Information Sciences Letters

Volume 12
Issue 3 *Mar. 2023*

Article 42

2023

Using Artificial Intelligence and Cybersecurity in Medical and Healthcare Applications

Ahmad A. Alzahrani
Department of Information Systems, College of Computers and Information Systems, Umm-AlQura University, P.O.Box 8XH2+XVP, Mecca 24382, Saudi Arabia, aalzahrani@uqu.edu.sa

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/120343

Using Artificial Intelligence and Cybersecurity in Medical and Healthcare Applications

Ahmad A. Alzahrani

Department of Information Systems, College of Computers and Information Systems, Umm-AlQura University, P.O.Box 8XH2+XVP, Mecca 24382, Saudi Arabia

Received: 16 Jul. 2022, Revised: 10 Jan. 2023, Accepted: 14 Jan. 2023.
Published online:1 Mar. 2023.

Abstract: Healthcare fields have made substantial use of cybersecurity systems to provide excellent patient safety in many healthcare situations. As dangers increase and hackers work tirelessly to elude law enforcement, cybersecurity has been a rapidly expanding field in the news over the past ten years. Although the initial motivations for conducting cyberattacks have generally remained the same over time, hackers have improved their methods. It is getting harder to identify and stop evolving threats using conventional cybersecurity tools. The development of AI methodologies offers hope for equipping cybersecurity professionals to fend against the ever-evolving threat posed by attackers. Therefore, an artificial intelligence-based Convolutional Neural Network (CNN) is introduced in this paper in which the cyberattacks are detected with more excellent performance. This paper presents unique conditions using the Ant Colony Optimization based Convolutional Neural Network (ACO-CNN) mechanism. This model has been built and supplied collaboratively with a dataset containing samples of web attacks for detecting cyberattacks in the healthcare sector. The results show that the created framework performs better than the modern techniques by detecting cyberattacks more accurately.

Keywords: Cybersecurity, Deep learning, Ant Colony Optimization, Convolutional Neural Network.

1 Introduction

Technologies are being developed to simplify our lives, advancing quickly every day. This technical innovation has been highly beneficial to the healthcare business. It facilitates completing any lengthy and laborious task and enables medical professionals like doctors to use this incredible technology safely. Before technology was brought to the healthcare sector, staff members had to perform duties manually, and patients had to sit through lengthy examination wait times [1]. Patients only communicated with the doctors through hospital visits, phone calls, and texts. The patient's condition could not be continuously monitored to provide an immediate and precise diagnosis. IoT and AI in the healthcare industry have the potential to significantly alter medical assessment, medical diagnostics, and patient treatment. John McCarthy first used the phrase "artificial intelligence" (AI) in 1956 at a symposium on the subject. The area of computer science known as artificial intelligence (AI) focuses on creating intelligent computer systems that resemble human intellect [2]. The processing of natural language, learning, and planning capabilities of machines enable intelligent systems to carry out new activities. Artificial intelligence (AI) is primarily used to simulate human brain abilities and carry out tasks ordinarily handled by humans. AI is a single, autonomous electronic entity that performs similar functions to a human healthcare professional.

A network of actual objects that can communicate and share information is known as the Internet of Things (IoT). The term "Internet of Medical Things" refers to sharing information utilizing connected IoT devices in healthcare (IoMT). To analyze detailed medical information, analyze logic, predictive analysis, complete specific tasks, and resolve issues without any human contact or input, artificial intelligence in healthcare is a method that employs various tools and algorithms to imitate human intelligence [3]. AI is a group of multiple technologies. Wearable technology, bio-sensing or fitness trackers, and hospital instruments are all examples of IoT devices employed in the healthcare industry. The medical information gathered may be EHR, claims, patient registries, health surveys, or information from clinical trials. AI is the most efficient method for processing all vast amounts of data and doing precise actual analysis. These innovations give up new avenues for intriguing options, including lowering doctor-patient visits, tracking long-term illness victims in real-time, helping patients to regain, and providing healthcare to remote areas [4]. For any latest tech, security is a concern, and this is

*Corresponding author e-mail: aalzahrani@uqu.edu.sa

no exception. Medical data theft involving IoT devices is a matter of life and death. Patients may become powerless if their pacemaker, dialysis machine, or oxygen delivery system is connected to the internet and open to many attacks. The confidentiality and safety of the gadget, the patient, and the hospital may all be in danger when using IoT - connected technologies in healthcare [5].

The ability to be integrated with existing technologies is a crucial aspect of AI technology [6]. Numerous fields, including chemistry and medicine, where AI-assisted computers start routine diagnoses, have profited from AI. Computer programming, economics, chemistry, biology, physics, astronomy, neurology, and social sciences are just a few of the many fields it encompasses. Cybersecurity is one of the most challenging issues that artificial intelligence is well suited to handle. Our lives are being transformed by this enabling technology [7]. Everything will become "smarter" and more effective if it is integrated into our homes, vehicles, and gadgets. Whether a piece of software is malicious or not, AI can identify it. The world can become more secure, fair, and ecologically sustainable thanks to new AI capabilities. Artificial intelligence-based approaches can assist us in overcoming the limitations of traditional cybersecurity tools due to their adaptability and flexibility [8].

