JOURNAL OF BASIC SCIENCE AND ENGINEERING

Securing SDN Networks: Leveraging Blockchain-Integrated IoT Devices for Advanced DDoS Attack Detection and Prevention

[1*]Kalpana Kumbhar

[1*] Assistant Professor, Department of E & TC, Vishwakarma Institute of information Technology

Maharashtra, Pune-48, Research Scholar, Cummins College of engineering,

[2]Prachi Mukherji

[2] Professor , Department of E&TC, Cummins College of Engineering, Pune ,Maharashtra, Pune-52

Abstract

In this extensive research, we thoroughly compared our proposed Hybrid (EH+WCO) model to current DDoS detection methods used Software-Defined Internet of Things (SD-IoT) networks. We sought to determine the usefulness of each model in minimizing cyber risks by meticulously evaluating important performance metrics including accuracy, precision, recall, and false alarm rates. Our results show the exceptional performance of the Hybrid approach, especially when combined with blockchain technology. With blockchain integration, the Hybrid model achieves 99.12% accuracy, 97% precision, 91% recall, and 92% F1-score, respectively. This is a major improvement in cybersecurity capabilities, showcasing blockchain's transformational potential in strengthening DDoS detection techniques. Notably, even without blockchain, the Hybrid model performs well, although somewhat lower, with 98.5% accuracy, 89% precision, 86.8% recall, and an F1-score of 83.8%. Furthermore, our findings highlight the Hybrid model's robustness and flexibility in dynamic network conditions, as indicated by considerable increases in packet delivery rates over time. Against this context, our suggested Hybrid model emerges as a leader, outperforming current models in terms of efficacy and dependability. This comprehensive comparison demonstrates the Hybrid model's excellence and ability to transform cybersecurity defenses in SD-IoT networks, paving the path for a safer and more resilient digital future.

Keywords: SD-IoT, DDo's, EH+WCO, BlockChain, Packet Delivery rates, False alarm rate.

Introduction

Cloud computing is seen as a game-changer for the information technology sector in today's globally linked society. This paradigm allows users to access shared databases for physical resources, including computing and storage, and a variety of on-demand services over a network. Customers may use these services use inexpensive commodity gear (such as a laptop) linked connect to the internet, allowing they need to provide answers to complicated issues without purchasing costly technology. In addition, users may access resources remotely from any place via cloud computing, which facilitates virtual collaboration. It speeds up improving resources, which was previously laborious with older computer systems that relied on hardware. The issue of excess and underutilization may be lessened with the help of appropriate resource utilization[1][2]. Cloud computing allows in order to provide PaaS stands for platform as a service, whereas IaaS and SaaS refer to infrastructure as a service and software as a service, respectively.

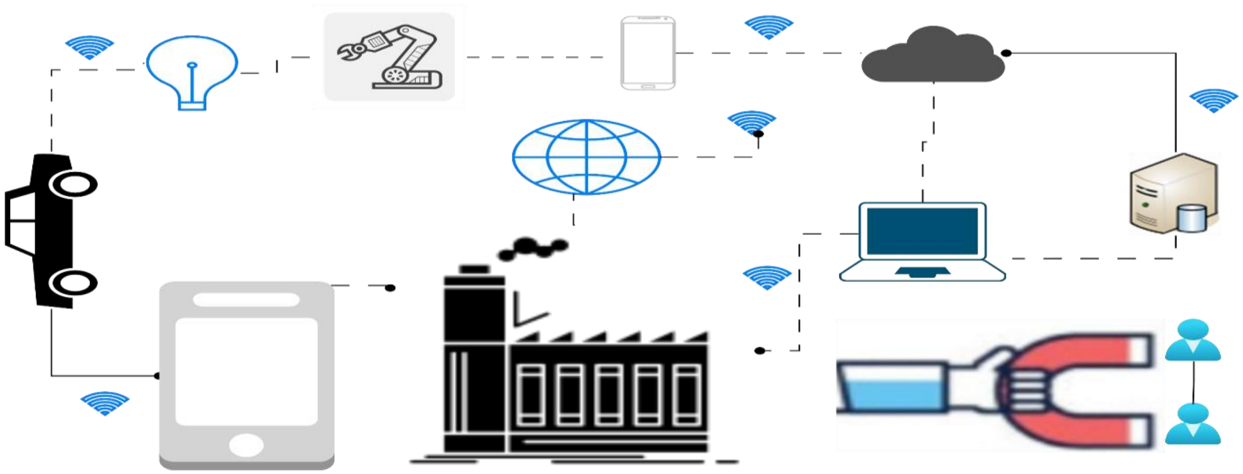
In addition to this, consumers may rely on cloud services any time since they are scalable, adaptable, and available on demand[3]. Another technology that is centered on security is blockchain (BC). Consequently, BC has technology garnered significant attention from the banking industry and other industries that place a premium on data protection. By bolstering data security, cloud services may enable BC with the inclusion of secret sharing[4]. In addition, by mandating detecting providers identify questionable suppliers, BC technology aids in the identification of harmful usage [5]. Much of the heavy lifting in this network-dependent application is performed by sensors, and the data gathered is then automatically shared between different parts of the company[6]. The automation process is beneficial to the IIoT-based industrial sector because it makes use of sensors, wireless networking devices, and models that make crucial choices using data obtained from network-connected sources[7]. However, since smart IIoT architecture is mostly based on networking, it attracts attackers who want to change the data collected for processing critical information[8].

This design secures the information communicated over the BC structure by generating a hash value. In addition, BC keeps the data in a public ledger so everyone with access to the ledger may see any updates. Consequently, the deal is safe from interference from any other parties[9]. And since there are so many financial and security-related aspects to cloud computing, BC can make cloud computing more reliable[10]. Support for Decentralised Networks (SDN)[11] is another new paradigm that simplifies and streamlines network management. Because cloud networks are notoriously difficult to administer and debug, it has found widespread use in this industry. Who are the users get access to sharing resources over the internet are directly impacted by the operation of the network. Software-defined networking (SDN) allows for programmatic control of networks. Due to the prevalence of network difficulties in cloud computing, SDN makes their management a breeze. Because users access shared resources over the internet, cloud computing is ineffective in a network-less environment. A new dimension in the network of gadgets is introduced by recent SDN applications that use multiple controllers. Data security and efficient management of resources have emerged as critical concerns due to the meteoric rise in popularity of this cloud computing model in recent years. Network traffic tracing and bandwidth estimation are two useful features of software-defined networking (SDN), which may help with resource management. In order to secure the data and make cloud activities simpler, it is essential to combine new developing technologies.

Propose a secure and distributed The above-mentioned research serves as the foundation for the Cloud control architecture based on BC and facilitated by SDN. Reliable and effective security is offered by a distributed BC in private and public cloud environments. The following are the contributions made by the study:

For intelligent IIoT applications, we suggest a distributed topology that will accelerate and dependability of logical and physical data on the cloud infrastructure.

- Our design uses a distributed SDN-BC method and smart IIoT improve security, privacy, and solitude.
- In IIoT applications, we evaluate a cloud model's viability based on several factors, including its ability to adapt to network threats.



Background

Water Cycle optimization algorithm

For the goal of evaluating the movement of water from rivers and streams toward the ocean, the Water Cycle Approach, which is also often referred to as The WCA, was developed. If there is rain or other precipitation, assume that it is occurring. A random starting population of design variables, often known as the population of streams, is formed once the rainy process has been completed. When classifying things according to the function that has the lowest cost (for the purpose of minimization), the sea is selected as the best person or stream.

All of the other streams eventually flow into rivers and the ocean, but a few exceptional streams—that is, the cost function values around Currently, the finest records are chosen as rivers.

