DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison

Mahmood A. Al-Shareeda¹, Selvakumar Manickam¹, Murtaja Ali Saare²

¹National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia
²Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

ABSTRACT

The security of the internet is seriously threatened by a distributed denial of service (DDoS) attacks. The purpose of a DDoS assault is to disrupt service and prevent legitimate users from using it by flooding the central server with a large number of messages or requests that will cause it to reach its capacity and shut down. Because it is carried out by numerous bots that are managed (infected) by a single botmaster using a fake IP address, this assault is dangerous because it does not involve a lot of work or special tools. For the purpose of identifying and analyzing DDoS attacks, this paper will discuss various machine learning (ML) and deep learning (DL) techniques. Additionally, this study analyses and compares the significant distinctions between ML and DL techniques to aid in determining when one of these techniques should be used.

Keywords: Deep learning, Distributed denial of service, Intrusion detection system, Machine learning

Corresponding Author:
Selvakumar Manickam
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
Gelugor, Penang, Malaysia
Email: selva@usm.my

1. INTRODUCTION

Numerous significant websites have recently been subjected to outside attacks. Because they cannot afford any neglect, not even for a brief period, many large corporations and government agencies are exposed [11]–[14]. The present network services should be less susceptible to attacks as a result of any flaws that could result in significant losses for both customers and businesses. Not all modern attacks have the same old goals as making money or getting sensitive information. Some of them are designed to halt services so that users can no longer use the intended service as long as the attacker can do so [5]–[7].

A single botmaster can command a large number of bots (zombies) to transmit a large volume of messages that completely consume the bandwidth in a distributed denial of service (DDoS) assault [8]–[10]. The primary target of a DDoS attack is the central service point. This kind of attack happens extremely quickly. As a result, detecting DDoS attacks is a significantly better security tactic than detecting crackers. DDoS attacks, however, are also updated in tandem with the development of security measures [11]–[13]. Since the former relies solely on the detection of anomalies or anomalous behavior, anomaly-based detection is thought to be more modern than signature-based detection in response to that [14]–[16]. The main motivation of this paper is to investigate the most often used machine learning (ML) and deep learning (DL) techniques for intrusion detection system (IDS), as well as to discuss when it is appropriate to employ each type of technique. The major contributions of this work are listed as follows: i) we present and analyze the related work based on ML and DL to detect DDoS attacks in detail; ii) we display the outcomes of both DL and ML methods based on IDS or DDoS attack detection; and iii) we draw attention to the clear distinctions between DL and ML methods.

Journal homepage: http://beei.org
The remainder of this paper is structured as follows. Section 2 describes IDS and DDoS attacks in details. We present the summaries of ML and DL approaches based on related works in sections 3 and 4, receptivity. Section 5 discuss the related work based on ML and DL approaches. Finally, section 6 concludes this paper.

2. BACKGROUND

2.1. Intrusion detection system

Strategically designed IDS watch network traffic for signs of attacks. IDS will examine the packets to find any potential risks after gathering information from networks and watching the traffic. The IDS can be categorized in a variety of ways, according to various studies, including Debar et al. [17] and Hindy et al. [18]. They have previously developed questionnaires and taxonomies to categorize IDS. This study will be based on the classification of [19], where they combined a sober classification with earlier trustworthy classifications and added DL to it. Host-based, network-based, or a hybrid of the two are the three types of data collection. On the basis of location, these sources are grouped. The IDS come in two different models. First, IDS is based on signatures (SIDS), which is reliant on appearances prior to attacks. Without possessing the attacks’ specific signatures, this style cannot detect attacks. Anomaly-based IDS (AIDS), the second approach, does not rely on plans of attack, in contrast to the signature-based model.

This paper will focus on anomaly-based IDS, which is the most effective strategy. One of AIDS’s most frequently cited benefits is its capacity to identify previously unidentified attacks by spotting an anomaly in network traffic. From a different angle, AIDS might be an IDS that is either self-learning or programmed. By developing a method for the fundamental operations with the allocated network traffic accumulated over a constrained period of time, self-learning AIDS is accomplished [20]. More specifically, users are the ones who decide how out of the ordinary a behaviour is in the system [21].