Businesses now rely on artificial intelligence (AI) technologies to support security analysts in providing quick and accurate responses to threats. Additionally, they help with network and sensitive data security [9]. Threats and other malicious actions can be found using AI. It can examine user activity, establish patterns, and pinpoint various issues in a computer network. It can adjust and react to a world that is constantly changing. It advances the analysis, research, and comprehension of cybercrimes by cybersecurity professionals. The ability of machine learning to recognize and respond quickly to potential issues in cybersecurity is a significant advantage. Data security is more crucial than ever right now. Hackers are becoming more intelligent and creative at exploiting the sensitive data of people, businesses, and organizations every day. Data toxicity, cyber-attacks, failures, new cyberattacks, data bridging, and data leaks are reported practically daily. Organizations, companies, governments, and customers who use communications systems are at risk from cybercriminals. Cyberattacks have been one of the top five most likely sources of severe and worldwide danger. Malicious hackers are growing more skilled daily, and cyberattacks are becoming increasingly complicated. This forces businesses and other network users to pay recently emphasized to their network security.

Cybersecurity is the term for the science and methods used to safeguard networks and data against harm or unauthorized access. It is essential because a large amount of information is gathered, processed, and stored by businesses, organizations, and military organizations. Cybersecurity can take various forms, including those used by the armed forces, enforcement agencies, courts, companies, transportation, intel agencies, and data management. Cybersecurity is a dynamic, multidisciplinary field that integrates crime, data management, and computer science. Reliability, identification, secrecy, non - repudiation, and integrity have been the security goals. Networks used by corporations, banks, organizations, and authorities are all at risk from cyberattacks. They range from group actions to unlawful citizenry by specific individuals. Ransomware, extortion, refusal attacks, social engineering assaults, and man-in-the-middle threats are examples of cyber threats; lowering the danger of cyberattacks is part of cybersecurity. The management must take aggressive measures to manage cyber hazards. Firewalls are one example of a cybersecurity technology that is readily accessible [10].

Although artificial intelligence techniques may aid in the battle against cybercrime, they are not infallible and may be used maliciously by hackers. AI has some constraints that keep it from becoming a standard utility. Cost, extensive resources, and training are some drawbacks of AI in cyber security. AI-based cybersecurity solutions are more expensive and resource-intensive than conventional, non-AI-based ones and may only be applicable in some situations. Absolute security is not attainable in the field of cybersecurity. [11]. Problems may arise if a machine learning-based security solution fails to detect a specific type of cyberattack because it does not have built into it. Hackers himself can utilize AI to design and test their malware, potentially making it AI-resistant. Many experts have cautioned that cyberattacks could become more harmful and challenging to detect than ever before. Although the positives outweigh the bad, some see cybersecurity AI as a blessing and a burden. Cybercriminals can employ AI systems to conduct attacks, much as AI technology can be used to recognize and thwart cyberattacks. Another issue is the need for cybersecurity professionals. These difficulties prohibit AI from dominating cybersecurity.[12]. The main advantages of AI include improved outreach, quicker and more accessible information access, and fewer errors in disease diagnosis and treatment. A few critical areas where AI has made substantial advancements are focused therapy delivery, personalized medicine, and prediction diagnosis. Digital consultations and follow-ups are efficient in terms of time and money.

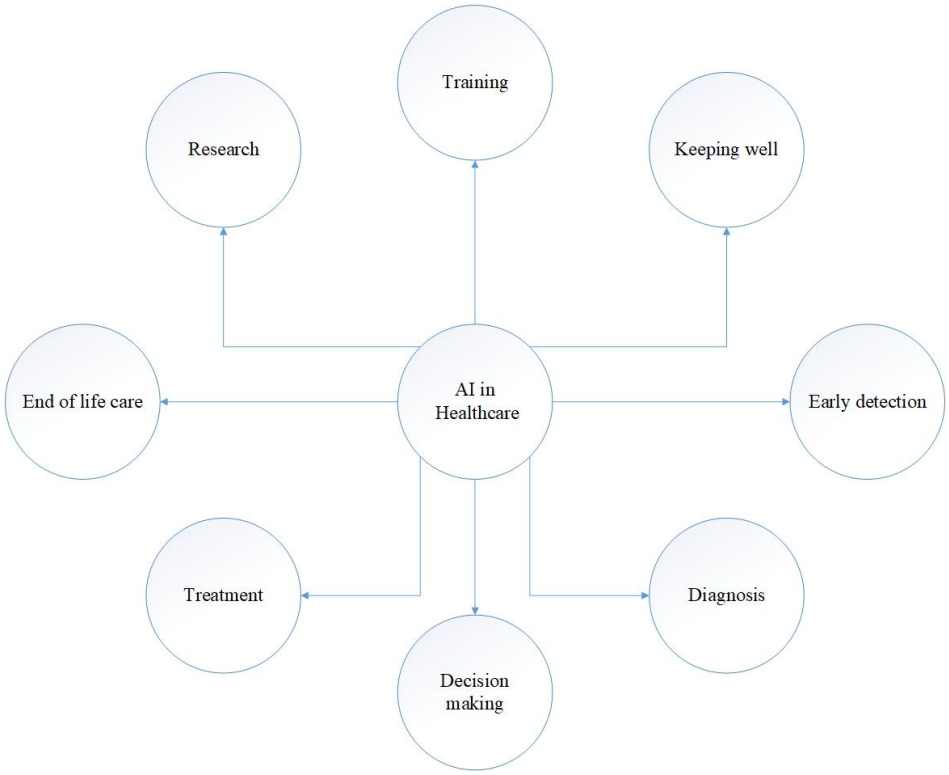

Figure 1. Applications of AI in healthcare

Fig. 1 Represents the applications of Artificial Intelligence in healthcare, such as training, keeping well, early detection, diagnosis, decision-making, treatment, end-of-life care, and research.

