Smart Healthcare Applications: Detecting DDoS Attacks Efficiently using Hybrid Firefly Algorithm

G. Sripriyanka
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
sripriyanka.2018@vitstudent.ac.in

Anand Mahendran
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India
manand@vit.ac.in (corresponding author)

Received: 28 November 2024 | Revised: 12 January 2025 | Accepted: 18 January 2025

 DOI: https://doi.org/10.48084/etasr.9760

ABSTRACT

The rapidly growing and emerging Smart Healthcare Applications (SHA) are reducing the burden on the existing healthcare system caused by limited medical infrastructure and increasing number of diseases. Bio-inspired anomaly-based detection systems are still affected by false positive rates because the approaches are synchronized with user-defined parameters that are unpredictable, resulting in convergence rate, discovery and utilization disparities, algorithm complexity, and unrealistic results. One of the most well-known and effective nature-inspired swarm intelligence metaheuristic algorithms is the Firefly Algorithm (FA). In this work, we propose a Hybridized Firefly Algorithm (HFA) that combines the advantages of the FA and Particle Swarm Optimization (PSO). The bio-inspired HFA is designed to mitigate Distributed Denial-of-Service (DDoS) attacks in SHA. We compare our algorithm with other DDoS attack resistant methods and conclude that our hybrid approach outperforms the existing FAs in terms of accuracy, error prediction, and attack detection time. The statistical results demonstrate the improved accuracy and effectiveness of our proposed HFA model with a higher accuracy of 94.9%, error prediction of 6%, and detection time of 1.12 ms compared to existing DDoS attack detection methods. The proposed HFA methodology is a decentralized architecture, more effective, highly reliable, and available for real-time SHA in terms of monitoring and detecting attacks.

Keywords-smart healthcare applications; bio-inspired computing; DDoS attack; firefly algorithm; particle swarm optimization; hybridized firefly algorithm

I. INTRODUCTION

In today's rapidly evolving world, internet technology is maturing and becoming more integrated into people's daily lives. People from all walks of life are increasingly concerned about medical issues as their lifestyles, health needs, and medical perceptions continue to evolve [1]. New medical ideas and services have emerged over time due to advances in science and technology. In India, the issue of an aging population has become a major concern for the government, prompting it to take action. In 2019, there were 1.35 billion people in India, and those aged 70 and above accounted for about 9% of the total population. China's elderly population is expected to reach 20% by 2040, a significant increase. As the elderly population continues to grow, so does the demand for medical services. In addition, the rapid spread of Internet of Things (IoT) sensors has greatly affected people's lives. Therefore, a more sophisticated and simple service platform is needed to ensure people's medical monitoring, but from the point of view of simplicity, so that an intelligent medical treatment as shown in Figure 1 is feasible [2]. Overcoming the time and place limitations of traditional medical services can improve the medical care experience [3, 4]. On the other hand, service platforms and networked systems are vulnerable to cyber-attacks. With interconnected systems and associated infrastructure, "cyberspace is an operational area defined by the use of technology to exploit information" [5]. The vulnerabilities have an impact on network performance, which is the ultimate purpose of network management. Therefore, it is necessary to take measures to reduce the likelihood of such compromises [6]. Cybersecurity techniques, concepts, and technologies, including Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), are just a few examples. For the most part, these systems focus on identifying possible

incidents, logging information about them, and attempting to halt or report them to administrators [7, 8]. However, bio-inspired IDSs identify threats more accurately than conventional systems [9]. The Particle Swarm Optimization (PSO) method searches for the best solution using agents called particles, whose velocities are altered by a probabilistic and predictable component [10]. Bioluminescence, which is commonly used for sexual selection by living organisms, such as fireflies, has inspired some methods [11, 12]. However, bio-inspired optimization models for vulnerability scanning in cyberspace with a self-tuned regular expression and fast convergence are sparse [13] Trust mechanisms in real-world networks have not been properly designed or implemented, according to the authors in [14]. Therefore, this article explores various bio-inspired and evolutionary algorithms used for attack detection and mitigation on Smart Healthcare Applications (SHA) with high optimization. Finally, these approaches have become the center of the attraction for the researchers or scholars working in various domains including the attack detection and mitigation on smart applications. This article uses the Hybrid Firefly Algorithm (HFA) method to contribute and solve various security vulnerabilities in SHA. The key contributions of this paper are as follows:

- This work uses a previously established firefly and particle group optimization scheme to address the security complexity and Distributed Denial-of-Service (DDoS) attack detection in SHA.
- The results of the proposed algorithm are compared with the Firefly Algorithm (FA) [12], Evolutionary Algorithms (EA) [15, 16], and the Bat algorithm [17].
- The robustness of the proposed algorithm proves its superiority in the convergence rate and optimal results.
- The numerical analysis shows that the proposed HFA is a more robust and trustworthy optimization technique for solving security problems in SHA.