2.2. Distributed denial of service attack

DDoS attacks intimidate networks at the moment since they target sensitive and significant centers. Furthermore, DDoS attacks are growing quickly, leaving little time for a proper response [22], [23]. New DDoS launch platforms, such Ox-booter, appeared in late 2018, according to Kaspersky Lab. These services support attacks with additional bandwidth of up to 420 Gb/s and more than 16,000 infected bots. Due to its simplicity and low price, this platform is extremely risky. Anyone can use this straightforward interface to execute one of numerous attacks against their target for only $20 to $50. Due to the low cost, attackers today do not need specialised tools or extra effort to damage their target. To put it another way, these illicit platforms that promote DDoS attacks were using internet of things (IoT) devices to conduct this attack [24]. Additionally, a DDoS attack is simple to execute because to the IoT, which allows the Internet to pervade practically every aspect of human existence [25].

2.3. DDoS attack

DDoS attacks are currently regarded as the most dangerous assaults on the internet. DDoS attack perpetrators try to stop authorised users from using services. These attacks pose a risk due to the possibility of simultaneous attack from multiple sources. Therefore, until it is blocked, it will be hard to reveal the actual IP address that causes this harm. DDoS assaults also use legitimate channels to send a tonne of messages. When this happens, the packets will come from trustworthy websites like colleges or companies that cannot be censored or shut down [26]. DDoS assault is simply depicted in Figure 1.

![Diagram of DDoS attacks](image-url)

**Figure 1. DDoS attacks**
Think of the hypothetical situations where victim ‘Y’ has an IP address of 2.2.2.2 and attacker ‘X’ has an IP address of 1.1.1.1. Using IP address ‘Y,’ ‘X’ can send request packets to example.com. Then, “X” requests information from example.com, such as “tell me all you know about “Z,” in addition to saying “hello.” Following that, example.com will give ‘Y’ IP address a tonne of information that the attackers don’t actually need. Additionally, an attacker “X” can request that example.com, example1.com, and example2.com give him or her “Y” IP address with a massive data set that is larger than “Y’s” actual storage space.” One outcome is that “Y” might not be able to respond to inquiries or carry out his duties.

Figure 2 illustrates the types of DDoS attacks with their examples. DDoS assaults typically fall into one of three categories: i) volume-based attacks, attacks that flood a target with a large volume of traffic in an effort to take advantage of its bandwidth; ii) protocol-based attacks, attacks that take advantage of a layer 3 or layer 4 vulnerability by consuming the processing power of the attacker target or middle-level crucial resources like a firewall, which can result in service interruption; and iii) application layer attacks, attacks that connect to a victim in a reasonable way to take advantage of a vulnerability in layer 7 and use transactions and monopolising processes to overtax the server’s resources.

Figure 2. DDoS attack types with their examples

3. MACHINE LEARNING BASED FOR IDS

Because a signature-based IDS takes a long time to develop, test, and deploy everytime an unexpected assault happens, there is an urgent need to rely on less human reliant solutions in IDS. By offering a system that can learn from data and deliver predictions about the unseen data by employing the learnt data, anomaly-based IDS based on ML technology provides a solution for this problem [28]. The most typical use of ML techniques will be covered in the sentences that follow. Additionally, a detailed description of each approach used in IDS will be added along with recent relevant publications [29]. The several types of ML IDS are shown in Figure 3. Table 1 lists the method and advantage of ML approaches in details.