2 Related works

The CORONA virus-related epidemic catastrophe, which started in 2020, has had a significant negative influence on the entire world. Artificial intelligence is a critical component of the medical sector, notably in the diagnostic phase when it is used to recognize illness signs using various machine learning methods. The indications found in different diagnostics are utilized to forecast the treatment outcomes of earlier sickness identification, which helps to save lives. Automation interpreting has effectively utilized machine learning methods. Information security could be prioritized using innovative cybersecurity technologies to get good outcomes. Information confidentiality for the medical sciences can be improved using artificial intelligence. Additionally, they create their machine learning-based cyber security methods. It is challenging to compare techniques among all of the articles that are looked at objectively because the results of each research are published using various approaches on diverse demographics with different sampling probabilities and properties [13].

From the "Internet of Computers" to the "Internet of Things," the functioning of the Internet is constantly evolving. The majority of interconnected systems, or "cyber-physical systems," are created by the fusion of several elements, including individuals and their virtual environments, intelligent products, embedded devices, and technology. The Internet of Computers and cyber-physical systems may face several serious concerns, including cyber security dangers and moral dilemmas. While every gadget and piece of information is linked and available on the networks, attackers might use this to commit various frauds. Sensing devices could be used in medical healthcare IoT-CPS to collect patients' routine health and physiological information. This study suggests an IoT-CPS with AI capabilities that clinicians could use artificial intelligence to identify patients' ailments. Artificial intelligence was developed to identify very few diseases, including diabetes, cardiovascular disease, and movement abnormalities. Every illness manifests differently in individuals or the aged. A database is acquired from the Kaggle source to use IoT-CPS with AI. AI-enabled IoT-CPS Algorithms are utilized for the categorization to find disorders. The research findings demonstrate that, in terms of Effectiveness, Precise, Memory, and F-Score, the suggested AI-enabled IoT-CPS system identifies patient illnesses and falls incidents in senior citizens more effectively than traditional algorithms. Although they aren't intended to replace people entirely, computers can help people function less [14].

While governments from many nations are now establishing a new standard to relaunch their economies, the COVID-19 outbreak also isn't letting down. Healthcare experts who serve as the front lines in hospitals and clinics combating the COVID-19 threat have a high fatality ratio up to this point. Artificial intelligence, dependent on computer sciences researched since the 1960s, might help healthcare experts defend themselves from the SARS-CoV-2 virus and treat the patient effectively and securely. AI could help in many different domains, from diagnostic to therapy to pharmaceutical to outbreak forecasting. To help medical workers deal with the COVID-19 outbreak and the risk of upcoming epidemics, this review will emphasize Machine learning and artificial intelligence in the medical sciences. Unfortunately, this SOP can only be utilized with very little information [15].

The globe is teeming with innovative concepts and technologies, and engineers create machinery to do the labor instead of people. With intelligent systems, the process is easier to execute. Proper methods or consultations are carried out with specialists who are accessible internationally, thanks to technological innovation. In this situation, it is apparent that the healthcare industry is among the global expectations that call for the utmost care possible when transmitting information. The network's endpoints are evaluated depending on their vulnerability to combat the problems posed by a cyber-attacker. In addition to creating the program for information storage, a superior method must be added to ensure the confidentiality of the data saved. Each network operator faces a challenging issue during this procedure. This paper aims to clarify ideas linked to health forecasting and treatment by constructing more consistent network security measures. The suggested optimum neural network representations are distinguished using the concluding procedure of accessible information. The results reveal that the proposed models outperform the previous system by 4.76%, with reliability of 98.89%. However, as productivity increases, an individual product design cannot suit the different requirements of individuals [16].

An increasing number of cyber security flaws and risks have been established using Internet of Things systems in healthcare settings. The employment of artificial intelligence-based cybersecurity defense systems for collecting, identifying, and mitigating known and upcoming threats is constrained due to the absence of an extensive data repository that catches medical equipment weaknesses. Designers outline a method that gathers information on different healthcare devices' reported flaws from resources like vendors and Industrial control systems - CERT vulnerability notifications to create a database of cyber threat information. They add sources of information from Wiki data and public data sets to the intelligence collection. The Cyber Security Graph Database incorporates the pooled assets with risk information from earlier studies. The enhanced graph's extracted features help search for pertinent data and may support a variety of AI-assisted safeguarding jobs. Researchers discovered that the improved cooperative key generation provided graph depictions of more excellent quality because of the inclusion of different components. When the Mean Average Precision values were calculated over a statistics gathering assignment, the increased cooperative key generation resulted in a 31% gain. The accuracy of the graph embedding will be even more enhanced in the head as they add to the combined vital age with other information sources. The numerous natural language processing jobs on information security textual data would be significantly enhanced by these enhanced graph embeddings [17].

Blockchain technology has received much attention with a new emphasis on a wide range of technologies, from information management, financial sectors, cyber security, IoT, and food research to the healthcare sector and brain study. Employing blockchain technology applications to enable secure and confidential healthcare information administration has attracted much attention. Additionally, blockchain modernizes conventional medical methods by allowing safe and personal information sharing and better diagnostics and therapy. Blockchain technology can contribute to future personalized, authentic, and reliable medicine by combining all accurate clinical information related to a patient's health and displaying it in a modern, safe healthcare setting. While using blockchain as a paradigm, they examine the recent and current changes in the medical industry in this article. In addition to the difficulties encountered and the possibilities for the future, they also talk about the blockchain’s applications. However, this technique has a unique collection of problems [18].