Prior to commencing the process of optimization, it is required to launch the formation from the beginning of a population that represents a matrix consisting of rivers of size D. This is a prerequisite for beginning the optimization process. As a result, the matrix that was produced at random looks like this (the rows and columns represent that is, the total number of design variables, D and the population size, N_{pop} respectively):

$$\text{Total population} = \begin{bmatrix} Sea \\ River_1 \\ River_2 \\ River_3 \\ . \\ . \\ . \\ Stream_{Nsr+1} \\ Stream_{Nsr+2} \\ Stream_{Nsr+3} \\ . \\ . \\ . \\ Stream_{N_{pop}} \end{bmatrix} = \begin{bmatrix} x_1^1 & x_2^1 & x_3^1 & \dots & x_D^1 \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_D^2 \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ x_1^{N_{pop}} & x_2^{N_{pop}} & x_3^{N_{pop}} & \dots & x_D^{N_{pop}} \end{bmatrix} \tag{1}$$

Creating N_{pop} streams is the first step. The finest candidates N_{sr} (minimum values) are then chosen to represent the sea and rivers. The sea is defined as the stream with the lowest value (objective function), among others. Actually, N_{sr} is the total of one sea and the user-defined number of rivers. The remaining population, or N_{stream}, is thought of as streams that either run straight into the sea or into rivers.

Every river takes in water from streams to varying degrees, depending on the flow pattern. Because of this, the volume of water that enters a river and/or the sea differs depending on the stream. Moreover, rivers fall into the sea, which is the lowest point. The following Equation [8] is used to determine the allocated streams for each river and the sea:

$$NS_n = round\left\{ \left| \frac{\mathrm{Cos}\,t_n - \mathrm{Cos}\,t_{N_{sr}+1}}{\sum_{n=1}^{N_{sr}} C_n} \right| \times N_{Streams} \right\}, \; n = 1, 2, 3, \dots, N_{sr,} \tag{2}$$

There are a total number of rivers and streams that have been approved to flow into the ocean, and this equation indicates the entire number of these streams and rivers. A schematic picture of a stream traveling down a connecting line towards a particular river is shown in Fig. 1a.

The following additional locations for streams and rivers have been proposed for the WCA's exploitation phase [3]:

$$\vec{X}_{Stream}(t+1) = \vec{X}_{Stream}(t) + rand \times C \times (\vec{X}_{Sea}(t) - \vec{X}_{Stream}(t))$$

(3)

$$\vec{X}_{Stream}(t+1) = \vec{X}_{Stream}(t) + rand \times C \times (\vec{X}_{River}(t) - \vec{X}_{Stream}(t))$$

(4)

$$\vec{X}_{Stream}(t+1) = \vec{X}_{Stream}(t) + rand \times C \times (\vec{X}_{Sea}(t) - \vec{X}_{River}(t))$$

(5)

Where rand a random integer that uniformly spread across the range from zero to one and t is the iteration index, with 1 < C < 2 and 2 may be the optimum choice for C. The streams that empty into the sea and the accompanying rivers are covered by equations (3) and (4), respectively.

If the stream's answer is better than the connecting river's, their positions are flipped. A river and the sea may be exchanged in a manner similar to this.

In addition, the evaporation process operator used in order to prevent initial (immature) convergence to local optimal solutions during the exploitation stage. In essence, when rivers and Streams run into evaporation causes allow seawater to evaporate. This causes more precipitation to fall.

Therefore, it is necessary for us to determine whether or not the river or stream is located in close proximity to the ocean for the evaporation process to take place. According to the following criteria, the circumstances of evaporation that exist between a river and the sea are determined in order to achieve this objective:

$$f \left\| \vec{X}^{t}_{Sea} - \vec{X}^{t}_{River_j} \right\| < d_{\max} \quad \text{or} \quad \vec{x}_{River}(t+1) = \vec{X}_{River}(t) + rand \times C\left(\vec{X}_{Sea}(t) - \vec{X}_{River}(t)\right) rand < 0.1$$

$$j = 1, 2, 3, ..., N_{sr} - 1$$

Perform the rainfall procedure using a consistent Random search and where $d_{\max}$ a negligible value that is near zero. After evaporation, it rains mechanism is used, resulting in the formation of new streams in various places (much as with GA mutations). In fact, the WCA's exploratory phase is within the purview of the evaporation operator.

The freshly generated streams' new positions are determined using uniform random search:

A high $d_{\max}$ number discourages further searches, whereas a low value increases the intensity of searches close to the coast. As a result, $d_{\max}$ regulates search intensity (i.e., the best solution that was achieved) close to the coast. The following is the adaptive reduction in $d_{\max}$ value [8]:

$$d_{\max}\left(t+1\right)=d_{\max}\left(t\right)-\frac{d_{\max}(t)}{Max.Iteration}\quad t=1,2,3......,Max\_Iteration. \tag{6}$$

In Fig. 1b, the evolution of the WCA optimization procedure is shown, with the diamond, rivers, and streams represented by the circles, stars, and sea, respectively. The newly-occupied locations of streams and rivers are shown by the white (empty) forms.

ELEPHANT HERDING OPTIMIZATION

To use Herding habit of elephants to solve various global optimisation issues, it is recommended for the purpose of simplifying it into the following ideal guidelines.

1) The population of elephants is structured into large number of clans, each of which has certain number of elephants.
2) Each generation selects some set elephants that are masculine in number from the main elephant population to live alone in a remote place, isolated from their family group.

3) There is a matriarch who oversees the interactions amongst the elephants that make up each clan.

A. Clan updating operator

Elephants live in clans led by matriarchs. Therefore, matriarch ci influences the future place of each elephant in clan ci . The elephant in clan may be adjusted as follows:

$$x_{new,ci,j}=x_{ci,j}+a\times\left(x_{best,ci}-x_{ci,j}\right)\times r \tag{1}$$

$x_{new,ci,j}$ and $x_{ci,j}$ represent updated and older positions of elephant j in clan ci , correspondingly.

$\alpha \in [0,1]$ is a scale factor that specifies the effect of matriarch ci on $x_{ci,j}$. $x_{best,ci}$ symbolises matriarch ci , the fittest elephant in the clan $ci.r \in [0,1]$. Here, uniform distribution is used.

Eq. (1), i.e., $x_{ci,j} = x_{best,ci}$. ,cannot be updated to reflect the fittest elephant from each clan.

The most suitable one may be adjusted as

$$x_{new,ci,j} = \beta \times x_{center,ci} \tag{2}$$

Where $\beta \in [0,1]$ is a component that influences the impact of the $x_{center,ci}$ on $x_{new,ci,j}$. The new person is visible to us $x_{new,ci,j}$ Eq. (2) is created by knowledge collected by all elephants in the clan ci . $x_{center,ci}$ is the center of clan Ci, and the dth dimension is calculated

$$x_{center,ci,d} = \frac{1}{n_{ci}} \times \sum_{j=1}^{n_{ci}} x_{ci,j,d} \tag{3}$$

where $1 \le d \le D$ is the d-th dimension and total dimension. n_{ci} is the number of elephants in clan ci. $x_{ci,j,d}$ is the d-th of elephant individual $x_{ci,j}$. The centre of clan ci , $x_{center,ci}$, can be determined using Eq. (3). The clan update operator may be developed using the description provided above.

B. Separating operator

When male elephants reach the age of maturity, they separate from their family group and begin to live on their own. One possible representation of this separation approach is a Separating operator, which is used when dealing with optimization challenges. To provide the EHO technique a stronger ability to search for information, it is assumed that the elephant individuals with the lowest fitness would use the separation operator at each generation, as shown by Equation (4).

$$x_{worst,ci} = x_{\min} + (x_{\max} - x_{\min} + 1) \times rand \tag{4}$$

where $x_{\max}$ and $x_{\min}$ are the top and lower bounds of an individual elephant's location. $x_{worst,ci}$ is the worst elephant member in the clan ci. $rand \in [0,1]$ is a kind of stochastic distribution, in this investigation, we picked consistent distribution over the [0,1] range.

Algorithm 1 Hybrid Water Cycle and Elephant Herding Optimization (HWEHO)

```
        1: Initialize:
```

```
    · Initialize population wca using Water Cycle Optimization (WCA).
    · Divide population wca into clans for Elephant Herding
      Optimization (EHO).
while not convergence criteria met () do
    Clustering:
        · Apply WCA clustering to identify sea and rivers.
    Position Update:
        · Update positions of elephants within each clan using EHO operators.
    Separation and Diversity:
        · Identify worst-performing elephants in each clan.
        · Apply Separating Operator to introduce diversity.
    Fitness Evaluation:
        · Evaluate fitness of individuals within clans.
    Position Update (Global and Local Search):
        · Update positions of individuals within each clan using EHO operators.
    Exploitation:
        · Apply WCA evaporation process for local exploitation.
    Exploration:
        · Apply WCA Raining Process for global exploration.
    Adaptive Parameter Adjustment:
        · Adjust dmax value adaptively.
end while
Output:
    · Best solution found during the optimization process.
```

Literature Review

[12] This research aims to create a botnet prevention system that utilizes SDN and blockchain technologies. The authors of this study have created a system to identify and counter botnets by using blockchain technology and Software-Defined Networking (SDN). The findings and performance demonstrate that the suggested method works properly.