Figure 3. ML techniques

3.1. Naive Bayes

The classification procedure is carried out using this technique, which is based on bayesian networks. Naive Bayes (NB) is regarded as the simplest and most straightforward method for creating classifiers. Class labels for issue scenarios are specified by the classifiers. The classifier then displays feature value vectors. The class labels will have been drawn based on a few particular sets. Fadhil et al. [30] suggested a method for developing DDoS attack detection that involved statistically analysing network traffic using NB. As a properly designed, practically implemented model for DDoS attack detection, in [31] also used the NB classifier.
Table 1. Method and advantage of ML approaches

<table>
<thead>
<tr>
<th>Method</th>
<th>Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fadlil et al. [30]</td>
<td>Create a new method for detecting DDoS attacks. Anticipated to function in conjunction with IDS to forecast the occurrence of DDoS attacks.</td>
</tr>
<tr>
<td>Ye et al. [32]</td>
<td>It is followed by the extraction of the switch flow table’s 6-tuple characteristic values and the creation of a DDoS attack model. Our work is useful for identifying DDoS attacks in software defined networking (SDN).</td>
</tr>
<tr>
<td>Lucky et al. [33]</td>
<td>Deployed in low-cost settings for effective, speedy detection and mitigation of DDoS attacks. The design is examined, and the findings demonstrate that the new architecture adds no extra burden to the monitored network.</td>
</tr>
<tr>
<td>Putri et al. [34]</td>
<td>On the testbed ISCX dataset, Snort finds up to 42 alerts of a DoS assault. Because of the disparity in accuracy between value and the clustering tool WEKA, mnef-cluster data packets are randomly chosen from a data value pack and utilised to calculate the centroid’s value.</td>
</tr>
<tr>
<td>Chaudhary and Shrimal [35]</td>
<td>The goal of this study is to create a genetic algorithm-based IDS for DDoS attacks in MANETs. According to the implementation results, the suggested IDS, which is based on evolutionary algorithms, can effectively identify DDoS attacks on MANETs.</td>
</tr>
</tbody>
</table>

3.2. Support vector machine

Vapnik was the first to suggest this approach, and since then it has shown excellent outcomes to garner more interest in ML research. SVM can perform regression and classification using supervised learning [36]. A dataset that includes the DDoS assault was produced by Subbulakshmi et al. [37] who subsequently worked to identify this attack using enhanced support vector machines (ESVM). By merging the SVM classification techniques, Ye et al. [32] created a model for DDoS attack detection in 2018.

3.3. Decision tree

One of the most popular and basic methods used in data mining and ML is the decision tree. The category-targeted value is determined using observations about a category and a decision tree as a protection mechanism. As a result, it will categorise data in accordance with the previously learnt dataset [38]. A decision tree-based method was created by Zekri et al. [39] for automatically and successfully identifying signature-based DDoS flooding assaults. A ML model capable of learning from assault patterns according to both anomaly-based DDoS attack detection and signature-based DDoS attack detection were created in [32] as well, taking advantage of both of their advantages.

3.4. Artificial neural network

In order to execute computational tasks, a set of basic neurons were originally introduced to artificial neural network (ANN) in 1943 by McCulloch and Pitts. These neurons had functioning that was identical to that of biological neurons, and they resembled biological networks [40]. In order to identify and mitigate known and unidentified DDoS attacks in a real-time setting, Saied et al. [41] developed a model. Seven writers created a paradigm for danger assessment of IoT utilising ANN to counter these attacks within the framework of [42].

3.5. K-mean clustering

One of the most popular methods for dividing a dataset into K groups is clustering. This approach refines the K initial cluster centers in a data set by each case that will enter the nearest cluster center after first identifying the initial cluster centres. To identify DDoS attacks of unknown sessions, Hao et al. [43] developed a detection algorithm. Suggested a method for identifying DDoS attacks using the clustering algorithm of K-means, and they attained a 97.83% accuracy rate [33].

3.6. Fuzzy logic

This method was developed using fuzzy set theory. This theory’s reasoning, which is based on conventional predicate logic, is approximate rather than precise. In order to distinguish malicious packets from legitimate traffic and take appropriate action to prevent DDoS attacks, Iyengar and Ganapathy [44] developed a fuzzy logic model according to a set of predetermined rules. A mechanism for anticipating and detecting DDoS assaults in IEEE 802.15.4 was developed by an author of Balarengadurai and Saraswathi [45] by utilising fuzzy logic algorithm.