The Internet of things has drawn considerable interest from both the business and educational worlds because of the profound changes it has brought to humankind. The concept of intelligent technologies, microgrids, firms’ ability, sustainable cities, and many more ideas have all been established due to the Internet of Things rapid growth. Cyber security of IoT systems is increasingly a significant problem, particularly for the medical industry, where recent breaches have revealed devastating Internet of things security flaws. There are many well-established conventional network safety methods. However, due to the resource-constrained architecture of Internet of Things connected systems and the distinctive characteristics of Internet of Things protocols, the established preventive mechanisms cannot be used to safeguard the connected systems networks and gadgets from information security. Researchers desire data, technologies, and strategies from the Internet of Things to improve protection. To tackle the issues above, it offers a framework for developing context-

aware IoT security features that may detect suspect data in the Internet of Things usage scenarios. The proposed framework is built on top of the Internet of Things Flocks, a cutting-edge IoT Platform data generation tool. Researchers could establish an Internet of Things use environment with both honest and dishonest IoT networks, increasing activity by utilizing the Internet of Things-Flock technologies.

Additionally, Internet of Things -traffic Flocks could be converted through an Internet of Things database using the recommended architecture's accessible software. Researchers first developed an Internet of things healthcare dataset that incorporates combined conventional and Internet-of-things assaulting activities using the methodology proposed in this research. The created information was then subjected to various machine learning algorithms to identify cyber-attacks and defend the medical system against them. A critical application scenario like the IoT healthcare environment will benefit from the context-aware IoT safety technologies developed using the Suggested framework. Meanwhile, the defense of IoT application-level protocols against DDoS attacks receives little attention [19].

Donee and Seong discussed the opportunities and challenges in the application of AI in healthcare industries [4]. This study looks at the present state of AI-based technological applications and how they affect the healthcare sector. Along with a comprehensive review of the literature, this research examined a variety of genuine examples of Artificial intelligence uses in healthcare. The results demonstrate that big hospitals now use intelligent technologies to assist healthcare practitioners in patient diagnostics and caring procedures for various illnesses. Artificial intelligence technologies also impact the efficiency of facilities handling administration and medical staff members. Medical practitioners are embracing artificial intelligence; however, its applications could be viewed from utopian and dystopian angles. Rapid advancements in Artificial intelligence and related technology will help healthcare professionals improve patient value and streamline operational processes. However, successful deployments of Artificial intelligence would require intense planning and tactics to overhaul the entire medical care system and operations to benefit fully from what technologies have to give.

3 Proposed ACO-CNN method

The approaches that are now in use have a variety of shortcomings, including scalability, large databases, complex data, dependability, sluggish results, etc. Therefore, it is essential to consider an approach that may address these issues more effectively. The study's analysis of this CNN methodology is based on the advantages of these methods, and their compatibility with the kinds of data researchers use to assess their efficacy. This approach deals with the issue by considering the optimization utilizing highly scalable CNN algorithms. The majority of previously suggested solutions need help becoming solid and scalable. Fig. 2 depicts the block diagram of the proposed model, and the following list explains each component.

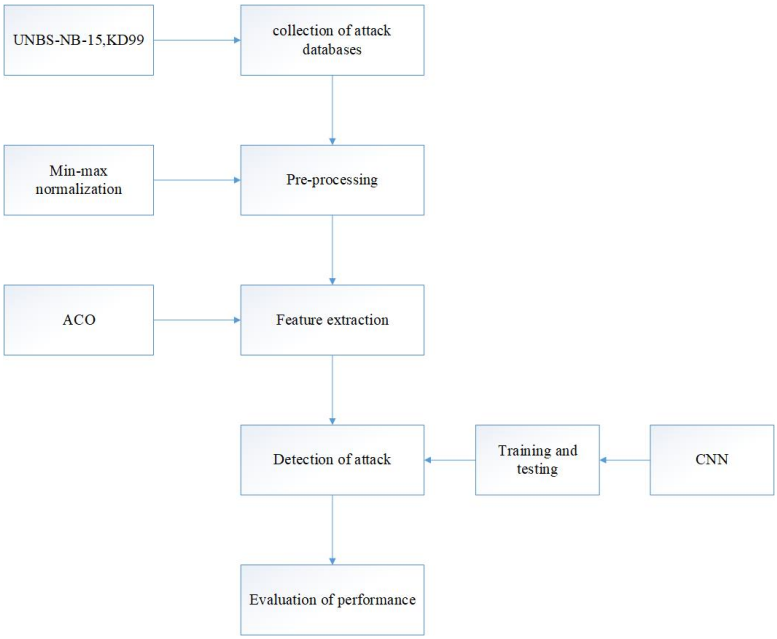

Figure 2. Proposed ACO-CNN model

3.1 Data Collection

To assess the efficacy of methods, this study employs the reference UNBS-NB-15 database, one of the most recent and well-liked datasets. The UNBS-NB-15 database is given in table 1.

Table 1. UNBS-NB-15 database

Features selection	Ranking	Feature description
Dbytes	0.491	Server-client transactions
Sload	0.464	Client (bits-per-second)
Sttl	0.444	Client-server (time)
Rate	0.429	Rate
Dmean	0.406	Mean packet size transferred by the server
Sbytes	0.642	Client-server transactions
Smean	0.477	Mean packet size transferred by the client
ct-state-ttl	0.454	Count
Dttl	0.439	Server-client (time)
Dur	0.409	Countdown time

The IXIA Perfect Storm program was used to create the database, which was then split into nine categories—Backdoor, DoS, Exploits, Reconnaissance, Generic, Shellcode, Fuzzers, Worms, and Analysis—by taking into account the traffic that both approved clients and attackers generate [20]. In addition, a different testing source is used, the KDD99 database [21], as shown in table 2.