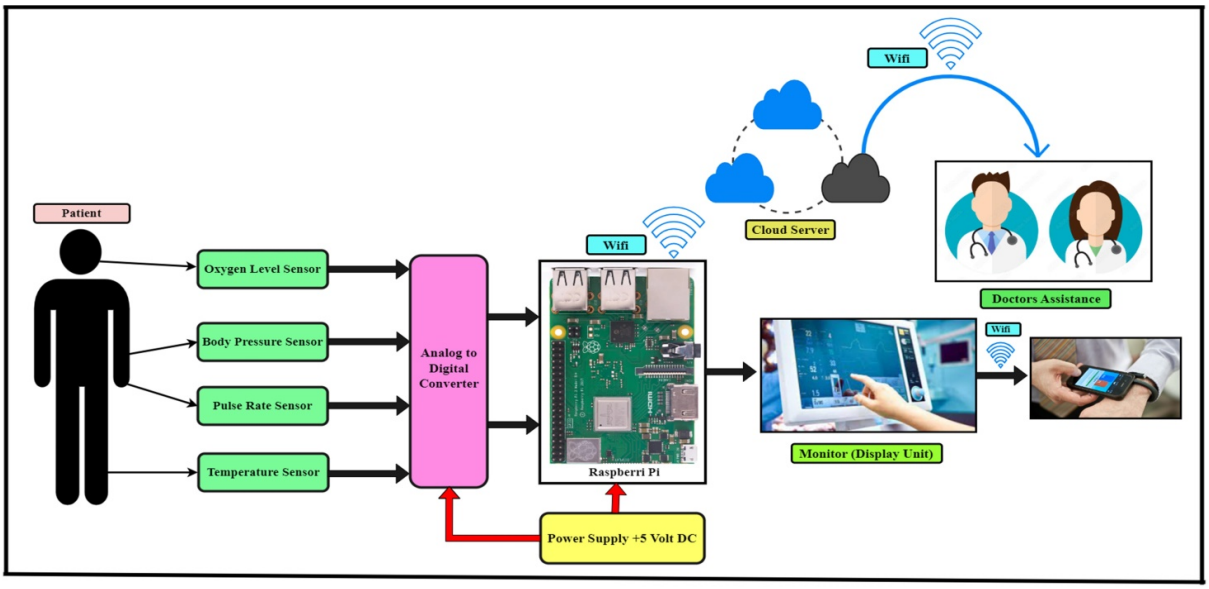

Fig. 1. Smart healthcare monitoring scenario.

A. *Related Works*

SHA have recently attracted attention from the networking and digital security communities due to their rapid technological evolution. The authors in [18] used OpenHAB 2 to design, develop, and deploy a prototype of a secure wireless home automation system. Using a 16-channel relay and an Arduino Mega 2560, they interfaced the Arduino Mega 2560 with OpenHAB software running on a Raspberry Pi Model B. An automated smart home prototype was developed using the Raspberry Pi as a server remotely controlled by an Android app and a web application. The AI4SAFE-IoT architecture presented by authors in [19], is primarily designed for IoT edge layer infrastructure. This architecture recommends three main modules: cyber threat attribution, cyber threat hunting, and cyber threat intelligence. Each security module is defined in the proposed architecture, and its functionality is demonstrated in real-world scenarios against various threats. According to the study in [20], many of the attack threats were on standby, just waiting for the deployment of the smart IoT devices. As noted by the authors in [21], node attacks are usually the most difficult to detect. Their approach aimed to address the difficulties mentioned in previous studies in order to provide low-load secure systems that can be integrated into devices at the production stage. According to the authors in [22], a game-theoretic approach to anomaly detection can be used to combat single-attack scenarios. It is possible to construct bio-inspired detection mechanisms that use techniques such as feature selection for clustering of invasion datasets, as well as computational learning approaches such as Complex Tree, Naive Bayes, and Support Vector Machine (SVM) classifiers. One of these is the Ant Colony Optimization (ACO) algorithm. Bio-inspired optimization techniques have been developed based on the natural foraging activity of ants [23]. An Ant Colony Optimization with Encryption Curve Cryptography (ACO-CC-SMIM) is presented in this paper as an effective

method to improve the security of medical image management. It has also been used to select the most significant features for a low complexity IDS [24]. The feature selection results were further improved by combining ACO with a feature-weighted SVM classifier [25, 26]. Both intrusion detection and data mining have used it as an independent bio-inspired method or as a combined method with machine learning techniques. The fuzz learning method for data clustering with K-means grouping as a classifier was used by the authors in [27] to reinforce the clustering problem of the first cluster center with fast union. Intrusion detection was addressed using the Multilayer Perception (MLP) algorithm. Using cross-validation with IDS data, the redesigned particle swarm colony was merged with Enhanced PSO to improve the optimization results and classification accuracy [28].

B. Security Attacks on Smart Healthcare Applications

IoT security, vulnerabilities, and countermeasures need to be identified and studied from a human healthcare perspective to enable the full use of IoT in the medical healthcare [29]. Attackers attempt to steal patient information, deny system services, and update data in various healthcare areas. It's important to note that there are two types of attackers in SHA, internal and external. Internal attackers lurk in the shadows, causing damage without being detected. Because of their presence within the system, the attacker's identity can be easily determined. External attackers are those that operate outside of the system. Due to their exclusion from the system, they are extremely difficult to identify [21]. Figure 2 depicts their malicious behavior after discreetly observing the system's processes [30]. DDoS attacks occur when an attacker overloads the system's communication channels with unknown traffic, preventing other nodes from using the system's resources. They typically exploit Network Allocation Vector (NAV) behavior by modifying control frame flags [31-33]. This type of attack is difficult to detect because IEEE 802.11 nodes do not countercheck all control frame flags [34]. In the DDoS attack, patient data could be accessed without proper authentication and authorization. As a result, the data cannot reach any other sensors in the network because the data channel is congested. System care providers, network operations, and sensor tasks are all compromised by this form of attack. Patient information, misleading recipients, misleading information, and a challenger repeating the current communication to compromise it are some of the ways an attacker can manipulate data in this type of attack. The alteration of data can result in the death of a patient. Overall, every layer of the network is targeted by a DoS attack [7].