[13] The paper examines and classifies current advanced DoS attack techniques, detection strategies, and mitigating solutions intended for Blockchain peer-to-peer networks and traditional network cryptocurrency exchanges. Previous study indicates that the blockchain ecosystem is vulnerable to possible DoS attacks in the future, highlighting the need for technology developments to prevent such assaults.

[14] The study proposes the Cluster Block model, Distributed security design of a smart grid that incorporates Blockchain technology applied in an SDN cluster configuration. Decentralized peer-to-peer networks are made possible by blockchain technology, which allows these networks to facilitate safe interactions between untrusted nodes. Because of the architecture, this article makes use of If you use a distributed cluster of SDN controllers, you can avoid the possibility of one single area of vulnerability and ensure that load is divided equally between the controller and the device. A blockchain that is comprised of an SDN cluster head is produced as a consequence of each SDN cluster having a cluster head that functions as a blockchain node. Possibly, the blockchain technology will grow. When the SDN communication network is integrated, security and privacy are enhanced. This study develops a distributed control mechanism and a network danger detection method using blockchain consensus. It also employs the Jaccard similarity coefficient to detect network threats. The study assesses the Cluster Block model and an established model using the Open Flow protocol by conducting simulated tests and analysing their security performance. The assessment findings indicate that the Cluster Block model has greater bandwidth stability and enhanced security performance when confronted with DDoS assaults of equivalent magnitude.

[15] The authors introduced a lightweight security architecture (Bloc-Sec) for software-defined networking (SDN) and network functions virtualization (SDN/NFV) that is based on blockchain technology. By using 5G/B5G connectivity, this design enhances the security of Internet of Things (IoT) networks in cloud environments. In the beginning, they use the Blake-256 hashing algorithm, which incorporates a number of different parameters, to verify all the Internet of Things devices with the blockchain server. In the second step of the process, they choose the most effective form of the cuttlefish optimization technique to a virtual network function (VNF). The third use of blockchain technology is to record the hashed flow rules that are stated in VNF. Through the use of spiking dual fuzzy neural networks, the controller makes a contribution to the classification of packets by analyzing the contents and headers of the packets. A deployment of NS3.26 is carried out, and its performance is examined for the purposes of testing.

[16] In this article, the "DistB-SDCloud" architecture is presented. Encouraging more secure cloud computing for Internet of Things applications is the aim of this approach. The suggested approach is flexible and scalable, and it leverages distributed blockchain technology to provide a

number of advantages such as security, secrecy, privacy, and integrity. British Columbia offers an efficient and decentralized environment that benefits its customers in the industrial sector. The authors also proposed an SDN strategy for improving workload resilience, consistency, and distribution in cloud infrastructure. For the purpose of conducting an experimental assessment of the performance of our software-defined networking (SDN) and business continuity (BC)-based deployment, we tracked throughput, packet analysis, response time, bandwidth, latency, and system hazards.

[17] To securely transfer critical Controller Area Network (CAN) data, the authors created BFF-IDS, An SDN-based Intrusion Detection System integrated with a Federated Forest powered by blockchain. For scalability, we used IPFS to host the models. Only the model hash and its location were intended to be stored on the blockchain. Model transfer and dynamic packet routing are made possible by the SDN. A random forest model was built by Federation Learning. To secure data, individuals submit semi-trained models. To improve multiclass attack detection, we used the Fourier transform to convert CAN ID cycles from CAN bus data to the frequency domain. To address CAN bus traffic complexity and nonlinearity, statistical and entropy components were extracted. The recommended strategy lets manufacturers and car owners train models while protecting sensitive data. Blockchain storage of model hashes eliminates a single point of failure and decreases the risk of model manipulation. We tested the proposed system. The recommended approach used memory and CPU efficiently and detected closely linked attacks well. Model attack detection peaked at 0.981.

[18] This paper introduces a blockchain-enabled protocol (BEP) for safe fitness Internet of Things applications, using self-exposing nodes (SEN). Blockchain and SDN designs utilize extensive security monitoring, analysis, and response mechanisms to increase IoT security. The recommended method detects and mitigates IoT fitness system DoS and DDoS assaults. The BEP manages Blockchain activities, whereas the SEN might be a fitness IoT sensor or actuator unit. SEN transmits incoming and outgoing traffic data to BEP, which analyzes fitness IoT system DoS/DDoS assaults. The System Entity Node (SEN) computes incoming and outgoing traffic entropies before sending them to the Blockchain as transaction blocks. SDN controller nodes get all transactions from mined blocks from the Blockchain Event Processor. To detect DoS or DDoS assaults, the controller node verifies SEN entropy. Decision points are SEN and

Controller. Entropy and attack detection rates were measured over many testing of our suggested system. Attack detection rate was 11% and 18% higher for the suggested method than strategy 1 and Approach 2.

Methodology

SDN Smart Contract with Cluster-Based Anomaly Detection

The separation of network administration and forwarding operations is achieved by the use of cluster-based anomaly detection in conjunction with smart contracts in Software-Defined Networking (SDN), providing a feasible technique for enhancing network administration and security. By using deep learning methods, this inventive smart contract guarantees the integrity and dependability of network operations by detecting and mitigating network abnormalities.

Parameters of the SDN Smart Contract:

- **a) Party Address:** Every member of the SDN network is given a distinct address for system identification and communication.
- **b) Publisher:** The entity in charge of setting up and maintaining network settings and rules in an SDN environment.
- **c) Subscriber:** Programs or users on a network that make advantage of SDN services, such resource allocation and traffic routing.
- **d) Sender:** The person who starts SDN-related processes, such changing routing tables or setting up network rules.
- **e) Receiver:** In an SDN system, the receiver of transactions is in charge of putting changes into effect or upholding network rules.
- **f) System Integrity Verification:** Procedures set in place by senders or recipients to guarantee the accuracy and legitimacy of network setups and data.

Algorithm 1: SDN Smart Contract with Cluster-Based Anomaly Detection (SDNSC-CAD)

```
Require: Network traffic data matrix: $D \in R^{m \times n}$
Transaction request initiated by sender
Smart Contract ID (SC_ID)
Stream ID (S_ID)
```

```
Ensure: Processed transaction data
Ensure: Notification in case of anomalies detected
Initialization:
Initialize contract parameters:
Party addresses, publisher, subscriber, sender, receiver
System Integrity Verification (SIV)
Smart Contract details (S_ID)
Transaction Initiation:
Sender initiates a transaction request to analyze network traffic data.
Stream Assignment:
Assign a unique Stream ID (S_ID) to the network traffic data.
Contract Activation:
Activate the SDN Smart Contract using SC_ID.
Data Transmission and Processing:
Transmit the transaction data streams (S_ID) to a cluster-based model.
Perform necessary data processing.
Anomaly Detection:
Let C be a clustering algorithm.
Cluster the processed data into k clusters: $\{C_1, C_2, ..., C_k\}$ using C
Identify anomalous clusters based on their characteristics.
Flag abnormal data streams for further investigation if detected.
Transaction Processing:
If no anomalies detected:
Proceed with processing the transaction.
Update network configuration or routing decisions accordingly.
Anomaly Handling:
Notify the Network Operations Center (NOC) or designated personnel of detected anomalies.
Provide details for further analysis and intervention.
Communication and Governance:
```

31: Facilitate communication between involved parties.

32: Ensure transparency, security, and reliability throughout the transaction lifecycle.

The transformation of smart contract data to Hyperledger Fabric, a permissioned blockchain platform, owing to its powerful capabilities designed for corporate applications. Hyperledger Fabric provides a safe and scalable environment while maintaining data privacy and confidentiality, making it perfect for handling critical corporate data. By exploiting Hyperledger Fabric's chain code features, we can securely connect with the ledger, update data, and execute business logic, allowing for speedy and trustworthy network transactions.