Table 2. KDD99 database

Features	Descriptions
Protocol-type	Protocols that are utilized in a connectivity
Flag	Connection's status flag
Dst-bytes	Sending data (in bytes) from destination-source
Urgent	Urgent packet number (source-destination), etc.
Duration	Connection time (seconds) source-destination
Service	Services at the destination
Src-bytes	Sending data (in bytes) from source-destination
Wrong-fragment	Wrong-fragment lists (sender-receiver)
Land	1-connection from the same source; otherwise-0

3.2 Pre-processing

The dataset has been preprocessed using min-max normalization in a developed framework. Knowledge normalization can be used in knowledge stream mining as a preparation technique. The database's correlating nursing number is altered by raising the numbers until they fall within the required points, such as within 1.0. Starting with the first stage, Eqn computes the min-max normalization performed using the Min-Max normalization method. Through min-max normalization, a value f of y is changed into f' within the range $[new_{\min(y)}, new_{\max(y)}]$. The component calculates tuples with partial data by suggesting one of the many alternatives, such as the majority, minimum, mean, constant, and variance, before performing the normalization procedure to the database. The min-max normalization is computed by Eq. (1):

$$f' = \frac{[f - \min(y)] \times [new_{\max(y)} - new_{\min(y)}]}{[\max(y) - \min(y)]} + new_{\min(y)} \quad (1)$$

Where, $\min(d)$= minimum value of the attribute, and $\max(d)$= maximum value of the attribute. Eq. (2) displays the formula reduced for determining social control.

$$f' = \frac{f - \min(y)}{\max(y) - \min(y)} \quad (2)$$

A minimum and maximum normalization, or min-max normalization maintain the connection between the values of the data sources.

3.3 Feature Extraction

Ant Colony Optimization algorithm is applied in feature extraction. Here the databases with specific attributes are extracted from the group of samples, and these extracted databases are used for the detection of cyberattacks.

3.3.1 Ant Colony optimization algorithm

Approximative optimization is currently done using the ant colony optimization method. The ant search activity is what propels the optimization of the ant colony. Ants can find the quickest path to their food supply thanks to their primary means of communication. The Ant Colony Optimization approach (ACO) utilizes this ant's exceptional quality. One of the essential attributes in the database that needs to be modified initially is the pheromone rate. A matrix (h) holds all the pertinent data to explore the feature. The ant colony optimization settings are changed before the principal computation, such as the experimental function F. Choose the resources and finest subset for the upcoming repeat.

The Ant Colony Optimization algorithm must first have its factors initialized, which is the first and most crucial stage. Many candidate ants are present. Other characteristics of the ACO algorithm include strong toughness and an isolated calculative process. ACO works brilliantly in resolving complex optimization problems and can be used interchangeably with different strategies. ACO employs the updated pheromone, and ants move according to mathematical formulas in the search area. The basis of ACO is local and global searches.

3.3.2 Transition probability of region (m)

The algorithm determines the healthcare system suspected of cyberattack for estimating a region's transition probability.

$$P_a(r) = \frac{r_a(r)}{\sum_{i=1}^{d} r_i(r)} \quad (3)$$

Here, d is the number of worldwide ants, and $r_a(r)$ stands for the total amount of pheromones at area a.

3.3.3 Pheromone update

A chemical termed a pheromone is released by an ant, affecting other ants' behavior. An ant's communication pheromone update is calculated using the equation,

$$z_k(z+1) = (1-r)z_k(z) \quad (4)$$

Here 's' denotes the evaporation rate of the pheromone.

3.3.4 Edge traversed equation

Following each stage of the building, all the ants update the neighborhood pheromone. Only the most recent edge that each ant crossed is where they use it.

$$\tau_{jk} = (1 - \Psi) . \tau_{jk} + \Psi . \tau_0 \quad (5)$$

3.4 Detection using CNN

Cyberattacks in healthcare systems are identified using CNN classifiers. The four layers that make up the CNN classifier are the convolutional layer, the Max pooling layer, the fully connected layer, and the output layer. The dataset samples intensify before Convolutional Neural Network training. Throughout the training, CNN is the model that operates the quickest. The dataset samples provided should be uniform. The formula for the normalization of each data. The formula for the normalization of collected data in the training set is given in Eq. (6)

$$z(j,k) = \frac{O(j,k)-\mu}{\sigma} \quad (6)$$

a) Convolutional layer

The convolution layer employs each layer to examine each dataset's complexity after gathering several datasets as input. It is directly connected to the qualities in the images we have been given.

$$f_u^m = x(\sum_{v \in N_u} f_v^{m-1} * p_{vu}^m + x_u^m) \quad (7)$$

An input choice is represented by N_u - it. The output has been given as an additive bias k. If the sum of the maps v and k is greater than map u the kernel is applied to map u.

b) Max pooling layer

This layer reduces the neuron size used in the downsampling layer. The number of parameters, and the training time are all reduced by the pooling layer. The threshold for overfitting is 50% of training data and 100% of test data.

$$x_{mjk} = mix_{(r,t)\in} f_{mrt} \quad (8)$$

Map, f_{mrt} is the element at (r, t) within the pooling region q_{jk}.

c) Fully connected layer

In categorizing datasets, a completely Connected Layer has been used. The FC layers are positioned before all of the Convolution layers. The FC layer makes it easier to map the illustration between the input and output. Fully connected layers make up the network's upper levels. The output of the max pooling layer serves as the input for the fully connected layer.

