Stochastic Modelling and Computational Sciences

A DTOHE BASED INTRUSION DETECTION FOR CLOUD COMPUTING WITH BLOCKCHAIN TECHNOLOGY

Mrs. Jasmine Samraj[1] and Mrs. Abirami. K[2]
[1]Associate Professor, Research Supervisor, PG & Research Department of Computer Science Quaid-E-Millath Government College for Women (Autonomous),Chennai
[2]Research Scholar (Ph.D), PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (Autonomous), Chennai
[1]dr.jasminesamraj@qmgcw.edu.in and [2]abiramik.research@gmail.com

ABSTRACT
Network intrusion attacks are one of the major problem in the recent development of internet of things(IoT) enabled systems. Due to massive connection within various networks, malicious activities are keep on increasing. One of the challenging problems in the network are intrusion attacks and its obstruction of network flow. The presented system considers The serious issue of network abstraction in cybersecurity network and employed a blockchain enabled in tuition detection system. The primary goal of the system is to detect the intrusion attacks in the early stages. The presented approach considered distributed three based one hot encoding (DTOHE)technique for detection of intrusion attacks in the cloud platform using blockchain Technology. The Swarm intelligence model is employed in the same network in order to optimize the features of the data set. The presented approach consider UNSW-NB15 dataset. The proposed methodology utilized the security at the place of private and public key selection. The major constraints in the network in terms of malicious activity is suppressed, and detection of attack in the early stages is improving in the presented system. The overall performance in terms of accuracy is improved comparing with existing state of the art approaches. The presented approach achieved the accuracy of 91.3%, precision of 89% and recall value of 91%.

Keywords: Blockchain, Intrusion detection, Internet of Things, DTOHE, cloud security.

I. INTRODUCTION
A cloud computing platform is a web-based processing environment where applications, systems, facilities regulations, and numerous other services are practically offered on public servers [1]. It is represented as a user desire to lower total costs and level of complexity. Because of the many benefits of instant delivery of services, such as dynamic distribution of resources, improved resilience to failure, and greater flexibility, it is becoming becoming increasingly common. Virtualization solutions featuring the ability to self-service are used by a number of cloud service providers (CSPs), such as Google, Amazon, and Microsoft. The fundamental requirement of cloud-based computing is virtualization [2]. Regular increases in information are a result of a significant increase in technological advances in IT [3].

Hackers gained advantages from cloud computing since it generates massive amounts of data at speeds exceeding 665 Gb/s [4]. As it has become the focus of attackers, the cloud's massive amounts of data have emerged as its largest issue [5].

The cloud is attractive to hackers because of its open, dispersed structure and the volume of traffic it generates [6]. Attackers have the ability to obstruct user products and services, manipulate private information, and abuse the CSP's resources and amenities. An incursion is a threat which takes advantage of users' confidential are sensitive data are that uses up resources like CPU, the bandwidth, and memory. Firewalls and other conventional security measures are insufficient. However, a suitable system is required in order to give users protection.

By examining the network's data, an intrusion detection system (IDS) may discover are identify intrusions.

Host-based IDS and network-based IDS are the two primary categories of IDS depending on deployment methodologies. While network-based IDS examine the entire network, host-based IDS solely observes the host

computer system for potential threats. When using host-based IDS, each cloud node has their own IDS and memory. Since block chain technology received a lot of interest among researchers and sector, it has become more widely used recently. A common way to think of a blockchain is as an ongoing collection of documents called blocks which are connected by cryptographic hashes.

Blockchains Fig 1., which allow open and integrity-protected storage of information, are often maintained through a network of other people. This article explores the possibility of integrating blockchain technology along with systems to detect and prevent intrusions, which has been inspired by the flexibility of blockchain technology.

A header and a body are the two fundamental parts of each block in a blockchain, which is a linked data structure. A nonce, a prior hash, a Merkle root hash, a timestamp, and a difficulty goal make up the header part. A list of transactions can be found in the body part. A block chain's structure is seen in Fig. 1. All blocks are cryptographically connected to one another, the first block remains referred to as the "genesis," and blocks are dispersed across network nodes [16].