C. Problem Forumulation

DDoS attacks flood healthcare networks with malicious traffic, overwhelming system resources and rendering services inaccessible. Traditional methods for detecting and mitigating these attacks suffer from limitations such as high false positive rates, inability to adapt to dynamic attack patterns, and excessive computational requirements, making them unsuitable for resource-constrained healthcare IoT environments. There is an urgent need for a lightweight, efficient, and adaptive solution that can protect the SHA from DDoS attacks without compromising performance or patient care.

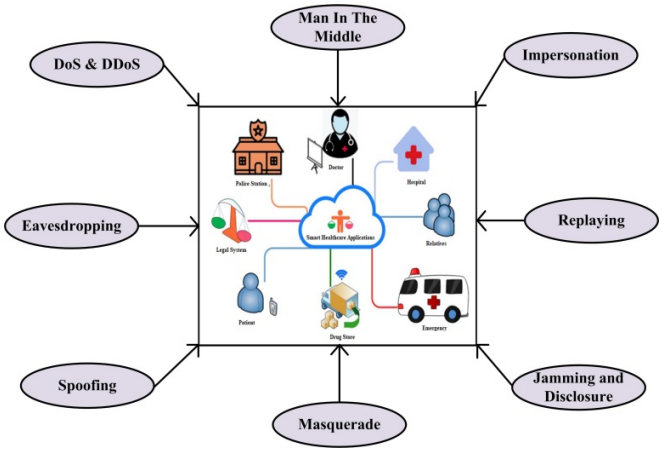

Fig. 2. Various attacks in SHA.

II. PROPOSED METHODOLOGY

An HFA model can provide an effective and efficient method of protecting SHA from DDoS attacks by monitoring and controlling the flow of traffic between networks and devices. It enables the identification and mitigation of malicious traffic, thereby reducing the impact of DDoS attacks on the SHA, as shown in Figure 3. By deploying an HFA model, healthcare organizations can ensure the stability and security of their applications and provide uninterrupted access to healthcare services. Each component of this proposed model is discussed in detail below.

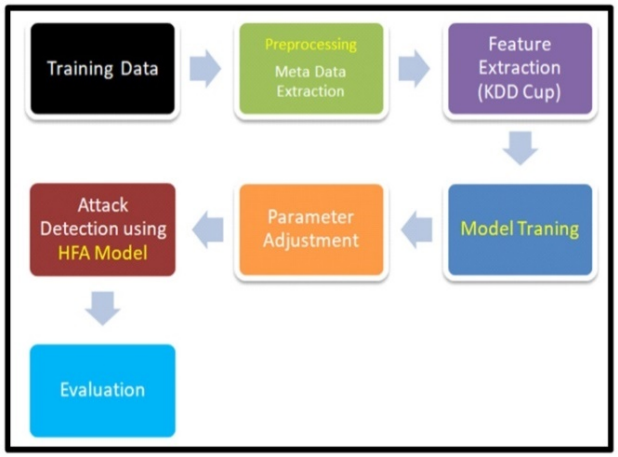

Fig. 3. Flow of DDoS attack detection in SHA.

A. Preprocessing Module

The primary purpose of this module is to periodically collect header information from SHA packets. Using the SHA controller, it is possible to send instructions to the switch to collect packets, which is a great advantage. If the collection interval for DDoS attacks is too long, the system may not be able to respond in time because the intrusion will cause irreparable damage and system loss. If the collection interval is too short, the SHA controller has to process more data, which increases the data processing overhead and slows down the

data collection process. The SHA controller then uses this header information to calculate the latency and packet loss rates for the network flow [35]. The results of the experiments showed that our network flow model was able to accurately detect and classify the flows with a high degree of accuracy.

B. Feature Extraction Module

To obtain the network flow characteristics, this module uses the packet collection and preprocessing module. It is necessary for the hybrid algorithm to know the characteristics of the network flow in order to detect DDoS attacks. While attackers can use a variety of attack methods to attack a particular network flow, there are some rules that apply to most DDoS attacks on that particular flow. A DDoS attack can be detected based on the characteristics of the network flow during the attack. Considering the previous analysis of DDoS attacks, it is possible to describe them in six distinct characteristics. These characteristics include the duration of the attack, the number of packets sent, the source of the attack, the type of attack, the victim, and the target. Once the attack is detected, the targeted system can be protected from further damage. Finally, the source of the attack can be investigated and action can be taken if necessary.

C. Hybridized Firefly Algorithm

The FA is a problem solver according to the No Free Lunch theorem, but it still introduces certain problems. HFAs have been created by mixing FA with other algorithms. In the present study we propose a new method using the combination of PSO and FA to form the HFA illustrated in Figure 4 and described in algorithm 1. Hybridization can help improve the performance of both algorithms and make them more adaptable to different tasks and environments. It can also help reduce the complexity of the algorithms, making them easier to implement and more efficient. The experiments demonstrated a better categorization accuracy compared to other algorithms. The proposed HFA with an enhanced mutation function that considers both local and global search capabilities. The FA is a society approach, where each firefly is treated as a vector position in the search area, that is, a perfect solution *x:* $C=(c_{x1},...,c_{im})$, where $x=1,2,...,\xi$, and ξ denotes the total number in the firefly community and m denotes the problem's dimension, which can be stated as the location of a firefly *x*. The following equation can be used to express the firefly brightness or attractiveness:

$$\mu(\delta) = \mu_0 \mathrm{e}^{-L\delta_{xy}^2} \quad (1)$$

Where δ_{xy} is the distance between fireflies *x* and *y*, μ_0 is the fluorescence brightness or attraction level at distance $\delta_{xy} = 0$, and *L* is the light absorption coefficient. The Euclidean distance of the fireflies can be expressed as the distance between them.