d) Softmax layer

The Softmax layer is used to convert the scores transformed into a normalized probability. This layer may identify any kind of cyberattacks in the healthcare system. The following equation, Eq. (9), can be used to express it,

$$\sigma(\vec{X})_n = \frac{e^{x_n}}{\sum_{u=1}^{n} e^{x_u}} \tag{9}$$

Algorithm: ACO-CNN mechanism

Input: *Cyberattack samples*
Output: *Detection of cyberattacks in the healthcare system*
Load input image data
$I = \{I_1, I_2, I_3 \ldots\}$ *// data acquisition*
Pre-processing of images *// min-max normalization*
$f' = f - \min(y) \Big/ \max(y) - \min(y)$
Feature extraction *// Ant Colony Optimization*
Initialize the starting point of the suspected system
If (ant moves onto the following position)
Compile the subset.
Identify the attacks in the healthcare system using Eqn. (1)
Else
Identify the next element. using Eqn. (2) *// pheromone update*
Continue until a halting requirement is satisfied.
end if
Return
Detection of cyberattacks in the healthcare system *//CNN Classifier*

4 Results and Discussion

4.1 Accuracy

Accuracy may be gauged by how likely a record, which might be an attack or normal traffic, would be accurately identified. To evaluate the accuracy of the assault detection, utilize Eq. (11).

$$Accuracy = \frac{T_{Pos} + T_{Neg}}{T_{Pos} + T_{Neg} + F_{Pos} + F_{Neg}} \tag{11}$$

4.2 False alarm rate

FAR, also referred to as the possibility that a record was misclassified, stands for false alarm rate. It is calculated using Eq. (12).

$$FAR = \frac{F_{Pos} + F_{Neg}}{T_{Pos} + T_{Neg} + F_{Pos} + F_{Neg}} \tag{12}$$

4.3 Recall

The recall is sometimes referred to as sensitivity. It determines the proportion of "attacks" correctly classified as such compared to all "attacks," It can be calculated using Eq. (13).

$$R = \frac{T_{Pos}}{T_{Pos} + F_{Neg}} \tag{17}$$

4.4 Specificity

Specificity is a measure of the possibility of test attacks without resulting in false positive results. It is calculated using Eq. (14).

$$Specificity = \frac{T_{Neg}}{T_{Neg} + F_{Pos}} \tag{18}$$

Table 3. Comparison of Performance metrics with and without optimization (ACO)

	Avg. Detection Accuracy (%)	Avg. False Alarm rate (%)	Avg. Recall (%)	Avg. Specificity (%)
Without Optimization (CNN)	92.5	5.9	92.2	93.6
With Optimization (ACO-CNN)	99.55	0.84	98.1	98.02

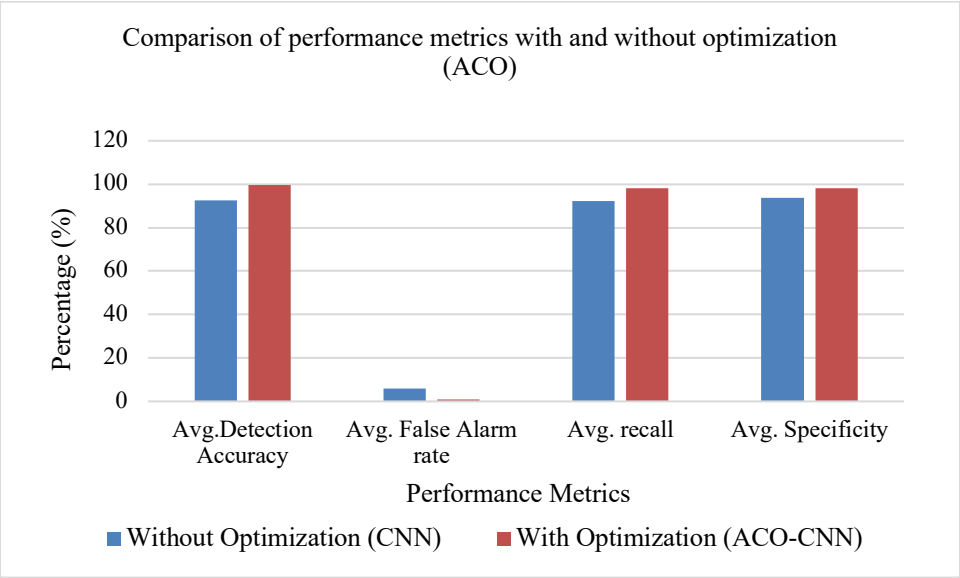

Figure 3. Comparison of performance metrics with and without optimization (ACO)

Table. 3 illustrates the comparison of performance metrics with and without optimization. The outcomes show that the proposed CNN model with ACO mechanism (ACO-CNN) achieved very high detection accuracy, 99.55%, and very low FA,R 0.84%, compared with the model without optimization, as shown in Fig. 3.

Table 4: Performance evaluation for UNBS-NB 15 database for proposed and existing methods

Method	Detection accuracy	False Alarm rate	Recall	Specificity
ANN [22]	97.44%	2.56%	84.89%	15.11%
IRIDS [23]	90.32%	2.01%	5%	50.37%
Proposed ACO-CNN	99.15%	0.55%	98.45%	98.31%