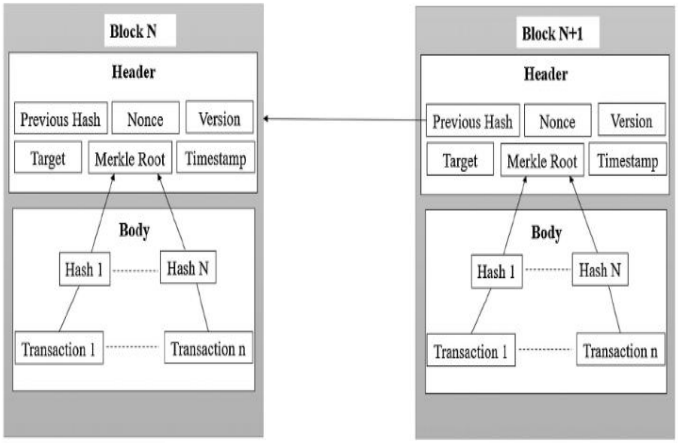

Fig1: Block chain structure

Additionally, every node in the block chain network must possess an identical block list, which is shown in Fig. 2, in order to abide by the principles of block chain technology. Every node in the network receives a broadcast whenever a new block is uploaded. A consensus process that validates a transaction in the block is used by every node for confirming the new block. Proof of work and proof of stake are two examples of consensus techniques that can be used to guarantee that all nodes possess the identical block list [17, 18].

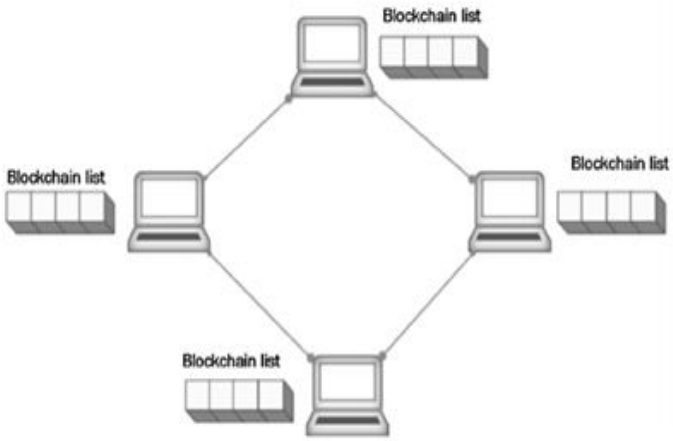

Fig 2: P2P network

- The proposed model is created with the goal of testing the presence of intrusion attacks in the early stages.
- The introduced approach thought about dispersed three based one hot encoding (DTOHE)technique for identification of interruption assaults in the cloud stage utilizing blockchain Innovation.
- The Multitude knowledge model is utilized in a similar organization to upgrade the highlights of the informational index.
- The introduced approach consider UNSW-NB15 dataset. The proposed technique used the security at the spot of private and public key choice.

The rest of the journal is framed as literature study in Section II. In this journal, dataset details are provided in Section III. System methods are explained in Section IV. Results are discussed in Section V. The journal is further concluded with future scope.

II. RELATED WORK

A. Ahmed et.al [7] The author presented a system where machine learning algorithms are utilized to detect the malware attacks on the internet of things(IoT) enabled systems full stop the presented approach detects the critical mitigation of Malware attacks through comparison of Logistic regression algorithm Gaussian Naive bayes(GNB), Decision tree(DT) algorithm, Random forest algorithm(RF),K-nearest neighbour(KNN) algorithm and extremely gradient boosting algorithm for network traffic oriented attack detection full stop heterogeneous dataset is implemented here to accurately extract the attack features and identify the unique feature patterns on malicious attacks.

A. Hekmati et al. [8] The author implemented artificial intelligence enabled cyber security network to check the security constants present in the network. In order to obtain high security to be enclosed in the cyber security network to protect the network from different distributed the nail of services attacks which are the common attacks in internet furistic attack malicious entities and sophisticated attacks propose to model with truncated crunchy distribution network is developed. For the presented system having a complex architecture and data privacy is enabled. Further, the exploration of system need to be included with different parameters and location on large scale.