3.7. Genetic algorithms

One of the most common ML methods that is according to evolutionary concepts is this algorithm. To put it more plainly, this method approaches problem-solving much like a biological examination [46]. A developed method based on evolutionary algorithms for DDoS attack detection in mobile ad hoc networks was proposed by Chaudhary and Shrimal [34] in 2019. A scalable, real-time traffic mode analysis based on DDoS attacks detection using machine learning and deep learning techniques: ... Mahmood A. Al-Shareeda}
evolutionary algorithms has been developed by [47] for the detection and mitigation of DDoS assaults on the Hadoop distributed processing infrastructure.

4. DEEP LEARNING BASED FOR IDS

As an early technique to identify aberrant behaviour in a network, ML-based intrusion detection methods were criticised for their shortcomings, including low throughput and high false positive rates. It has been demonstrated that deep networks offer benefits through the traditional detection based on ML techniques in hodo’s study of intrusion detection technologies [19]. A method is utilised to train layers of hierarchical networks utilising unsupervised learning greedily with prehensility, taking inspiration from the human brain. Other methods that rely on the fundamentals of DL have been developed since the discovery of deep networks. Deep networks architecture has typically been divided into two categories: generative architecture and discriminative architecture [19]. The two primary structures and the included approaches are shown in Figure 4. Table 2 lists method and advantage of DL approaches in details.

![Deep Learning](image)

**Figure 4. DL techniques**

<table>
<thead>
<tr>
<th>Method</th>
<th>Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tang et al. [48]</td>
<td>An IDS for SDNs that is enabled by gated recurrent unit RNN (GRU-RNN) Our test findings demonstrate that the proposed GRU-RNN does not impair network performance</td>
</tr>
<tr>
<td>Farahnakian and Heikkonen [49]</td>
<td>A strategy that uses DL for IDS. One of the most well-known DL models is used in our method, called DAE To prevent overfitting and local optimum, the proposed DAE model is trained in a greedy layer-wise manner</td>
</tr>
<tr>
<td>Elsaeidy et al. [50]</td>
<td>A system for smart city intrusion detection based on restricted boltzmann machines (RBMs) The effecti veness of the suggested method in very accurate attack detection. Additionally, the suggested approach performs better than the classification model used without the features learning stage</td>
</tr>
<tr>
<td>Imamverdiyev and Abdullayeva [51]</td>
<td>Comparison of the suggested method’s accuracy with that of gaussian-bernoulli RBM, DBN type DL approaches, and bernoulli-bernoulli RBM on DoS attack detection is provided The suggested multilayer deep gaussian-bernoulli type RBM yields higher accuracy.</td>
</tr>
<tr>
<td>Liu et al. [52]</td>
<td>To increase the validity and effectiveness of feature extraction, a convolutional neural network (CNN) modelling approach for intrusion detection was applied. The convolution kernel was chosen and convolved with the data to extract local correlation The new approach can raise classification accuracy for jobs involving intrusion detection and recognition</td>
</tr>
<tr>
<td>Mohammadpour et al. [53]</td>
<td>Suggest using DL to create an efficient and adaptable network intrusion detection system (NIDS) The learning process for IDS can be used with CNNs (IDSs)</td>
</tr>
</tbody>
</table>

4.1. Generative architecture

The goal of generative models is to depict the existing systems graphically. These graphical representations show distributional dependence. These graphs have nodes and arcs in them. The relationships...
between the nodes, which can have millions of parameters, are represented by arcs, which stand in for random variables [54], [55].

The shared statistical distribution thus represents the nodes’ and their associated variables’ products [56]. In addition, there are factors that are hidden from view in the graphical models. The labels of the data are not necessary for generative model training. These models are therefore connected to supervised learning. For classification purposes, these models go through an unsupervised learning pre-training stage. The lower layers were taught separately from the other layers during a pre-training step, enabling the other layers to be trained one layer at a time, starting at the bottom and working up. After pre-training, all subsequent layers will be trained [56]. Deep auto-encoders (DAE), recurrent neural networks (RNN), deep belief networks (DBN) and deep boltzmann machines (DBM) are the four sub-classes of generative models.