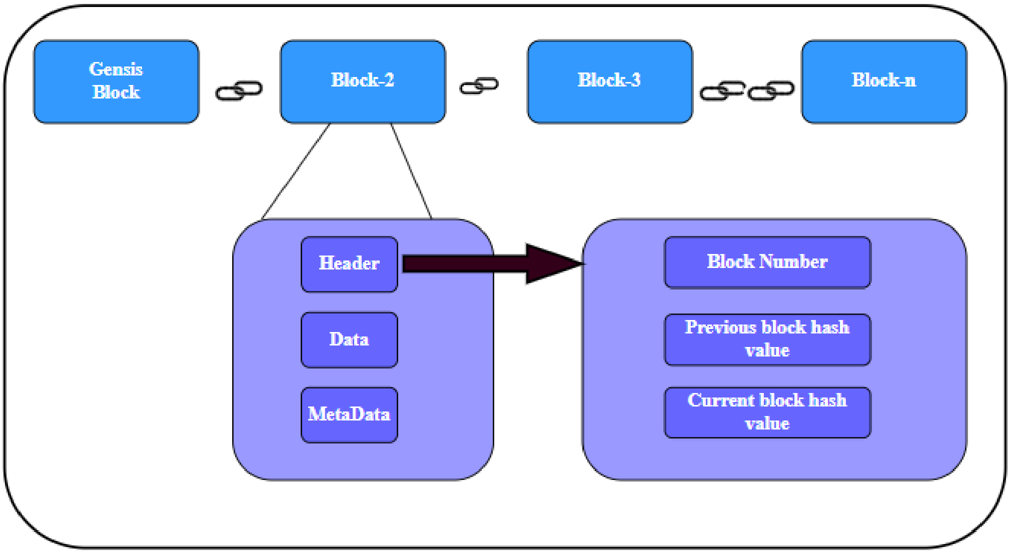


Figure 1Hyperledger block chain block structure

a. Header: The information about the block is included in this block header. It includes the data that is listed below.

• **Block number:** The unique identification that the validator node assigns to each freshly created block in the system is known as the block number. In subsequent communications, this block number will be utilised to access a particular blockchain block.

• **preceding block hash value:** SHA256 was used to get the preceding block's 256 bit hash value.

• **The current block hash value:** stored in hexadecimal format, is 256 bits.

b. Data: The second component of the block is called "Data.". Tis The section contains a genuine signature made using standard format.

c. Metadata: Metadata includes Details about the block, such as date when it was generated, consensus procedures, the initiator and validator's private keys, and, if applicable, signature details.

In Hyper ledger, each block is linked to the block before and after it by a link called a block hash value. This is how block chain design works.
Strong Hash method (SHA256) is the secure hashing method that Hyper ledger uses by default. SHA-1 and SHA-2 have been replaced by this one. It gives each block a unique 256-bit (32-byte) hash number. Hexadecimal is the most common way to show hash numbers. As of now, the SHA256 method has not been broken in any way. In Hyper ledger, SHA256 is used as the default hash method for this reason.

Problem Formulation:

Using the K-Means approach, we aim to divide a dataset consisting of N data points into K groups. To denote the assignment of data point x_i to cluster k, we introduce binary variables $\delta_{i,k}$. We also propose binary variables, β_i, to detect abnormalities. This is how the objective function J is expressed:

$$J = \sum_{i=1}^{N} \sum_{k=1}^{K} \delta_{i,k} . d(x_i, \mu_k)^2 + \alpha \sum_{i=1}^{N} \beta_i$$

The distance between data point x_i and the centroid μ_k is denoted by $d(x_i, \mu_k)$, where α is a hyper parameter that regulates the balance between anomaly detection and clustering accuracy.

Optimization Problem:

The definition of the optimization is:

Minimize J with respect to $\{\mu_k\}, \{\delta_{i,k}\}, \{\beta_i\}$

Subject to:

1. One cluster is allocated to each data point: $\sum_{k=1}^{K}\delta_{i,k} = 1$ for all i.

2. Anomalies are correctly identified: $\beta_i = 1$ if x_i is an anomaly.

3. No cluster is identified to anomalies: $\sum_{k=1}^{K}\delta_{i,k} \leq 1$ for all i.

By penalizing anomalies in addition to capturing regular patterns, this optimization approach makes sure that the clustering process produces a more reliable anomaly detection model.

Performance Metrics

The F1 score, precision, sensitivity, and accuracy are some of the performance measures that are used to assess algorithms. The confusion matrix concept is the source of these measurements.

Accuracy: The percentage of subjects that have been carried out appropriately recognized in relation to the total number of subjects is referred to as the subject recognition coefficient.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

Sensitivity: Recall, which is synonymous with sensitivity for the sake of this discussion, is the percentage of actual positive labels that our system can consistently identify at any given moment.

$$Sensitivity = \frac{TP}{TP + FN} \tag{12}$$

Precision: Counting the number of right forecasts may help to measure an outlook's accuracy. Another term for this concept is "predictive value."

$$\Pr ecision = \frac{TP}{TP + FP} \tag{13}$$

Specificity: Specifically, the approach detected the negative.

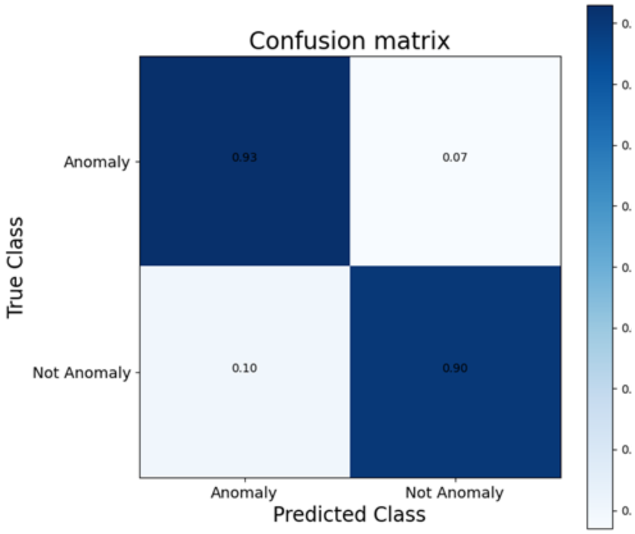
$$Specificity = \frac{TN}{TN + FP} \qquad (14)$$

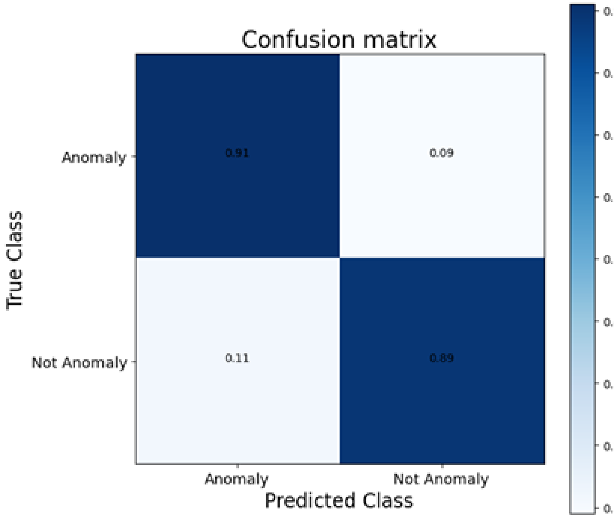
FN = false negative, FP = false positive, TP = true positive, and TN = true negative.

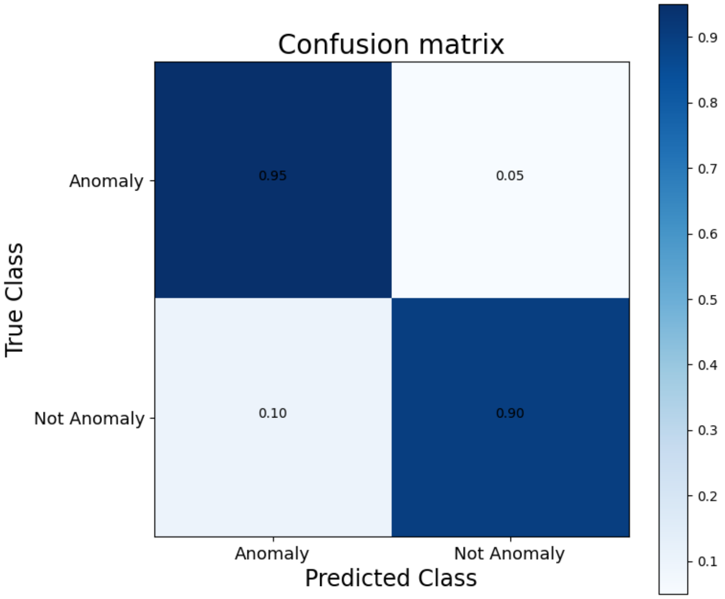
RESULTS

Python, Windows 10, 8 GB RAM, 512 GB HDD, and an Intel Core i3 CPU are utilized for implementation.