H. Somaya et.al [9] The author presented of powerful machine learning algorithm to detect the intrusion attacks present in the network. The meta-heuristic parameters and tunable heuristic parameters are helpful to create a customized model for detecting the attacks. The paper presented with large scale IOT network unable to data set for procuring the boat neck attacks. The classification model is measured in terms of accuracy.

R. F. Hayat et.al [10] The Other presented distributor Daniel of services mitigation attack detection and protection system using blockchain network. The presented system considered device based verification mechanism using blockchain algorithm that excludes the malicious attacks in the large scale IOT network. The proposed Framework utilizes the blockchain benchmark available the performance of the network.

N. Agarwal et.al [11] The author present at the system in which vulnerable attacks are detected in the remote area network using secure future extraction technique. Distributed denial of services (DDoS) attacks have major drawback with the all arrival activity in large area network. Remote and Edge basis are highly impacted by The DDoS Attacks. The percentage system discuss on the significant problem of DDoS attack implemented here

Z. A. El Houda et.al [12] In the presented journal detection of intrusion attacks using explainable artificial intelligence tools are Explorer. Machine learning and deep learning algorithms are helpful to detect the real time attacks in our use in IoT models. Here, artificial intelligence tools are utilized for in-depth explanation of malware attacks and finally detect the cyber constraints present in the network using the pattern analysis method. The trust and transparency are considered as an important key features in the presented system.

M. Alsharif et.al [13] The author presented an internet of think enabled malicious cyberattack detection system where forget computing mechanism is developed. IoT devices reduce the delay cost by cloud computing environment and reduces the challenges present in the fog environment. The security in storage systems are reduced in the presented system

F. Khan et.al[14] The water presented a cybersecurity detection system using and simple approach. The presented approach considered long short term memory network where the decision tree algorithm classifies The attacks in Rio as normal system and attack oriented system as two categories. The presented approach deployed with infrastructure as service environment and provide a clarity on fog culture in the network cloud.

Y. Zhang et.al [15] The Other presented a system in which network intrusion detection attacks are analysed of the presented approach consider generalized adverse network model incorporated with the less lost function and high accurate constraints with a clean the labelled data and producers are correlated result with respect to the injected models. the presented approach explore a local training and testing architecture that detect the pattern of attack scenario in the early stages.

III .SYSTEM DESIGN

The proposed model is developed with UNSW-NB15 dataset.

Experimental results and analysis

Using the UNSW-NB15 dataset, performance indicators for the DTOHE classification have been assessed in this section. The performance is contrasted with cutting-edge techniques. The block chain model's output, that can be utilised to assess the effectiveness of an IDS, is shown in Fig. 4. The instances of a predicted class are represented by the confusion matrix's columns, whereas the actual class is specified in each row. UNSW-NB15 dataset:

Table 1. Sample dataset preview

id	duration	protocolo	service	sload	dload	sloss	dloss	spkt	ct_srv_sr c	ct_src_dpo rt_ltm	ct_dst_spor t_ltm	attack_cat
1	0.000011	udp	-	1.80E+08	0	0	0	0.011	2	1	1	Normal
2	0.000008	udp	-	8.81E+08	0	0	0	0.008	2	1	1	Normal
3	0.000005	udp	-	8.54E+08	0	0	0	0.005	3	1	1	Normal
4	0.000006	udp	-	6.00E+08	0	0	0	0.006	3	2	1	Normal
5	0.00001	udp	-	8.50E+08	0	0	0	0.01	3	2	1	Normal
6	0.000003	udp	-	1.05E+09	0	0	0	0.003	2	2	1	Normal
17	0.246422	tcp	http	41165.16	7272.08	2	1	24.4521	2	2	2	attack
18	0.819719	tcp	smtp	34890	17303.5	8	8	39.0342	1	1	1	attack
19	0.000008	sep	-	52000000	0	0	0	0.008	1	1	1	attack
20	0.53435	tcp	ftp-data	4775.896	21274.5	1	2	76.3357	1	1	1	attack

Table 1: shows the sample dataset contents.