$$\delta_{xy} = ||C_x - C_y|| = \sqrt{\sum_{K=1}^{m}(C_{xk} - C_{yk})^2} \quad (2)$$

The authors of the original FA suggest that (2) can be swapped with the following equation:

$$\mu(\delta) = \frac{\mu_0}{1+L\delta_{xy}^2} \quad (3)$$

The distance between two fireflies will steadily decrease as they attract each other. Equation (4) could be used to substitute (2) according to the concept of equivalent infinite substitution, reducing the number of calculations and increasing the speed of operation.

$$C_x^{n+1} = C_x^n + \mu_0 e^{-L\delta_{xy}^2}(C_x - C_y) + \varphi(r - 0.5) \quad (4)$$

Using (3) the firefly can travel from location x to a more desirable position y, as shown in the following equation:

$$C_x^{n+1} = C_x^n + \frac{\mu_0}{1+L\delta_{xy}^2}(C_x - C_y) + \varphi(r - 0.5) \quad (5)$$

where n is the current number of observations, and r is a random number between 0 and 1 with a uniform distribution following the step size factor φ. We provide a population diversity-based location update technique to address the issues of sluggish convergence and easy fall into optimal solution FA values. We also provide an adjustable step size update technique to prevent the optimal solution vibration problem and increase the optimization accuracy. For each firefly, (5) states that it depends on the attraction of other fireflies with high fluorescence brightness to itself when updating its position. The research reveals that the entire search field can converge to the locally optimal after multiple location updates due to the absence of randomness in the global search. As indicated in (6), this work proposes to quantify group diversity by computing the mean distance length from each individual to the group center.

$$\beta^n = \frac{1}{|S|}\sum_{x=1}^{|S|}\sqrt{\sum_{y=1}^{m}(C_{xy} - C_y)^2} \quad (6)$$

Where $|S|$ is the population size, C_y is the j-dimensional component of the mean center of the population, and β^n reflects the diversity index of the n-th generation. The firefly location update approach is adjusted based on the diversity features discussed earlier. The new location update formula is:

$$C_x^{n+1} = C_x^n + \mu_0 e^{-L\delta_{xy}}(C_x - C_y) + \delta(C_x - C_b) + \varphi(r - 0.5) \quad (7)$$

In the formula below, T_{max} is the current iteration and T_{itex} is the current integer of iterations:

$$C = \frac{T_{max} - T_{itex}}{T_{max.}} \quad (8)$$

According to (7), the value is relatively large in the early stages of the algorithm, and the result obtained is a negative number. The firefly will search completely randomly in the direction closest to the best, resulting in a more sophisticated local search in (8). Both algorithms have proven to be effective in solving optimization problems. The hybridization of FA and PSO is done by combining the two algorithms into a single model. This hybrid model takes advantage of the strengths of both algorithms and can be used to produce more efficient and more accurate solutions to problems. In the proposed HFA-PSO algorithm, the main purpose is to obtain reliable results in a limited number of evaluations, which is achieved by evaluating a fixed number of functions. Particles are able to remember their velocity (V) and their personal best spot (G_{best}), whereas fireflies are not able to do so.

```
Algorithm 1: Hybridized Firefly Algorithm
Input: Firefly population P = P_1, ..., P_n
Output: Malicious nodes and malicious
nodes (Gbest Solution)
Begin
Initialize the population and evaluate the
fitness value;
C_G ← Select the best solution in the
Current
For T ← 1 to Max
   Sort population based on the fitness
   value;
   C_GOOD ← First_Half(C);
   C_WORST ← Second_Half(C);
   For i ← 0 to number of C_GOOD solutions
      For j ← 0 to number of C_GOOD solutions
         If f(C_i) > f(C_j) then
          Calculate the attractiveness and
          distance for malicious nodes;
          Update the position;
         End If
      End For
   End For
   For i ← 0 to number of C_WORST solutions
      Create trivial solution X_i(T);
      Perform the crossover Y_i(T);
      Perform the selection C_i(T);
   End For
C ← Combine(C_GOOD, C_WORST);
C_G ← Select the best solution in the
current;
T ← T + 1;
End For
End Begin
```

D. DDoS Attack Detection Model

The preprocessing module is a module that collects and preprocesses the packets. Since the characteristics of network attack flows are different from those of normal network flows, attack detection is considered as a classification task. The feature extraction module extracts the features of the network flows. Finally, the data samples are used to train the attack module. Figure 4 depicts the DDoS attack detection process using HFA. The HFA training model is used to detect and export the impact of a DDoS attack on the system's network flows. An input layer with convolutions is placed on top of a pool layer and is followed by a fully connected and an output layer. It is necessary for the input layer to accept the data that will be used for the detection process. There are several layers involved in this process; the first is the density layer, whereas the second is the fully connected layer, in which complete graphs are assembled using the weight matrices. The PSO algorithm has a time complexity of $O(n^3)$, where n is the number of variables in the problem. This means that as the number of variables increases, the algorithm's execution time also increases exponentially. The HFA has a time complexity of $O(n^2)$, which is significantly lower than the time complexity of the PSO algorithm. This means that the HFA is more efficient and computationally faster than the PSO algorithm for problems with an increasing number of variables.