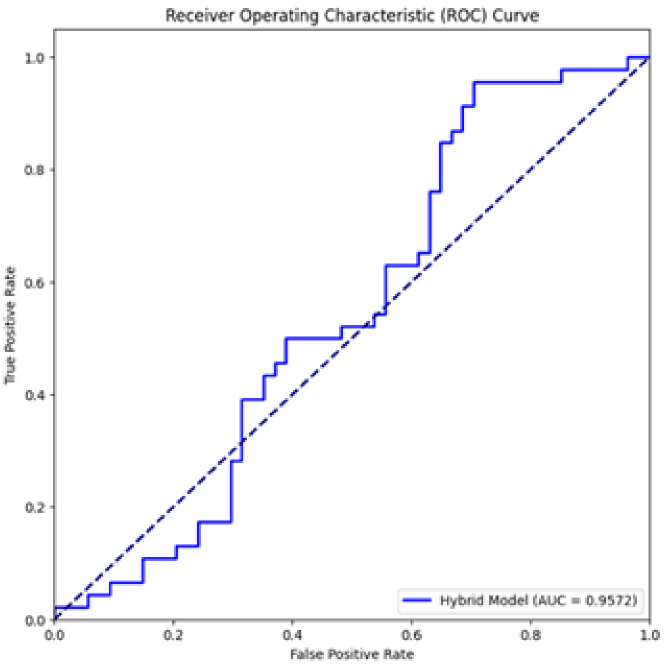
This research used a hybrid model to identify anomalies using the water cycle optimization technique and elephant heading optimization. Our hybrid model was also compared to water cycle optimization and elephant heading optimization models.







The confusion matrix above displays two classes: "Anomaly" and "Not Anomaly," with rows and columns representing each class. Each cell's value indicates the percentage of data points that were expected to belong to a certain class but actually belong to a different class. The number 0.95 in the top left cell, labelled "Anomaly" and "Anomaly," indicates that 95% of the data points identified as anomalies by the model were indeed anomalies. The number 0.10 in the bottom left cell, labelled "Not Anomaly" and "Anomaly," indicates that 10% of the non-anomalous data items were inaccurately classified as anomalies. The confusion matrix indicates that the model is working well, with most values aligning on the diagonal, showing a high number of accurate predictions. It is crucial to take into account the particular context of the issue and the significance of accurately categorizing each class to assess the model's performance.



The ROC curve demonstrates a classification model's performance over thresholds. This graph displays TPR on the y-axis and FPR on the x-axis. The image shows a blue ROC curve with a positive slope, which is desirable. A perfect classifier would have a ROC curve that extends vertically up the left side of the plot and then horizontally across the top. The fact that the model is able to appropriately differentiate between good and negative circumstances is shown by this phenomenon. The performance of the model is represented by the region to the right of the ROC area under the curve. The graphic shows a hybrid model with an AUC of 0.9572, which is regarded outstanding. An AUC of one suggests a flawless model, while AUC 0.5 shows the model is no better than random prediction. Overall, the ROC curve in the above figure demonstrates that the hybrid model is effective at distinguishing between positive and negative cases. The model has a high AUC, and the figure's upper-left corner displays the ROC curve.

Table 1 Execution time—query

No. of transactions	Hyperledger fabric v2.0	Hyperledger

10	0.15	0.08
100	0.96	0.55
1000	10.26	3.11
10,000	56.25	14.25

Table 2 Latency on average—question

No. of transactions	Hyperledger fabric v2.0	Hyperledger sawtooth
10	2.25	1.23
100	3.57	2.1
1000	17.21	13.64
10,000	72.35	32.11

Table 3 Time of execution—the initialization procedure

No. of transactions	Hyperledger fabric v2.0	Hyperledger sawtooth
10	1.3	0.64
100	2.31	1.24
1000	10.55	6.11
10,000	74.21	55.3

Table 4 Average Latency—Initialization Process

No. of transactions	Hyperledger fabric v2.0	Hyperledger sawtooth
10	3.2	1.2
100	8.2	5.68
1000	26.1	23.13
10,000	56.2	48.34

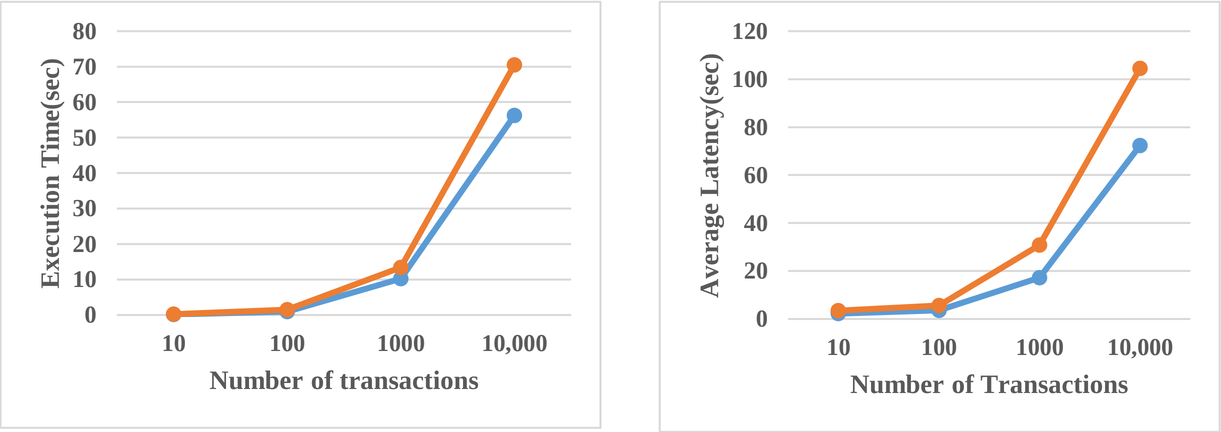
Table 5 Execution time—validation process

No. of transactions	Hyperledger fabric v2.0	Hyperledger sawtooth

10	5.19	2.32
100	10.22	6.12
1000	25.2	20.31
10,000	71.33	57.2

Table 6 Average latency—validation process

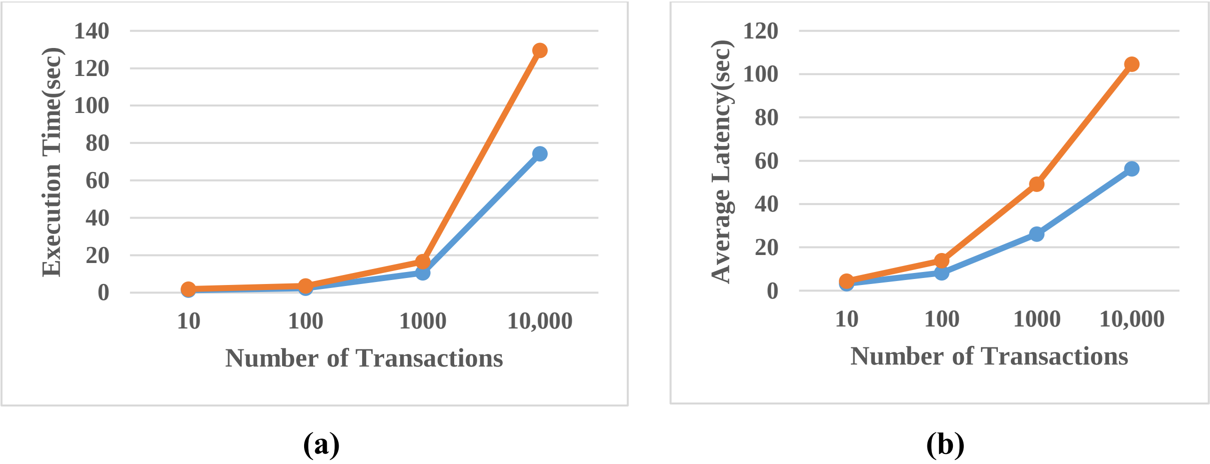
No. of transactions	Hyperledger fabric v2.0	Hyperledger sawtooth
10	7.12	6.78
100	20.23	16.98
1000	44.13	37.11
10,000	86.12	77.09