IV. METHODOLOGY

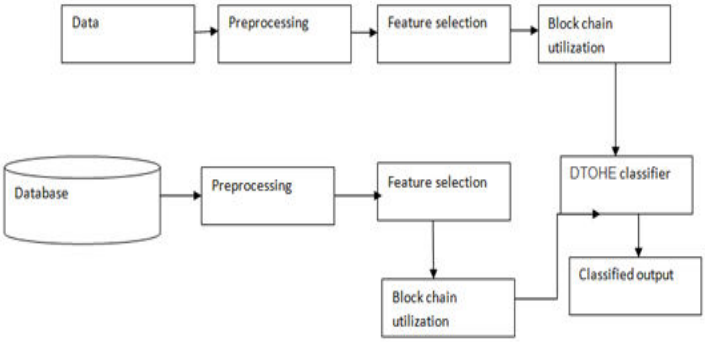

Fig 3: System architecture of proposed DTOHE model

In the present research, researchers offer a unique DTOHE-based intrusion detection system with five modules to address the aforementioned issues: initial processing, blockchain, database, choosing characteristics, and categorization. The swarm intelligence algorithm reduces the previously processed information to produce a lower-dimensional reconstruction characteristic, and the classified result is produced by the categorization module. The database of the database module, also known as the feature library, contains the packed features associated with every traffic. The classification module can get testing and updating from this library.

Data privacy, reliability, and accessibility (CIA) in the cloud are under threat from growing security concerns. Ransomware, DDoS, and DoS assaults are just a few of the many malware, spyware, and Man-in-the-middle (MITM) threats that cloud-based IoT systems must contend with. To enable comprehensive recognition of attacks and rejection on these networks which interact 24 hours a day via the internet, an extremely efficient while smart ML model is needed. Fig. 3 depicts the structure of the framework employed in this study. In order to defend against network assaults in a cloud context, an improved DTOHE machine learning model that utilises tree topology is created. The database including IoT-based network intrusions is chosen from the datasets already collected during the first round of data collecting.

A. Data Preprocessing

The datasets are cleared of any incorrect are missing values for data during the course of the data pretreatment procedure. The datasets were examined for instances with insufficient are incorrect values, such as nan, inf, +inf, etc. Because the dataset was so huge, these samples were eliminated. Additionally, several of the features which possess values that remain constant and don't participate in the training's ML learning process is found out. Such features are not necessary because they will just increase operating expenses and computational requirements. Protocol, response_body_len, spkts, ct_flw_http_mthd, trans_depth, dwin, ct_ftp_cmd, and is_ftp_login are some of these features. Flags were taken down. Particle swarm optimisation (PSO) was used to pick features in order to verify that this strategy was effective.

B. Feature Selection

Feature Selection Using PSO: A feature selection methodology is a method for selecting a particular category of attributes that is detailed, brief, and realistic. In this study, a correlation-based feature selection (CFS) approach which employs data acquisition and volatility to evaluate the value of features is chosen. A particle swarm optimisation (PSO) algorithm is also used as a search method concurrently. A feature set is modelled as a group of particles that form up a swarm in a particle swarm optimisation (PSO)-based feature selection approach. Each of the numerous particles that are dispersed across a hyperspace is assigned a position ξn and a velocity υn, both of which are completely arbitrary. Assume that w stands for the inertia weight constant and that $\delta 1$ and $\delta 2$ stand for the intellectual and interpersonal learning constants, correspondingly. The next step is to define $\sigma 1$ and $\sigma 2$ as the random numbers, ln as particle n's personal best position, and g as the overall location of all the particles. Thus, the fundamental guidelines for upgrading each particle's position and velocity are as follows:

$$\xi n(t + 1) = \xi n(t) + \upsilon n(t + 1) \quad (1)$$

$$\upsilon n(t + 1) = w\upsilon n(t) + \delta 1\sigma 1(ln - \xi n(t)) + \delta 2\sigma 2(g - \xi n(t)) \quad (2)$$

C. Blockchain Module

A blockchain's purpose is to provide a cryptographically safe method to acquire a block—a chronologically ordered list of records—that is both openly observable and unchangeable. Blockchains are utilised as a public, global information about transactions since they are usually distributed and synchronised throughout a network of peer-to-peer connections [19]. Every member of the blockchain network can examine the stored data and accept are verify it based on a consensus algorithm. The sequence in which entries were verified determines how they are put to the blockchain after they have been accepted. A blockchain is a collection of blocks, each of which has a transaction history recorded in it. The blockhead contains the metadata, and the block body contains the records of the transactions.