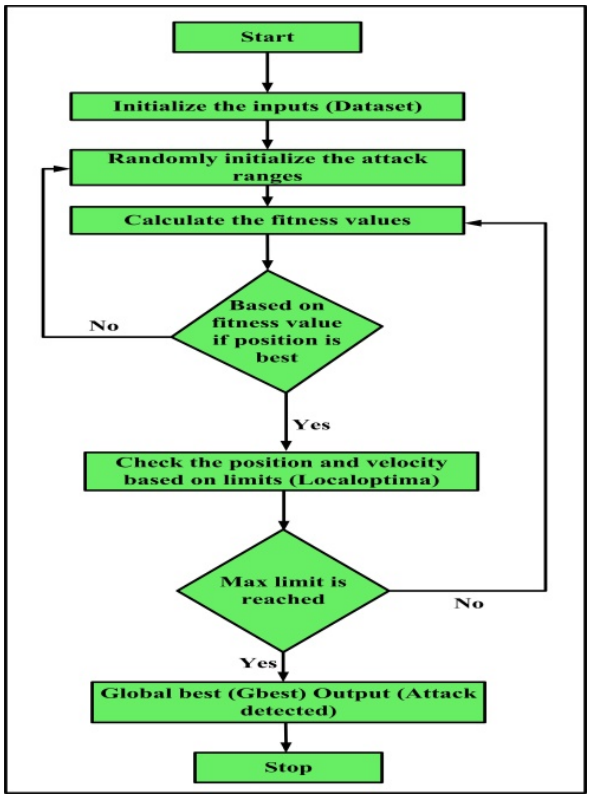

Fig. 4. Flow of the HFA.

III. RESULTS AND DISCUSSION

This section discusses the results of the algorithms used to detect attacks on the KDD Cup'99 dataset [7, 8]. A table and a graph are used to compare three different methods: the HFA, the FA, the EA, and the Bat algorithm. When it comes to testing anomaly detection algorithms, the most commonly used dataset is the KDD Cup'99. There are about 4 terabytes of raw (binary) TCP dump data, which can be translated into about 5 million programs, each about 100 bytes in size. The data from the two weeks of testing contain approximately 2 million records. There are 4,900,000 individual connection vectors in the training dataset, each with 41 features and designated as either regular or an attack, each with a specific type of attack. The results are compared through a simulation experiment with diverse network scenes. The efficiency of the HFA approach is evaluated using the simulation results of Contiki OS and Cooja simulator. Contiki OS and Cooja simulator provide an efficient way to detect and mitigate DDoS attacks in SHA. They are designed to ensure that SHA remain secure and available at all times. In our experiments, networks with a given number of DDoS nodes are randomly distributed in a 1000×1000 area. The number of cognitive nodes is 50,100,…,500. The cognitive radio nodes are initially randomly positioned in the given location. The attack was successful in retrieving sensitive data

from a medical system, highlighting the importance of protecting medical systems from malicious actors.

A. Performance Evaluation

We use test set vectors to construct some common metrics for evaluating our technique [36]. Before we discuss these metrics in detail, let's review some of the metrics that were used to calculate them:

- True Positive (*TP*): The mean of the successful simulation vectors that were correctly predicted as successful simulations.
- True Negative (*TN*): The mean of the unsuccessful test vectors that are correctly predicted as unsuccessful simulations.
- False Positive (*FP*): The mean of the vectors that were incorrectly predicted as successful simulations.
- False Negative (*FN*): The mean of the vectors that were incorrectly predicted as unsuccessful simulations.

We calculated the most well-known measures for evaluating classification algorithms using these metrics:

- Accuracy: This is the performance metric that measures how well a model's predictions align with the true outcomes.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (9)$$

- Percentage of error prediction: This is the performance metric that measures the percentage of incorrect detections.

$$\%\ of Err_p = \frac{Wrong_p}{N} * 100 \quad (10)$$

where N is the number of sample nodes provided as input and $Wrong_p$ are and the incorrect predictions generated by the network.

- Attack detection time: This is the performance metric that refers to the time it takes to detect the attack and it is measured as follows.

$$D_{time} = \sum_{i=1}^{n} DDoS_i * Time\ [MU_i] \quad (11)$$

where $DDoS_i$ is the number of DDoS nodes and $Time\ [MU_i]$ is the time taken to identify attacks.

1) Accuracy

Table I shows the results of attack detection accuracy, which is one of the most basic and fundamental performance indicators of any type of network. The attack detection accuracies for the four bio-inspired approaches are compared in Figure 5. It can be observed that the detection accuracy is not linear. In addition, the attack detection accuracy of HFA is 8% better than that of FA, 14% better than that of the EA, and 19% better than that of the Bat algorithm.

2) Error Prediction

Table II and Figure 6 show the comparison of error prediction. When a network is composed of both trusted and untrusted nodes, the percentage of error prediction does not increase accordingly, as was previously observed [2]. For all four methods the percentage of error prediction increases as the number of nodes increases. However, when HFA is used, the increase in the number of nodes seems to have less impact than for the other methods. This can also reduce the risk of system failures by addressing them before they become major problems.