4.1.1. Recurrent neural network

Both supervised and unsupervised deep generative networks fall under this category. In order to boost model dependability, the RNN model uses a sort of architecture called a feedback loop that links layers one after another in addition to storing the data from the most recent input [57]. IDS was trained using KDD Cup’99 by [58] utilising RNN with long short-term memory (LSTM) architecture. In SDN-based networks in 2018, Tang et al. [48] used RNN for IDS.

4.1.2. Deep auto-encoder

One of the categories of generative models is DAE. There are various variations, including stacked auto-encoder and denoising auto-encoder [59]. To avoid learning its identity function, the auto-encoder trains in a bottleneck structure where the hidden layer is more tethered than the input layer [60].

The proposed method, which relies on a DAE to detect attacks, was tested using the NSL-KDD dataset in [61]. In order to aid in the detection of intrusions, this experiment employed bottleneck characteristics to the dimensionality reduction of the large amount of data. Using a DAE, Farahnakian and Heikkonen [49] developed a solution for an IDS in 2018.

4.1.3. Deep boltzmann machine

When trained on a large volume of unlabeled data and fine-tuned with labelled data, DBM is one of the generative architectures that is regarded as a decent classifier. A link exists between the input units and the hidden units in DBM but not between units on the same layer. DBM is therefore a unidirectional graphical model [62]. Deep RBM was used by Elsaiedy et al. [50] in 2019 to extract high-level characteristics. After that, apply the newly learnt features to the identification of various DDoS attacks. The deep RBM model’s learned features were quite useful and noteworthy. An approach to identify DoS attacks based on a deep RBM model was proposed in 2018 by Imamverdiyev et al. [51].

4.1.4. Deep belief networks

DBN is created by stacking DBM with one or more hidden layers. Using data that has been labelled, RBMs can learn a common probability distribution of training data. It is regarded as a probabilistic generative model as a result [63]. To minimise the dimensionality of the features in this work [64], they have chosen features layer by layer using the DBN technique. The capabilities of DBN were used by Alom et al. [65] for intrusion detection. The proposed approach, which was evaluated on the NSL-KDD dataset, is capable of both detecting and categorising assaults.

4.2. Discriminative architecture

The second class of deep network architecture is discriminative architecture. The discriminative power of this model, which is determined by describing the posterior distributions of conditioned classes from the input data, determines how well it can classify data. Discriminative architecture has two subclasses: RNN and CNNs.

4.2.1. Recurrent neural network

In order to convert the output of an RNN employed as a discriminative model for training data into labelled data, pre-segmentation and post-processing are necessary. When the output data explicitly follows the input data sequence and is labelled, RNN also uses the discriminative power for classification [66].

4.2.2. Convolutional neural network

CNN is the second kind of discriminative deep networks, along with several convolutional and gathering layers stacked in an array to produce a multi-layer neural network [65], [67]. The max pooling layer should come after each convolutional layer. Finally, the fully-connected layer is formed nonlinearly by stacking various traditional and max pooling layers in the neural system [68]. KDD Cup’99 was utilised by...
Liu et al. [52] to test the CNN-based suggested model. A powerful and adaptable NIDS that uses CNN was proposed by Mohammadpour et al. [53] for use with the NSL-KDD dataset.

5. RESULTS AND DISCUSSION
In this section, we present the summaries of ML and DL approaches based related works mentioned in sections 3 and 4, respectively. The papers that use ML approaches to detect DDoS assaults are compiled in Table 3. While, the related works that based on DL techniques are summarized in Table 4.