An new strategy for exchanging signatures in the distributed IDS environment is provided in the suggested architecture. For identifying attacks and network security enhancement, the suggested structure combines both signature-based and anomaly-based detection techniques. According to our understanding, the usage of a blockchain in distributed IDS for signature exchange would be a first. This paradigm is suggested for a distributed setting in which every node is interconnected in a distributed manner. By examining packets that are arriving over the network, every node will have the ability to able to spot threats. Every time a packet reaches a node, it is intercepted and subject to a signature-based detection phase that looks for harmful patterns. This stage involves training the suggested classifier with the current UNSW-NB15 dataset.

D. Classification

The dataset's categorization into attack and normal packets is crucial for ensuring the safety of the cloud computing infrastructure. There are two types of classification: binary classification and multiclass classification. Two classes are produced via binary categorization. More than two classes are produced via multiclass classification. The classification of multiple classes has been done. One hot encoding technique involves transforming category information into a binary matrix form, that can help machine learning algorithms make better forecasts. One hot encoding is the lawful pairing of a single high bit and all subsequent low bits in digital circuits and machine learning. A 32-bit IP address was encoded completely when one hot encoding was used.

A categorical value reflecting a numerical value in the database was thought of as the 32-bit IP address. The 1 through N-1 categories were used to represent the 32-bit IP address.

A binary vector called a one-hot encoding-based vector puts one value of the relevant index of labelled data to 1 and sets the remaining values to 0. As a result, learning outcomes from a tree model using labelled data as numbers can be expressed as decimal points. If that's the case, categorical data can't be categorised precisely. Categorical data can be accurately identified, though, if a one-hot encoding-based vector is used. Nodes, leaves, and edges make up a tree's three basic structural elements. An attribute that will be used to split the data is labelled on each node. Every node contains a variety of edges that are labelled in accordance with the attribute's potential values. Either two nodes are a node and a leaf are connected by an edge. A decision value is assigned to each leaf to help with data sorting. Starting at the root node, following the tree's branches down until you get to a leaf node that corresponds to the class in order to make a decision using a tree. Each tree stands in for a set of rules that classify data based on the characteristics of the dataset. Below is a list of the tree model that is utilised with one hot encoder.

When there is only one class of data in a set, there does not exist uncertainty, and the entropy is zero. Determining which class each element in the final subset belongs to is the goal of decision tree classification, which involves repeatedly dividing the input data set into subsets. In equation (3), the entropy calculation is displayed. For the various classes in the data collection, given probability p1, p2,.., ps

$$Entropy: H(p1,p2,...ps) = \sum_{i=1}^{s}(p_i \log(l / p_i)) \quad (3)$$

$$Gain\ (D,S) = H(D) - \sum_{i=1}^{s} p(D_i)H(D_i)$$

When given a data set, the function D, H(D) calculates the entropy in the data set's class-based subsets. The entropy of those subsets can be examined once more when the subset is divided into s new subsets S = D1, D2,...,Ds using some characteristic. If every example in a subset of a data set is from the same class, the subset is fully sorted and requires no further division. Equation (4) is used by the algorithm to determine the information gain of a split, and it then selects the split that offers the greatest information gain.

(4) The greatest gain ratio in equation (5) for splitting purposes, which guarantees a greater than average information gain.

$$GainRation(D,S) = \frac{Gain(D,S)}{H\left(\frac{|D_1|}{D},...,\frac{|D_s|}{D}\right)}$$

(5) A binary tree is created by the CART (Classification and Regression Trees) technique, which is used for decision-making processes.CART has a pruning method and manages data that is absent. To determine the ideal split, the SPRINT (Scalable Parallelizable Induction of Decision Trees) technique uses an impurity function called the gini index.