TABLE I. RESULTS OF ATTACK DETECTION ACCURACY

No of DDoS nodes	Detection accuracy (%)			
	HFA	FA	EA	Bat
50	94.9	92	90	88.23
100	93.15	91.75	88.15	86.54
150	92.08	90.89	87.58	85.12
200	91.05	89.85	86.55	84.56
250	90.23	88.23	85.25	83.25
300	89.25	87.55	84.32	82.14
350	88.15	86.15	83.15	81.05
400	87.05	85.08	82.03	80.26
450	86.55	84.05	81.16	79.85
500	85.62	83.15	80.05	78.56

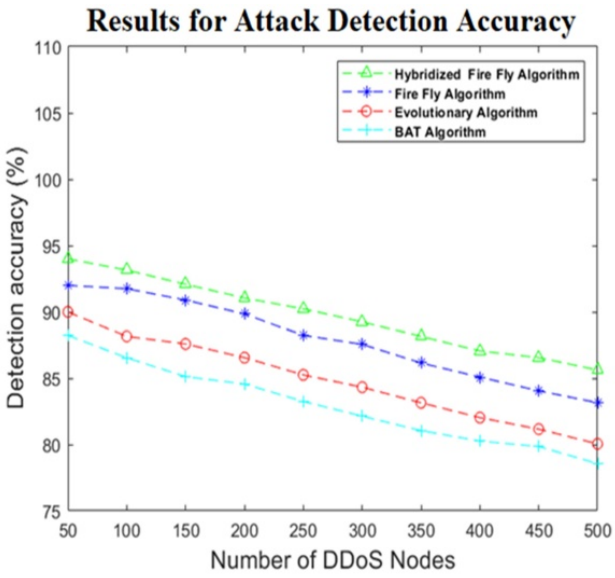

Fig. 5. Graph for attack detection accuracy.

TABLE II. RESULTS OF ERROR PREDICTION

No of DDoS nodes	Error prediction (%)			
	HFA	FA	EA	Bat
50	6	11	18	22
100	14	19	24	34
150	20	24	30	40
200	29	36	34	44
250	36	43	47	53
300	41	54	58	62
350	48	59	63	71
400	54	67	69	79
450	59	72	78	84
500	62	79	84	91

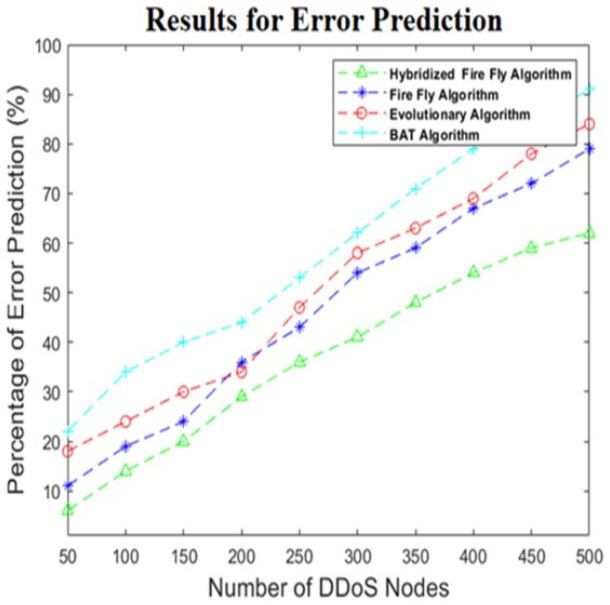

Fig. 6. Graph for error prediction.

3) Detection Time

In addition to the most important metrics, accuracy and error prediction, the time to detect an attack is a key element to investigate during the security design. Table III and Figure 7 present the detection time for the four algorithms. It can be observed that as the number of DDoS nodes increases, the detection time also increases, and as a result, the number of DDoS nodes depends on the detection time. The average detection time for 50 DDoS nodes was 1.12 ms with HFA, 1.69 ms with FA, 2.89 ms with EA, and 3.12 ms with Bat algorithm. The results indicate that HFA significantly reduces the detection time by 23% compared to the other algorithms.

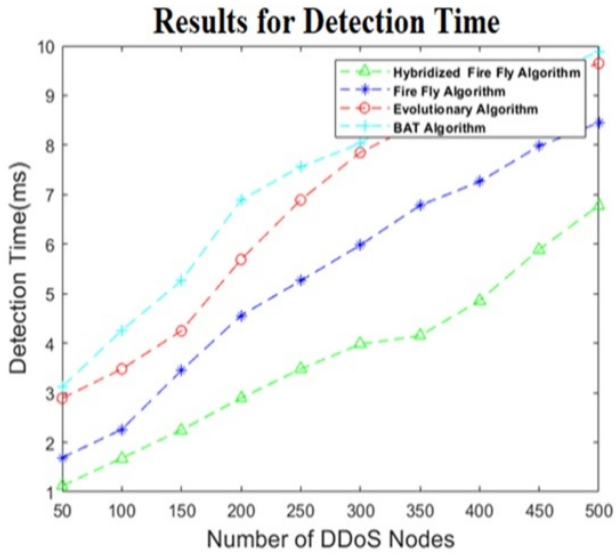

Fig. 7. Graph for detection time.

