colony based anomaly detection scheme for cloud environment ", Journal of Parallel and Distributed Computing **Volume 135** , **pp 219-233,(2020)**

[25] Saadia Ghribi, Amel Meddeb Makhlouf and Faouzi Zarai, "Multi-layer Cooperative Intrusion Detection System for Cloud Environment" In Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) – **Vol: 6: pp:36-44 2017**

[26] P. Patil1* , T. Bagwan2 , S. Kulkarni3 , C. Lobo4 , S.R. Khonde5, "Multi-Attacks Detection in Distributed System using Machine Learning", International Journal of Computer Sciences and Engineering, **Vol..7, Issue.1, pp. 601-605, Jan 2019**

[27] Dr. Manish Kumar1 , Ashish Kumar Singh2, "Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure",in 2020 International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India **pp,248-252 2020**

[28] Song Deng1 , Ai-Hua Zhou2 , Dong Yue1 , Bin Hu2 , Li-Peng Zhu2 , "Distributed intrusion detection based on hybrid gene expression programming and cloud computing in a cyber physical power system", IET Control Theory Appl., **Vol. 11 Iss. 11, pp. 1822-1829,2017**

[29] Osama Alkadi; Nour Moustafa; Benjamin Turnbull; Kim-Kwang Raymond Choo, "A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks", IEEE Internet of Things Journal, ,**pp, 1 - 1 ,2020**

[30] Hamid Reza Ghorbani , Roya Salek Shahrezaie "Toward a Policy-based Distributed Intruison Detection System in Cloud

Computing Using Data Mining Approaches" , in 2015 International Congress on Technology, Communication and Knowledge (ICTCK), Mashhad, Iran, **pp, 412-419,2015**

AUTHORS PROFILE

Montather Ali, he held a B.S degree in Elictrical-Computer and IT, Sana'a University and has finished a preliminary master degree from Faculty of Computer Science and information technology, Sana'a University in 2019, he is interested in cloud computig, data Science , data analysing and security field.

Prof. Fadl M.M Ba-alwi, Professor in Artificial Intelligence (AI), former he worked as

1- A Vice President of the Council for Accreditation & Quality Assurance- Ministry of higher Education & Scientific Research, Yemen.
2- Dean of the faulity of computer scince university.

Currently , he is working as a professor in Faculty of Computer and Information Technology at Sana'a University. He held a Ph.D. in Artificial Intelligence (AI) Data Mining field Computer Science –JNU- New Delhi-India.

Prof. Ghaleb H. Al-Gaphari received his Ph.D. degree in computer science (Artificial Intelligence specialization) from Basrah University, Iraq in 1999. He was a visiting scholar in the University of Pennsylvania, USA, where he did his postdoc in Information retrieval, from 2007 to 2008. Since that time, he worked as a lecturer of artificial intelligence in the computer faculty, in addition to research tasks, he has become a full professor of artificial intelligence in the same faculty in Sana'a University. He is the author of more than 20 articles. His research interests include AI, IR, NLP, Text Summarization, Object Oriented Design, Cloud Computing, Algorithms and Meta heuristic.