$$gini\ (D) = 1 - \sum p_j^2 \qquad (6)$$

Where pj is the likelihood that class Cj will appear in data set D. Assume that D is partitioned into the subsets D1 and D2, and that

$$gini_{split}(D) = n_1/n(gini(D_1)) + n_2/n(gini(D_2)) \qquad (7)$$

V.RESULTS AND DISCUSSIONS

```
Data 1: Genesis Block - 0
Hash 1: 39331a6a2ea1cf31a5014b2a7c9e8dfad82df0b0666e81ce04cf8173cc5aed3e

Data 2: [ 2.81289512  0.         -0.11529863 -0.49572946  2.23701294 -1.1419013
 -0.12650796  0.          0.          0.          -0.55437317
  0.02786755  1.4648859   0.          1.         -0.07380882  0.
  0.         -0.38995059  0.         -0.57672574  1.56000198 -0.28704658
 -0.06321168  1.09245621  0.          1.          0.         -0.42213385
 -0.04473913  1.94760172  1.64405295 -0.31871085 -0.26756332 -0.04613531
 -0.59554257  0.         -0.64501291  1.          0.        ] - 39331a6a2ea1cf31
a5014b2a7c9e8dfad82df0b0666e81ce04cf8173cc5aed3e
Hash 2: 54434b84f7e7e326cac8b27deb388a717d507a1fbf2f8e8d5715bb6d7d37ce8e

Data 1: Genesis Block - 0
Hash 1: 39331a6a2ea1cf31a5014b2a7c9e8dfad82df0b0666e81ce04cf8173cc5aed3e

Data 2: [ 1.08745728  0.         -0.12795972 -0.58914985  0.95452779 -1.1419013
 -0.12650796  0.          0.          0.          -0.55437317
 -0.05746556  0.73034097  0.          1.         -0.01253652  0.
  0.         -0.38990818  0.         -0.57653581  1.56000198 -0.22841756
 -0.02693312  1.09245621  0.          1.          0.         -0.35673914
 -0.04473913  1.9378633   0.70804603 -0.31871085 -0.20096582 -0.04547156
 -0.47537148  0.         -0.52082715  1.          0.        ] - 39331a6a2ea1cf31
a5014b2a7c9e8dfad82df0b0666e81ce04cf8173cc5aed3e
Hash 2: 5095081eca2ea8671d942ecde4411045834142657ba8541d1fd1e5fb14ec860c
```

Fig 4: Simulation result of DTOHE Model

Fig 4. Shows the simulation result of proposed DTOHE model on attack detection.

A. Evaluation metrics

Accuracy: Performance metrics are crucial to validate the results in terms of intrusion attacks present with the analysis. Accuracy is considered as the amount of truly positive terms present with respect to the overall data. Accuracy is calculated as

Accuracy = (TP + TN) / (TP + TN + FP + FN) (8)

Precision: The quality of detection model is evaluated using the precision defines as the ratio of truly classified attack patterns with respect to the positive occurrences.

Precision =TP / (TP + FP) (9)

Recall: The recall value act as the important parametric measurement calculated with ration of positively classified value with total of positive occurrence and negative occurrence.

Recall = TP/ (TP +FN) (10)

F1Score: the measure of relative composition of precision and recall scores and defines as the formula below.

F1Score = 2*(Precision*Recall)/(Precision+Recall) (11)

Table 2: Confusion matrix for Training process

Class	0	1
0	4261	67
1	45	45627

Table 2. Shows the confusion matrix of proposed model on intrusion attack detection during training process.

Table 3: Confusion matrix for Testing process

Class	0	1
0	3616	21
1	47	16316

Table 3. Shows the confusion matrix of proposed model during testing process. Confusion matrix is helpful to drive the number of vulnerable activity present within the network. The correctly classified values shows the presence of attack scenario in the network, true positive and false negative enable such conditions. Further the presence of false positive and true negative rate determines the occupancy of non-malicious attacks in the network.

Table 4: Performance measure of proposed model

Metrics	Training data	Testing data
Accuracy	91.3	81.6
Precision	89	73
Recall	91	82
F-score	87	74

Table 4. Shows the performance measure of proposed model. Through UNSWNB dataset.