TABLE III. RESULTS OF DETECTION TIME

No of DDoS nodes	Detection time (ms)			
	HFA	FA	EA	Bat
50	1.12	1.69	2.89	3.12
100	1.68	2.26	3.48	4.26
150	2.25	3.45	4.25	5.26
200	2.89	4.56	5.69	6.89
250	3.48	5.26	6.89	7.56
300	3.98	5.98	7.85	8.03
350	4.15	6.78	8.45	8.91
400	4.86	7.26	8.98	9.12
450	5.89	7.98	9.25	9.35
500	6.78	8.45	9.65	9.89

IV. CONCLUSION

In order to improve patient care and protect the patient's life in case of emergency, sensors are used in smart health monitoring and send the latest information about the patient's health. The security and privacy of Smart Healthcare Applications (SHA) are highly crucial due to various types of threats and attacks. Existing attack detection methods are mostly dependent on high cost and detection time. In this study, a traffic preprocessing strategy is proposed to detect Distributed Denial-of-Service (DDoS) attacks and to increase the detection accuracy of the system. This article mainly focuses on hybrid bio-inspired approaches for a huge diversity of DDoS attack detection and mitigation on SHA with excellent attack detection rates. We propose a Hybridized Firefly Algorithm (HFA) mechanism to detect and mitigate DDoS attacks on the SHA environment in real time. The proposed algorithm demonstrated the highest accuracy in detecting and mitigating DDoS attacks with 94.9%. The error prediction of 6% and the detection time of 1.12 ms are the best among all the existing attack detection methods. We have demonstrated that the HFA monitors and detects the DDoS attacks with less complexity and higher accuracy. The statistical results show that our proposed hybridized method provides the best results for DDoS attack detection and prevention for SHA. In the future, we intend to design and develop various hybridized bio-inspired models for monitoring, detecting, and preventing the various types of known and unknown attacks on smart Internet of Things (IoT) applications in real-time infrastructure with improved performance and low complexity.

REFERENCES

[1] M. A. Tunc, E. Gures, and I. Shayea, "A Survey on IoT Smart Healthcare: Emerging Technologies, Applications, Challenges, and Future Trends." arXiv, Sep. 05, 2021, https://doi.org/10.48550/arXiv.2109.02042.

[2] Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," *IEEE Access*, vol. 9, pp. 161546–161554, 2021, https://doi.org/10.1109/ACCESS.2021.3128837.

[3] A. K. Singh, A. Anand, Z. Lv, H. Ko, and A. Mohan, "A Survey on Healthcare Data: A Security Perspective," *ACM Transactions on Multimidia Computing Communications and Applications*, vol. 17, no. 2s, May 2021, Art. no. 59, https://doi.org/10.1145/3422816.

[4] G. Sripriyanka and A. Mahendran, "A study on security privacy issues and solutions in internet of medical things—A review," in *Intelligent IoT Systems in Personalized Health Care*, A. K. Sangaiah and S.

Mukhopadhyay, Eds. Cambridge, MA, USA: Academic Press, 2021, ch. 6, pp. 147–175, https://doi.org/10.1016/B978-0-12-821187-8.00006-X.

[5] H.-S. Weber, "Multilateral Approaches to Cyber Security Capacity Building: The Rise of Non-Traditional Actors," B.A. thesis, Faculty of Social Sciences, Ludwig-Maximilians-Universität, Munich , Germany, 2022, https://doi.org/10.5282/ubm/epub.91373.

[6] N. B. Aissa and M. Guerroumi, "Semi-supervised Statistical Approach for Network Anomaly Detection," *Procedia Computer Science*, vol. 83, pp. 1090–1095, 2016, https://doi.org/10.1016/j.procs.2016.04.228.

[7] K. O. Adefemi Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer, and O. A. Alimi, "Refined LSTM Based Intrusion Detection for Denial-of-Service Attack in Internet of Things," *Journal of Sensor and Actuator Networks*, vol. 11, no. 3, Sep. 2022, Art. no. 32, https://doi.org/10.3390/jsan11030032.

[8] K. P. Vijayakumar, K. Pradeep, A. Balasundaram, and M. R. Prusty, "Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network," *Processes*, vol. 11, no. 4, Apr. 2023, Art. no. 1072, https://doi.org/10.3390/pr11041072.

[9] S. Almufti, "The novel Social Spider Optimization Algorithm: Overview, Modifications, and Applications," *Icontech International Journal*, vol. 5, no. 2, pp. 32–51, Sep. 2021, https://doi.org/10.46291/ICONTECHvol5iss2pp32-51.

[10] N. Kunhare, R. Tiwari, and J. Dhar, "Particle swarm optimization and feature selection for intrusion detection system," *Sādhanā*, vol. 45, no. 1, May 2020, Art. no. 109, https://doi.org/10.1007/s12046-020-1308-5.

[11] D. Jovanovic, M. Antonijevic, M. Stankovic, M. Zivkovic, M. Tanaskovic, and N. Bacanin, "Tuning Machine Learning Models Using a Group Search Firefly Algorithm for Credit Card Fraud Detection," *Mathematics*, vol. 10, no. 13, Jul. 2022, Art. no. 2272, https://doi.org/10.3390/math10132272.

[12] B. Pitchaimanickam and G. Murugaboopathi, "A hybrid firefly algorithm with particle swarm optimization for energy efficient optimal cluster head selection in wireless sensor networks," *Neural Computing and Applications*, vol. 32, no. 12, pp. 7709–7723, Jun. 2020, https://doi.org/10.1007/s00521-019-04441-0.

[13] S. U. Otor, B. O. Akinyemi, T. A. Aladesanmi, G. A. Aderounmu, and B. H. Kamagaté, "An adaptive bio-inspired optimisation model based on the foraging behaviour of a social spider," *Cogent Engineering*, vol. 6, no. 1, Jan. 2019, Art. no. 1588681, https://doi.org/10.1080/23311916.2019.1588681.

[14] S. A. Alshaya, "IoT Device Identification and Cybersecurity: Advancements, Challenges, and an LSTM-MLP Solution," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 11992–12000, Dec. 2023, https://doi.org/10.48084/etasr.6295.