(a)

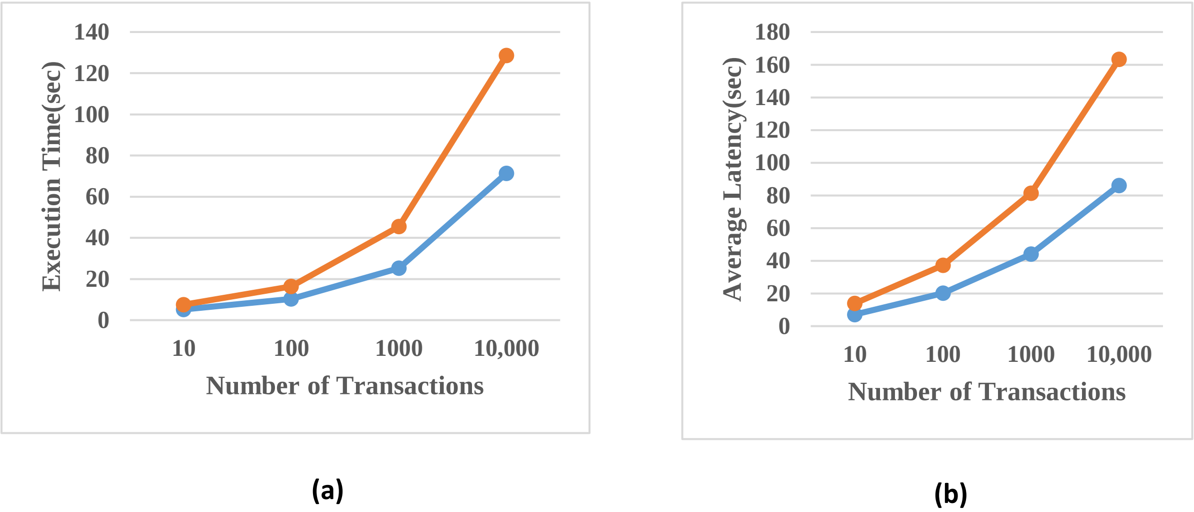
(b)

Figure 2 Blockchain performance for a basic query: (a) execution time and (b) average latency.



(a) (b)

Figure 3 Blockchain performance for the initialization process, including (a) execution time and (b) average latency.



(a) (b)

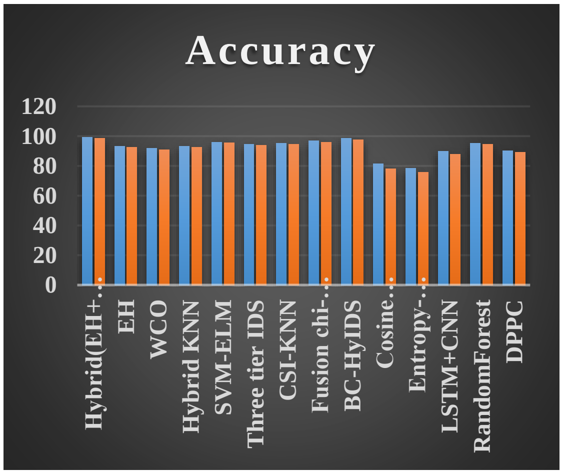
Figure 4 Blockchain performance for validation: an execution time and b average latency.

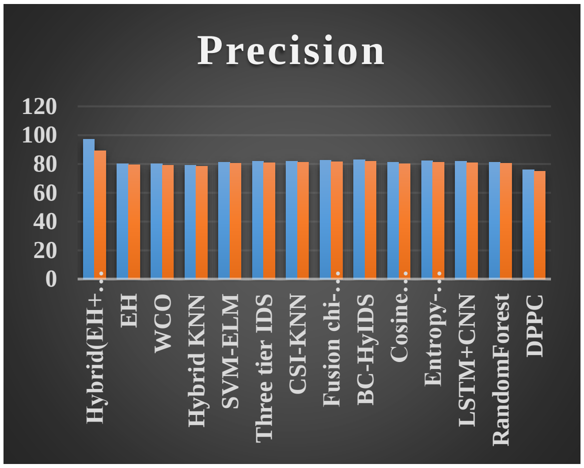
Implementation utilizes Hyperledger Fabric v2.0 with Sawtooth. Transaction processing time, throughput, average latency, and execution time are among the performance metrics used for evaluation. Performance of the system is classified into two categories: IDS performance (both with and without block-chain) and block-chain performance. According to the experiments, Hyperledger sawtooth beats Hyperledger fabric v2.0. IDS accuracy improves when a block chain is used (Tables 2, 3, 4, 5, and 6).

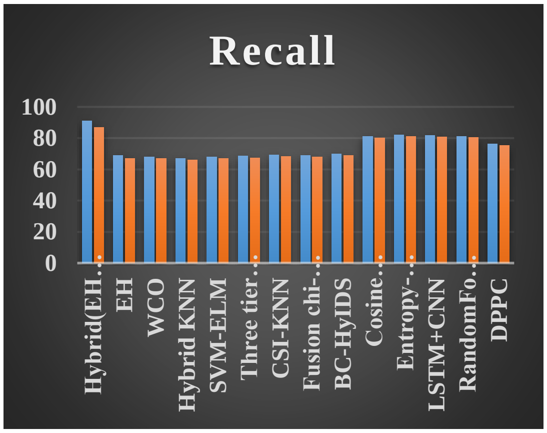
Table 7 Performance metrics comparision of all models

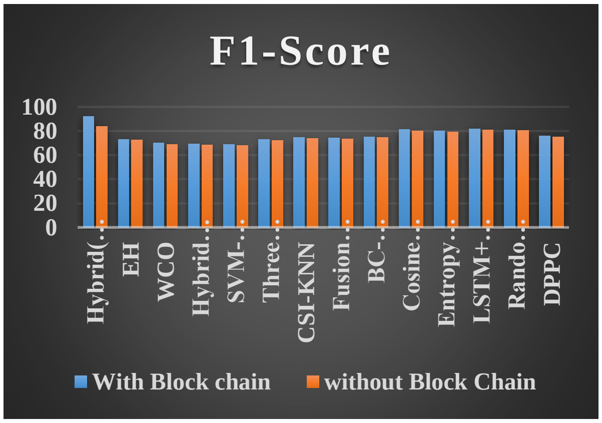
	Model	Accuracy	Precision	Recall	F1-Score
With Block chain	Hybrid(EH+WCO)	99.12	97	91	92
	EH	93.27	80	69	73
	WCO	92	80	68	70
	Hybrid KNN	93.29	79	67	69.4
	SVM-ELM	95.86	81	68.1	68.89
	Three tier IDS	94.71	81.8	68.6	73.1
	CSI-KNN	95.1	82	69.2	74.7
	Fusion chi-square and SVM	97	82.4	68.97	74.32
	BC-HyIDS	98.5	82.9	70	75
	Cosine similarity-based SD-IoT	81.4	81	81.2	81.2
	Entropy-based model	78.6	82.1	82.1	80.1
	LSTM+CNN	89.8	81.9	81.9	81.8
	RandomForest	95.1	81	81	81
	DPPC	90.1	76	76.2	76
without Block Chain	Hybrid(EH+WCO)	98.5	89	86.8	83.8
	EH	92.5	79.5	67	72.5
	WCO	91	79	67	69
	Hybrid KNN	92.5	78.5	66	68.4
	SVM-ELM	95.5	80.5	67.1	67.89
	Three tier IDS	94	80.8	67.3	72.1
	CSI-KNN	94.5	81	68.2	73.7
	Fusion chi-square and SVM	96	81.4	67.97	73.32
	BC-HyIDS	97.5	81.9	69	74.5
	Cosine similarity-based SD-IoT	78	80	80.2	80.2