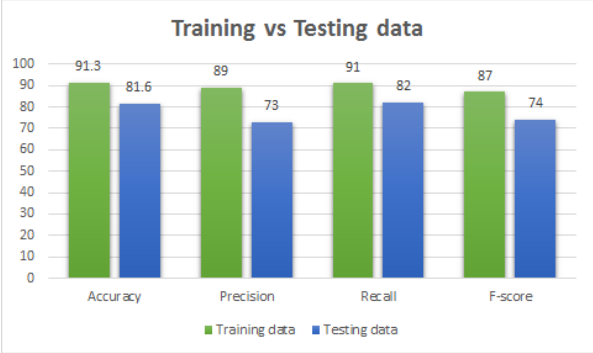

Fig 5: Comparison of Training vs. Testing data

Fig 5: Shows the comparison of Training vs. testing data.

Metrics	Proposed method	RESNET[20]	RNN [21]	DT[22]
Accuracy	91.3	88	81.15	81.26
Precision	89	88	81.81	80.36
Recall	91	86	99.63	75.08

Fig 6: Comparison of existing system and proposed DTOHE model

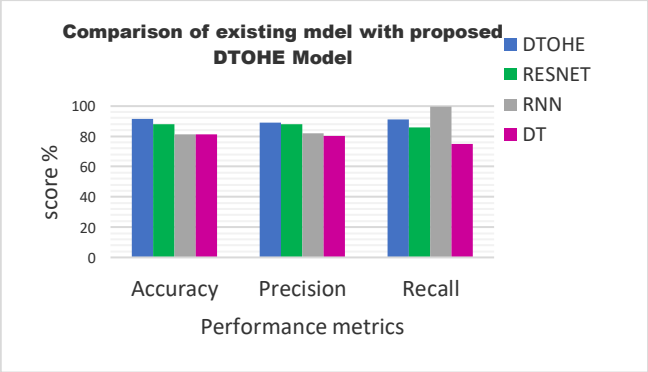

Fig 6. Shows the comparison of existing system and proposed DTOHE model in terms of accuracy, Precision and Recall. Through RESNET[20] 88% accuracy is achieved, 88% precision and 86% Recall is achieved. Further using existing model of RNN[21] employed with 81.15% accuracy, 81.81% precision and 99.63% Recall value. DT [22] model achieved with 81.26% accuracy, 80.36% precision and 75.08% Recall value. The proposed DTOHE model achieved 91.3% accuracy, 89% precision and 91% Recall.

VI. CONCLUSION

Network interruption assaults are one of the serious issue in the new advancement of web of things (IoT) empowered frameworks. Because of huge association inside different organizations, vindictive exercises are continue to increment. One of the difficult issues in the organization are interruption assaults and its hindrance of organization stream. The introduced framework considers the difficult issue of organization deliberation in online protection organization and utilized a blockchain empowered in educational cost discovery framework. The essential objective of the framework is to identify the interruption assaults in the beginning phases. The introduced approach thought about dispersed three based one hot encoding (DTOHE) technique for identification of interruption assaults in the cloud stage utilizing blockchain Innovation. The Multitude knowledge model is utilized in a similar organization to streamline the elements of the informational index. The introduced approach consider UNSW-NB15 dataset. The proposed technique used the security at the spot of private and public key choice. The significant imperatives in the organization as far as malevolent movement is smothered, and identification of assault in the beginning phases is working on in the introduced framework. The general presentation as far as precision is further developed contrasting and existing best in class draws near. The introduced approach accomplished the exactness of 91.3%, accuracy of 89% and review worth of 91%.

REFERENCES

[1] O. Alkadi, N. Moustafa, and B. Turnbull, “A review of intrusion detection and blockchain applications in the cloud:approaches, challenges and solutions,” IEEE Access, vol. 8,Article ID 104893, 2020.

[2] S. Prakash, “Role of virtualization techniques in cloudcomputing environment,” in Advances in Computer Communication and Computational Sciences Springer, Singapore,2019.

[3] M. Rana and J. Singla, “A systematic review on data mining rules generation optimizing via genetic algorithm,” in Proceedingsof the International Conference on Innovative Computing &Communications (ICICC), 2020.

[4] M. Idhammad, K. Afdel, and M. Belouch, “Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest,” Security and Communication Networks, vol. 2018, Article ID 1263123,13 pages, 2018.