[15] N. I. Haque, A. A. Khalil, M. A. Rahman, M. H. Amini, and S. I. Ahamed, "BIOCAD: Bio-Inspired Optimization for Classification and Anomaly Detection in Digital Healthcare Systems," in *2021 IEEE International Conference on Digital Health*, Chicago, IL, USA, 2021, pp. 48–58, https://doi.org/10.1109/ICDH52753.2021.00017.

[16] S. Dwivedi, M. Vardhan, and S. Tripathi, "Defense against distributed DoS attack detection by using intelligent evolutionary algorithm," *International Journal of Computers and Applications*, vol. 44, no. 3, pp. 219–229, Mar. 2022, https://doi.org/10.1080/1206212X.2020.1720951.

[17] A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, and R. Damaševičius, "Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things," *Electronics*, vol. 10, no. 11, Jan. 2021, Art. no. 1341, https://doi.org/10.3390/electronics10111341.

[18] R. A. Sowah *et al.*, "Design of a Secure Wireless Home Automation System with an Open Home Automation Bus (OpenHAB 2) Framework," *Journal of Sensors*, vol. 2020, no. 1, 2020, Art. no. 8868602, https://doi.org/10.1155/2020/8868602.

[19] H. HaddadPajouh, R. Khayami, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things," *Neural Computing and Applications*, vol. 32, no. 20, pp. 16119–16133, Oct. 2020, https://doi.org/10.1007/s00521-020-04772-3.

[20] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, Jul. 2020, Art. no. 102630, https://doi.org/10.1016/j.jnca.2020.102630.

[21] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications," *Sensors*, vol. 21, no. 11, Jun. 2021, Art. no. 3654, https://doi.org/10.3390/s21113654.

[22] C. Kiennert, Z. Ismail, H. Debar, and J. Leneutre, "A Survey on Game-Theoretic Approaches for Intrusion Detection and Response Optimization," *ACM Comput. Surv.*, vol. 51, no. 5, Aug. 2018, Art. no. 90, https://doi.org/10.1145/3232848.

[23] O. Almomani, "A Feature Selection Model for Network Intrusion Detection System Based on PSO, GWO, FFA and GA Algorithms," *Symmetry*, vol. 12, no. 6, Jun. 2020, Art. no. 1046, https://doi.org/10.3390/sym12061046.

[24] G. Sripriyanka and A. Mahendran, "Bio-inspired Computing Techniques for Data Security Challenges and Controls," *SN Computer Science*, vol. 3, no. 6, Aug. 2022, Art. no. 427, https://doi.org/10.1007/s42979-022-01292-w.

[25] D. Wang and G. Xu, "Research on the Detection of Network Intrusion Prevention With Svm Based Optimization Algorithm," *Informatica*, vol. 44, no. 2, Jun. 2020, https://doi.org/10.31449/inf.v44i2.3195.

[26] H. Grari, A. Azouaoui, and K. Zine-Dine, "A cryptanalytic attack of simplified-AES using ant colony optimization," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 5, pp. 4287–4295, Oct. 2019, https://doi.org/10.11591/ijece.v9i5.pp4287-4295.

[27] X. Kan *et al.*, "A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network," *Information Sciences*, vol. 568, pp. 147–162, Aug. 2021, https://doi.org/10.1016/j.ins.2021.03.060.

[28] R. O. Ogundokun, J. B. Awotunde, P. Sadiku, E. A. Adeniyi, M. Abiodun, and O. I. Dauda, "An Enhanced Intrusion Detection System using Particle Swarm Optimization Feature Extraction Technique," *Procedia Computer Science*, vol. 193, pp. 504–512, 2021, https://doi.org/10.1016/j.procs.2021.10.052.

[29] A. P. Johnson, H. Al-Aqrabi, and R. Hill, "Bio-Inspired Approaches to Safety and Security in IoT-Enabled Cyber-Physical Systems," *Sensors*, vol. 20, no. 3, Feb. 2020, Art. no. 844, https://doi.org/10.3390/s20030844.

[30] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020, https://doi.org/10.1109/ACCESS.2020.3037359.

[31] N. Jaya Krishna and N. Prasanth, "An Insight View on Denial of Service Attacks in Vehicular Ad Hoc Networks," in *Advances in Computational Intelligence and Communication Technology: Proceedings of CICT 2021*, Udaipur, India, 2021, pp. 273–285, https://doi.org/10.1007/978-981-16-9756-2_27.

[32] G. Sripriyanka and A. Mahendran, "Securing IoMT: A Hybrid Model for DDoS Attack Detection and COVID-19 Classification," *IEEE Access*, vol. 12, pp. 17328–17348, 2024, https://doi.org/10.1109/ACCESS.2024.3354034.

[33] G. Sripriyanka and A. Mahendran, "Mirai Botnet Attacks on IoT Applications: Challenges and Controls," in *Information Systems and Management Science: Conference Proceedings of 4th ISMS 2021*, Msida, Malta, 2021, pp. 49–67, https://doi.org/10.1007/978-3-031-13150-9_5.

[34] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016, https://doi.org/10.1109/JSEN.2015.2502401.

[35] G. Sripriyanka and M. Anand, "Issues and Solution Techniques for IoT Security and Privacy - A Survey," *International Journal of Computing and Digital Systems*, vol. 12, no. 4, pp. 909–928, Oct. 2022, https://doi.org/10.12785/ijcds/120175.

[36] S. Rengasamy and P. Murugesan, "Performance enhanced Boosted SVM for Imbalanced datasets," *Applied Soft Computing*, vol. 83, Oct. 2019, Art. no. 105601, https://doi.org/10.1016/j.asoc.2019.105601.