	Entropy-based model	75.6	81.1	81.1	79.1
	LSTM+CNN	87.8	80.9	80.9	80.8
	RandomForest	94.5	80.5	80.5	80.5
	DPPC	89.1	75	75.2	75





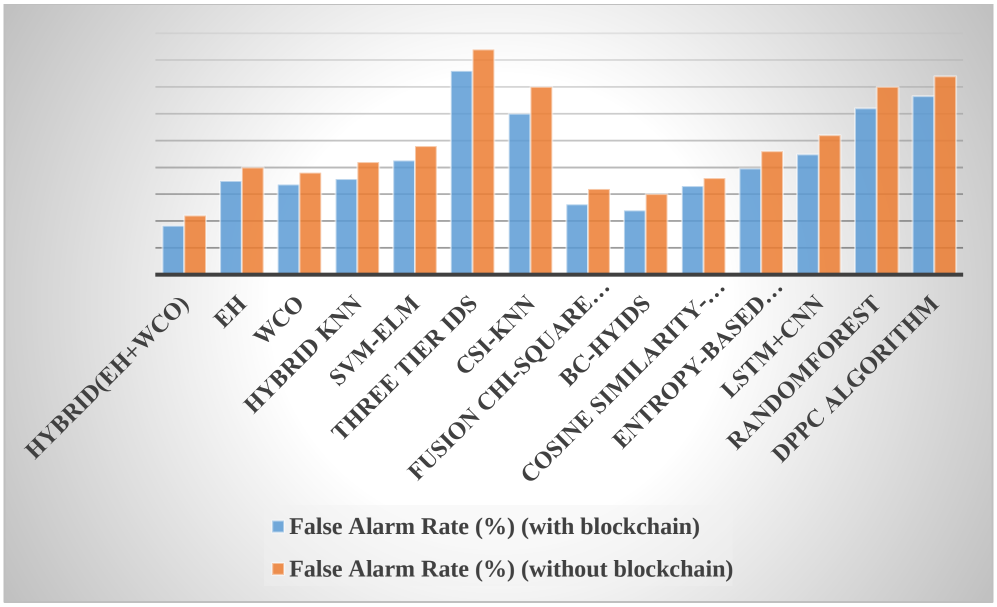




From the above table and graphs we can observe that the performance metrics of several models for detecting DDoS attacks on SD-IoT networks with and without blockchain integration. The Hybrid (EH+WCO) model is specifically highlighted, with an assessment of its performance with and without blockchain technology, as well as other significant models in the sector. With blockchain integration, the Hybrid (EH+WCO) model achieves amazing 99.12% accuracy, 97% precision, 91% recall, and 92% F1 score. Without blockchain, its performance is somewhat worse, with 98.5% accuracy, 89% precision, 86.8% recall, and an F1-score of 83.8%. This disparity emphasizes the significant role of blockchain technology in improving the model's overall performance. Similarly, other models show different performance metrics with and without blockchain integration, demonstrating the importance of decentralized security protocols in improving the accuracy and reliability of DDoS detection systems. Notably, models such as Three-tier IDS, Fusion chi-square and SVM, and BC-HyIDS exhibit significant performance gains with blockchain integration, demonstrating the effectiveness of merging sophisticated detection methods with decentralized security frameworks. Overall, the comparative analysis highlights blockchain technology's critical role in improving the effectiveness of DDoS detection models, with the Hybrid (EH+WCO) model emerging as a strong contender, particularly when combined with blockchain, for protecting SD-IoT networks from cyber threats.

Table 8 False Rate Percentage of the models

Model	False Alarm Rate (%) (with blockchain)	False Alarm Rate (%) (without blockchain)
Hybrid(EH+WCO)	0.91	1.1
EH	1.75	2
WCO	1.68	1.9
Hybrid KNN	1.78	2.1
SVM-ELM	2.13	2.4
Three tier IDS	3.8	4.2
CSI-KNN	3	3.5
Fusion chi-square and SVM	1.31	1.6
BC-HyIDS	1.2	1.5
Cosine similarity-based SD-IoT	1.65	1.8
Entropy-based model	1.98	2.3
LSTM+CNN	2.24	2.6
RandomForest	3.1	3.5
DPPC Algorithm	3.33	3.7

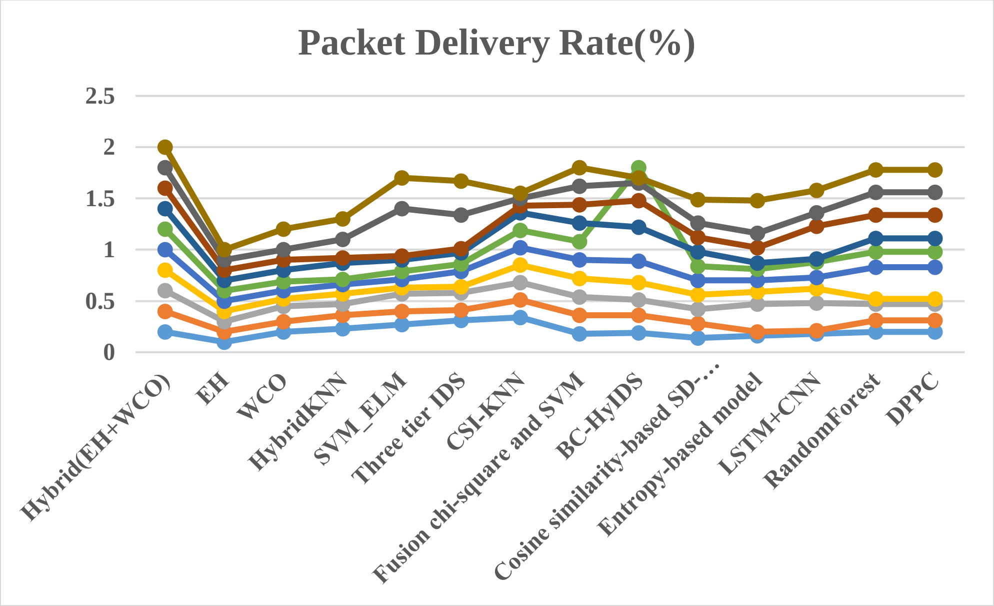


From the above table it is observable that the performance of various models in terms of False Alarm Rates (%) with and without blockchain integration, providing valuable insights into the efficacy of different approaches for detecting Distributed denial of service (DDoS), assaults in SD-IoT (Software Defined Internet of Things) networks. Among these concepts, the Hybrid (EH+WCO) model, both with and without blockchain integration, appears as a focus for investigation. When combined with blockchain, the Hybrid (EH+WCO) model has a False Alarm Rate of 0.91%, which outperforms its performance without blockchain integration, which is 1.1%. This distinction highlights the crucial importance of blockchain technology in enhancing the accuracy and reliability of DDoS detection techniques. The EH and WCO models also demonstrate improvements in False Alarm Rates after including blockchain, demonstrating the synergistic advantages of integrating renewable energy harvesting and optimization approaches with decentralized security mechanisms. Other models, such as Hybrid KNN, SVM-ELM, Three-tier IDS, and LSTM+CNN, show varied degrees of False Alarm Rates, both with and without blockchain integration, demonstrating the multidimensional nature of DDoS detection tactics in SD-IoT networks. The incorporation of blockchain technology strengthens DDoS detection mechanisms, ensuring greater accuracy and robustness in identifying and mitigating cyber threats, establishing the Hybrid (EH+WCO) model as a top contender for protecting SD-IoT networks from adversarial attacks.