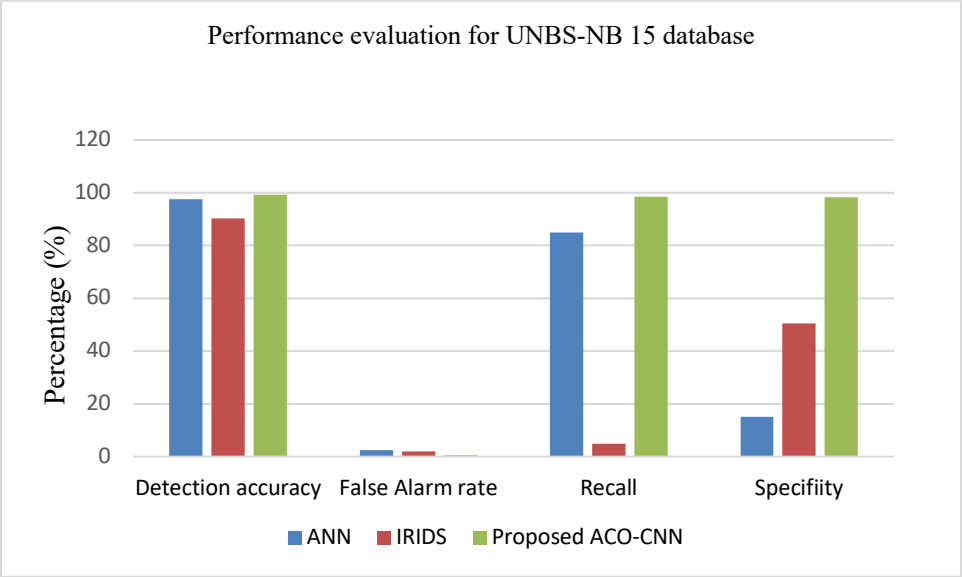

Figure 4. Comparison of performance measures for an existing and proposed method for the UNBS-NB 15 database

The performance assessment for the UNBS-NB15 dataset is shown in table 4. The results of the performance evaluation make it clear that the proposed (ACO-CNN) has a greater detection accuracy (99.15%) than all other currently used methods, including Integrated-rule based intrusion detection systems (IRIDS) and Artificial Neural Networks (ANN). Additionally, the proposed approach only produces a relatively low FAR value of 0.55%, compared to IRIDS and ANN's 2.01% and 2.56%, respectively. Additionally, compared to the current methods, the suggested model performs well regarding recall and specificity. Fig. 4 depicts a visual comparison of the current and suggested procedures for the UNBS-NB 15 database.

Table 5. Performance evaluation for the KDD99 database for proposed and existing methods

Method	Detection accuracy	False Alarm rate	Recall	Specificity
HGWCSO-ETSVM [24]	99.2%	2.42%	79.5%	94.3%
RNN [25]	97.84%	2.87%	90.46%	94.62%
Proposed ACO-CNN	99.25%	1.3%	98.42%	97.31%

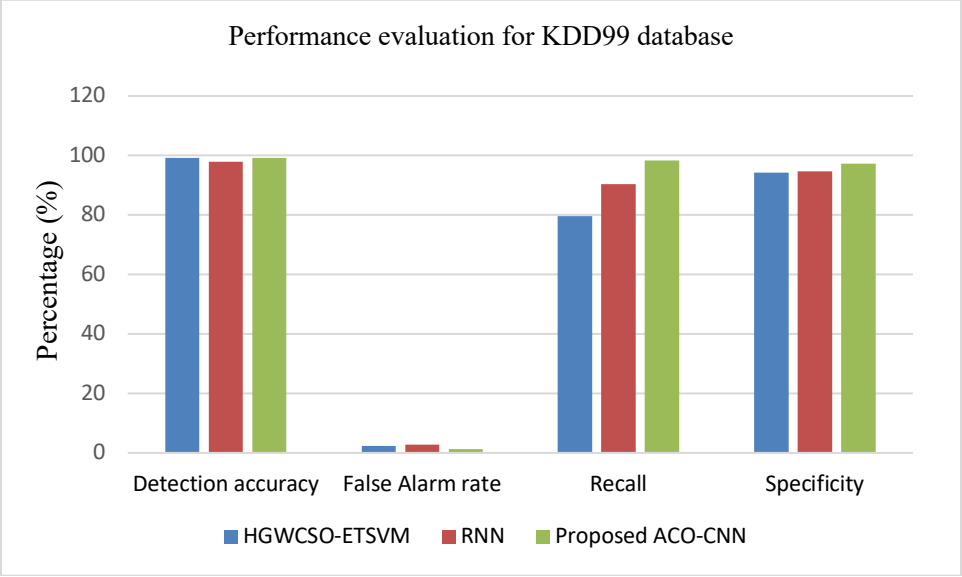

Figure 5. Comparison of performance measures for an existing and proposed method for the KDD99 database

The performance evaluation for the KDD99 dataset is shown in table 5. The results of the performance assessment make it clear that the proposed (ACO-CNN) method has a greater detection accuracy (99.25%) than all other methods that are currently in use, including HGWCSO-ETSVM and RNN. Additionally, it is noted that the HGWCSO-ETSVM and RNN both produce far higher FAR values than the suggested technique, which only manages to achieve a relatively low FAR value of 1.3%. Additionally, when compared to the current methods, the suggested model performs well in terms of recall and specificity. Fig. 5 depicts a visual comparison of the existing and suggested techniques for the KDD99 database.

Furthermore, it is noted that when compared to the KDD99 database, the UNBS-NB15 database offers superior classification accuracy and FAR. With this justification, it is clear that the KDD99 database does not adequately reflect either the current network traffic scenario or the low-tracing attack state. However, when all of these characteristics are considered, the UNBS-NB15 database is shown to be the best. Future threat detection and prevention strategies may take into account a variety of additional databases.

5 Conclusion

Even though there are numerous assault detection technologies and approaches, network infiltration is still unavoidable. Attackers and intruders are dangerously affecting the network's authorized systems by using contemporary techniques. This paper introduces the ACO-CNN model, a unique framework for better-identifying intrusions and tracking attacker behavior. The experiment includes a variety of operations, including feature extraction, pre-processing, and detection. During the pre-processing, the min-max normalization technique is used to increase the effectiveness of attack identification. In the feature extraction stage, the ACO approach is used to choose the top attributes from the dataset. The ideal characteristics are upgraded by creating improved fitness metrics. When using the CNN algorithm, the invader and normal qualities are detected more successfully. To provide more exact features, the chosen qualities are subjected to the training and testing approach. False Alarm Rate, recall, specificity, and accuracy are among the performance metrics evaluated. The proposed ACO-CNN approach yields higher performance metrics. The experimental data led to the conclusion that the recommended method outperforms existing methods. Future iterations of the approaches will combine advanced optimization with classification algorithms to successfully detect more threats.