<table>
<thead>
<tr>
<th>Table 3. Summary of ML-based related works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technique</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Fadil et al. [30] NB</td>
</tr>
<tr>
<td>Ye et al. [31] SVM</td>
</tr>
<tr>
<td>Zeki et al. [39] Decision tree</td>
</tr>
<tr>
<td>Lucky et al. [32] Decision tree</td>
</tr>
<tr>
<td>Putri et al. [33] K-mean clustering</td>
</tr>
<tr>
<td>Chaudhary and Shrimal [34] Genetic algorithm</td>
</tr>
</tbody>
</table>

Table 4. Summary of DL techniques-based related works

<table>
<thead>
<tr>
<th>Technique</th>
<th>AC (%)</th>
<th>Accuracy</th>
<th>Data-set used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tang et al. [48] RNN</td>
<td>89</td>
<td>IDS in SDN</td>
<td>NSL-KDD</td>
</tr>
<tr>
<td>Farahnakian and Heikkonen [49] DAE</td>
<td>96.53</td>
<td>IDS</td>
<td>KDD-CUP’99</td>
</tr>
<tr>
<td>Elsaedi et al. [50] DBM</td>
<td>-</td>
<td>Features extraction</td>
<td>Smart water distribution plant</td>
</tr>
<tr>
<td>Imamverdiveyev and Abdullayeva [51] DBM</td>
<td>-</td>
<td>DoS detection</td>
<td>NSL-KDD</td>
</tr>
<tr>
<td>Liu et al. [52] CNN</td>
<td>97.7</td>
<td>IDS</td>
<td>KDD 99</td>
</tr>
<tr>
<td>Mohammadpour et al. [53] CNN</td>
<td>99.97</td>
<td>IDS</td>
<td>NSL-KDD</td>
</tr>
</tbody>
</table>

Additionally, DL and ML methodologies diverge significantly. The situations in which ML or DL approaches are most appropriate could be determined with the help of these points. After summarising related works based on both ML and DL method, significant points have been identified. For instance, when the amount of data was larger, DL approaches outperformed ML techniques in terms of accuracy. The key distinctions between DL and ML are outlined in Table 5.

<table>
<thead>
<tr>
<th>Table 5. ML and DL comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML</td>
</tr>
<tr>
<td>A subset of AI is ML</td>
</tr>
<tr>
<td>With little data, ML was able to attain high accuracy and detection rates</td>
</tr>
<tr>
<td>Faster to train a model</td>
</tr>
<tr>
<td>More human engagement and effort are needed for ML</td>
</tr>
<tr>
<td>Various characteristics and classifiers must be tried in order to get the best results</td>
</tr>
<tr>
<td>The output is typically a numerical number, such as a score</td>
</tr>
</tbody>
</table>

6. CONCLUSION
More than 25% of internet users in 2018 used IPv6 networks, according to the internet society. As a result, IPv6 networks will be completely dependent on the internet, particularly in light of the IoT and its enormous IP requirement. This indicates that future networks’ data will be larger than IPv4 networks’ data. IPv6 networks are additionally quicker than IPv4 networks. DL approaches are anticipated to yield higher accuracy and detection rates in the new networks as a result of the comparison in this research. In spite of everything, ML techniques have been fully applied to the detection of DDoS attacks, and they have produced the above-mentioned excellent results. DL methods are still thought to be superior methods for handling larger amounts of data. Additionally, assaults have their own ever evolving defences against IDS. Although not on IPv6 networks, DL techniques have been employed for DDoS attack detection. The outcomes of both ML and DL strategies based on DDoS attack detection or IDS are shown in this paper’s conclusion. This paper also emphasises the clear distinctions between DL and ML methods. In future work, we extend this work by proposing new model to detect DDoS attacks for IDS.


BIOGRAPHIES OF AUTHORS

Mahmood A. Al-Shareeda obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He is currently a Postdoctoral Fellow at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include network monitoring, Internet of Things (IoT), vehicular ad hoc network (VANET) security and IPv6 security. He can be contacted at email: alshareeda022@gmail.com

Selvakumar Manickam is currently working as an Associate Professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include Cybersecurity, Internet of Things, Industry 4.0, and Machine Learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 Ph.Ds. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.

Murtaja Ali Saare Murtaja Ali Saare is an Assistant Professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master’s degree in Information Technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph.D at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work in reputable scopus indexed journal. He can be contacted at email: m_murtaja88@gmail.com and murtaja.a.sari@sa-uc.edu.iq.