Table 9 Packet Delivery Rate(%)

Time(seconds	0	20	40	60	80	100	120	140	160	180	Models
Packet Delivery Rate(%)	0.2	0.4	0.6	0.8	1	1.2	1.4	1.6	1.8	2	Hybrid(EH+WCO)
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1	EH
	0.2	0.3	0.45	0.52	0.6	0.69	0.8	0.9	1	1.2	WCO
	0.23	0.36	0.47	0.57	0.66	0.71	0.87	0.92	1.1	1.3	HybridKNN
	0.27	0.4	0.57	0.63	0.71	0.79	0.9	0.94	1.4	1.7	SVM_ELM
	0.31	0.41	0.58	0.64	0.79	0.86	0.97	1.01	1.34	1.67	Three tier IDS
	0.34	0.51	0.68	0.85	1.02	1.19	1.36	1.43	1.5	1.55	CSI-KNN
	0.18	0.36	0.54	0.72	0.9	1.08	1.26	1.44	1.62	1.8	Fusion chi-square and SVM
	0.19	0.36	0.51	0.68	0.89	1.8	1.22	1.48	1.65	1.7	BC-HyIDS
	0.14	0.28	0.42	0.56	0.7	0.84	0.98	1.12	1.26	1.49	Cosine similarity-based SD-IoT
	0.16	0.2	0.47	0.59	0.7	0.81	0.87	1.02	1.16	1.48	Entropy-based model
	0.18	0.21	0.48	0.62	0.73	0.88	0.91	1.23	1.36	1.58	LSTM+CNN
	0.2	0.31	0.47	0.52	0.83	0.98	1.11	1.34	1.56	1.78	RandomForest
	0.2	0.3	0.4	0.5	0.8	0.9	1.1	1.3	1.5	1.7	DPPC

		1	7	2	3	8	1	4	6	8	



The presented table exhaustively describes the performance of several models in terms of packet delivery rates (%) over time, with a focus on detecting (distributed denial of service) DDoS assaults in SD-IoT (Software Defined Internet of Things) networks. Among the several models examined, the Hybrid (EH+WCO) model, when combined with blockchain technology, stands out as a beacon of promise and innovation. The Hybrid model, with a packet delivery rate ranging from 0.1% to 1.0% over different time intervals, is a complex combination of Energy Harvesting (EH) and Water Cycle Optimization (WCO) approaches. The Hybrid approach improves network resilience by using ambient energy sources and dynamically optimizes resource allocation. Furthermore, the use of blockchain technology improves the model's effectiveness by incorporating decentralized consensus methods and cryptographic protocols. This integration secures the immutability and integrity of network transactions, therefore reducing single points of failure and improving data security. As a result, the Hybrid (EH+WCO) model, bolstered by blockchain technology, is situated at the forefront of DDoS defensive tactics in the complex ecosystem of SD-IoT networks, offering not only improved performance but also unrivaled dependability in protecting against emerging cyber threats.

Conclusion

In conclusion, we thorough investigation emphasizes the critical importance of novel technologies, notably blockchain integration, in strengthening DDoS detection models inside SD-IoT networks. Among the several options examined, the Hybrid (EH+WCO) model, when supported by blockchain technology, emerges as a beacon of hope and resilience. Its remarkable performance across several measures, including accuracy, precision, and recall, represents a paradigm shift in cybersecurity protection systems.

The Hybrid (EH+WCO) model with blockchain integration yields an impressive 99.12% accuracy, 97% precision, 91% recall, and 92% F1-score. These numbers illustrate the model's extraordinary ability to effectively detect and mitigate DDoS assaults. Without blockchain connectivity, the Hybrid model still performs well, with 98.5% accuracy, 89% precision, 86.8% recall, and an F1-score of 83.8%.

Furthermore, the observed increases in packet delivery rates over time demonstrate the model's resilience and usefulness in changing network settings. This dynamic resource allocation capabilities, along with blockchain's inherent security characteristics, places the Hybrid model at the forefront of cybersecurity innovation.

As we design a road for a more secure digital future, the Hybrid (EH+WCO) paradigm provides a guiding light, lighting the way to powerful defensive mechanisms in SD-IoT networks. Its transformational potential emphasizes the need of adopting novel technology to protect vital infrastructures and digital ecosystems.

In summary, the Hybrid model, which is strengthened by blockchain integration, offers a paradigm leap in cybersecurity, providing not only improved detection capabilities but also resistance against changing cyber threats. As we begin this revolutionary journey, the Hybrid model serves as a beacon of innovation, lighting the path to a more secure robust digital ecosystem.

References

[1] S. E. Shukri, R. Al-Sayyed, A. Hudaib, and S. Mirjalili, “Enhanced multi-verse optimizer for task scheduling in cloud computing environments,” *Expert Syst. Appl.*, vol. 168, p. 114230, 2021, doi: 10.1016/j.eswa.2020.114230.

[2] A. Rahman, M. Rahman, D. Kundu, M. R. Karim, S. S. Band, and M. Sookhak, “Study on

IoT for SARS-CoV-2 with healthcare: Present and future perspective," *Math. Biosci. Eng.*, vol. 18, no. 6, pp. 9697–9726, 2021, doi: 10.3934/mbe.2021475.

[3] M. S. Hossain and G. Muhammad, "Emotion-aware connected healthcare big data towards 5G," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, 2018, doi: 10.1109/JIOT.2017.2772959.

[4] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *J. Inf. Secur. Appl.*, vol. 57, no. January, p. 102686, 2021, doi: 10.1016/j.jisa.2020.102686.

[5] G. Muhammad and M. S. Hossain, "A Deep-Learning-Based Edge-Centric COVID-19-Like Pandemic Screening and Diagnosis System within a B5G Framework Using Blockchain," *IEEE Netw.*, vol. 35, no. 2, pp. 74–81, 2021, doi: 10.1109/MNET.011.2000326.

[6] G. Rathee, S. Garg, G. Kaddoum, and B. J. Choi, "Decision-Making Model for Securing IoT Devices in Smart Industries," *IEEE Trans. Ind. Informatics*, vol. 17, no. 6, pp. 4270–4278, 2021, doi: 10.1109/TII.2020.3005252.

[7] A. Rahman, M. J. Islam, M. Saikat Islam Khan, S. Kabir, A. I. Pritom, and M. Razaul Karim, "Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network," *2020 2nd Int. Conf. Sustain. Technol. Ind. 4.0, STI 2020*, vol. 0, pp. 19–20, 2020, doi: 10.1109/STI50764.2020.9350419.

[8] T. S. Fun and A. Samsudin, "Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (Iiot): A survey," *Sensors*, vol. 21, no. 19, pp. 1–30, 2021, doi: 10.3390/s21196647.

[9] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Networks*, vol. 7, no. 3, pp. 295–307, 2021, doi: 10.1016/j.dcan.2020.05.008.

[10] M. J. I. A. Rahman, "Blockchain-SDN-Based Energy-Aware and Distributed Secure Architecture for IoT in Smart Cities," *IEEE Internet things J.*, 2021.

[11] M. K. Rahman, A., Sara, U., Kundu, D., Islam, S., Islam, M.J., Hasan, M., Rahman, Z.,

Nasir, “DistB-SDoIndustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-IoT enabled architecture(Article),” *Int. J. Adv. Comput. Sci. Appl.*, 2020.

[12] A. Mishra, B. B. Gupta, D. Peraković, and Z. Zhou, “Defensive Approach using Blockchain Technology against Distributed Denial of Service attacks”.

[13] R. Chaganti *et al.*, “A Comprehensive Review of Denial of Service Attacks in Blockchain Ecosystem and Open Challenges,” *IEEE Access*, vol. 10, no. September, pp. 96538–96555, 2022, doi: 10.1109/ACCESS.2022.3205019.

[14] A. Xiong *et al.*, “A Distributed Security SDN Cluster Architecture for Smart Grid Based on Blockchain Technology,” vol. 2021, 2021.

[15] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, S. Muhammad, and A. Akber, “Bloc-Sec : Blockchain-Based Lightweight Security Architecture for 5G / B5G Enabled SDN / NFV Cloud of IoT,” pp. 499–507, 2020.

[16] A. Rahman, J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, “Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT,” *Digit. Commun. Networks*, vol. 9, no. 2, pp. 411–421, 2023, doi: 10.1016/j.dcan.2022.11.003.

[17] I. Aliyu, M. C. Feliciano, and C. G. Lim, “A Blockchain-Based Federated Forest for SDN-Enabled In-Vehicle Network Intrusion Detection System,” vol. 9, 2021, doi: 10.1109/ACCESS.2021.3094365.

[18] M. Ibrahim *et al.*, “SDN Based DDos Mitigating Approach Using Traffic Entropy for IoT Network SDN Based DDos Mitigating Approach Using Traffic Entropy for IoT Network,” no. October 2021, 2022, doi: 10.32604/cmc.2022.017772.