References

[1] S. Reddy, S. Allan, S. Coghlan, and P. Cooper, A governance model for the application of AI in health care, *Journal of the American Medical Informatics Association*, **27(3)**, 491-497, 2020.

[2] M. Elloumi, M. A. Ahmad, A. H. Samak, A. M. Al-Sharafi, D. Kihara, and A. I. Taloba, Error correction algorithms in non-null aspheric testing next generation sequencing data, *Alexandria Engineering Journal*, **61(12),** 9819-9829, 2022.

[3] S. Ellahham, N. Ellahham, and M. C. E. Simsekler, Application of artificial intelligence in the health care safety context: opportunities and challenges, *American Journal of Medical Quality*, **35(4)**, 341-348.

[4] D. Lee and S. N. Yoon, Application of artificial intelligence-based technologies in the healthcare industry: Opportunities and challenges, *International Journal of Environmental Research and Public Health*, **18(1),** 271, 2021.

[5] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, Applications of artificial intelligence and machine learning in smart cities, *Computer Communications*, 154, 313-323, 2020.

[6] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives, *Cryptography*, **3(1),** 3, 2019.

[7] A. El-Komy, O. R. Shahin, R. M. Abd El-Aziz and A. I. Taloba, Integration of computer vision and natural language processing in multimedia robotics application, *Information Sciences Letter*, **11(3),** 765-775, 2022.

[8] M. Senbekov et al., The recent progress and applications of digital technologies in healthcare: a review, *International journal of telemedicine and applications*, **2020**, 1-18, 2020.

[9] A. Bohr and K. Memarzadeh, The rise of artificial intelligence in healthcare applications, *In Artificial Intelligence in healthcare*, **2020**, 25–60, 2020.

[10] L. R. Nair, S. D. Shetty, and S. D. Shetty, Applying spark based machine learning model on streaming big data for health status prediction, **Computers & Electrical Engineering**, **65**, 393-399, 2018.

[11] Y. Lu and L. D. Xu, Internet of Things (IoT) cybersecurity research: A review of current research topics, *IEEE Internet of Things Journal*, **6(2),** 2103-2115, 2018.

[12] F. Pesapane, C. Volonté, M. Codari, and F. Sardanelli, Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States, *Insights into imaging*, **9(5),** 745-753, 2018.

[13] A. A. Sewisy, M. H. Marghny, and A. I. Taloba, Fast Efficient Clustering Algorithm for Balanced Data, *International Journal of*

Advanced Computer Science and Applications, **5(6),** 123-129, 2014..

[14] L. K. Ramasamy, F. Khan, M. Shah, B. V. V. S. Prasad, C. Iwendi, and C. Biamba, Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring, *Sensors*, **22(3),** 1076, 2022.

[15] A. A. Parikesit, N. R. P. Ratnasari, and D. Anurogo, Application of Artificial Intelligence-Based Computation in the Health Sciences to Ward off the COVID-19 Pandemic, *International Journal of Human and Health Sciences (IJHHS)*, **5(2),** 177-184, 2020.

[16] K. Vijayakumar et al., Intelligence-based Network Security System to Predict the Possible Threats in Healthcare Data, *Security and Communication Networks*, **2022**, 1-12, 2022.

[17] S. S. Ismail, R. F. Mansour, R. M. Abd ElAziz and A. I. Taloba, Efficient E-Mail Spam Detection Strategy Using Genetic Decision Tree Processing with NLP Features, *Computational Intelligence and Neuroscience*, 2022.

[18] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives, *Cryptography*, **3(1),** 3, 2019.

[19] F. Hussain et al., A framework for malicious traffic detection in IoT healthcare environment, *Sensors*, **21(9),** 3025, 2021.

[20] A. Rayan, A. I. Taloba, R. M. Abd ElAziz and A. Abozeid, IoT enabled secured fog based cloud server management using task prioritization strategies, *International Journal of Advanced Research in Engineering and Technology*, **11(9),** 2020.

[21] A. Elhadad, F. Alanazi, A. I. Taloba, and A. Abozeid, Fog Computing Service in the Healthcare Monitoring System for Managing the Real-Time Notification, *Journal of Healthcare Engineering*, 2022.

[22] O. R. Shahin, H. H. Alshammari, A. I. Taloba and R. M. Abd El-Aziz, Machine Learning Approach for Autonomous Detection and Classification of COVID-19 Virus, *Computers and Electrical Engineering*, **101**, 108055, 2022.

[23] A. I. Taloba, R. M. Abd El-Aziz, H. M. Alshanbari and A. A. H. El-Bagoury, Estimation and Prediction of Hospitalization and Medical Care Costs Using Regression in Machine Learning, *Journal of Healthcare Engineering*, 2022.

[24] V. Kumar, D. Sinha, A. K. Das, S. C. Pandey, and R. T. Goswami, An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset, *Cluster Computing*, **23(2)**, 1397-1418.

[25] E. M. Roopa Devi and R. C. Suganthe, Enhanced transductive support vector machine classification with grey wolf optimizer cuckoo search optimization for intrusion detection system, *Concurrency and Computation: Practice and Experience*, **32(4),** 2020.