[5] P. S. Bawa, S. U. Rehman, and S. Manickam, “Enhanced mechanism to detect and mitigate economic denial of sustainability (EDoS) attack in cloud computing environments,”International Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp. 51–58, 2017.

[6] S. Rajagopal and P. P. Kundapur, “Towards effective networkintrusion detection: from concept to creation on Azure cloud,” IEEE Access, vol. 9, Article ID 19723, 2021

[7] A. Ahmed and C. Tjortjis, "Machine Learning based IoT-BotNet Attack Detection Using Real-time Heterogeneous Data," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022, pp. 1-6, doi: 10.1109/ICECET55527.2022.9872817.

[8] A. Hekmati, E. Grippo and B. Krishnamachari, "Neural Networks for DDoS Attack Detection using an Enhanced Urban IoT Dataset," 2022 International Conference on Computer Communications and Networks (ICCCN), 2022, pp. 1-8, doi: 10.1109/ICCCN54977.2022.9868942.

[9] H. Somaya and M. Tomader, "Tuning the hyperparameters for supervised machine learning classification, to optimize detection of IoT Botnet," 2022 11th International Symposium on Signal, Image, Video and Communications (ISIVC), 2022, pp. 1-6, doi: 10.1109/ISIVC54825.2022.9800742.

[10] R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava and J. C. -W. Lin, "ML-DDoS: A Blockchain-Based Multilevel DDoS Mitigation Mechanism for IoT Environments," in IEEE Transactions on Engineering Management, doi: 10.1109/TEM.2022.3170519.

[11] N. Agarwal, A. Q. Md, V. T, P. K and A. K. Sivaraman, "A Robust Pipeline Approach for DDoS Classification using Machine Learning," 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), 2022, pp. 1621-1627, doi: 10.1109/ICICICT54557.2022.9917596.

[12] Z. A. El Houda, B. Brik and S. -M. Senouci, "A Novel IoT-Based Explainable Deep Learning Framework for Intrusion Detection Systems," in IEEE Internet of Things Magazine, vol. 5, no. 2, pp. 20-23, June 2022, doi: 10.1109/IOTM.005.2200028.

[13] M. Alsharif and D. B. Rawat, "Machine Learning Enabled Intrusion Detection for Edge Devices in the Internet of Things," 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2023, pp. 0361-0367, doi: 10.1109/CCWC57344.2023.10099276.

[14] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah and A. u. Rehman, "A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2022.3231424.

[15] Y. Zhang, Y. Zhang, Z. Zhang, H. Bai, T. Zhong and M. Song, "Evaluation of data poisoning attacks on federated learning-based network intrusion detection system," 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Hainan, China, 2022, pp. 2235-2242, doi: 10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00330.

[16] W. Gao, W. G. Hatcher and W. Yu, “A survey of Blockchain: techniques, applications, and challenges,”in 2018 27th Int. Conf. on Computer Communication and Networks (ICCCN), pp. 1–11, 2018.

[17] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat et al., “Provchain: A Blockchain-based data provenancearchitecture in cloud environment with enhanced privacy and availability,”in Proc. of the 17th IEEE/ACM Int.sym. on cluster, cloud and grid computing, pp. 468–477, 2017.

[18] M. Muzammal, Q. Qu and B. Nasrulin, "Renovating Blockchain with distributed databases: An open-source system,"Future Generation Computer Systems, vol. 90, no. Supplement C, pp. 105–117, 2019

[19] Bernabe, Jorge Bernal, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. "Privacy-preserving solutions for blockchain: Review and challenges." IEEE Access 7 (2019): 164908-164940.

[20] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, ''A deep learning approach to network intrusion detection,'' IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018.

[21] Y. Fu, F. Lou, F. Meng, Z. Tian, H. Zhang, and F. Jiang, ''An intelligent network attack detection method based on RNN,'' in Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC), Jun. 2018, pp. 483–489.

[22] Bahzad Taha Jijo and Adnan Mohsin Abdulazeez "Classification Based on Decision Tree Algorithm for Machine Learning ",Journal of Applied Science and Technology Trends Vol. 02, No. 01, pp. 20 – 28 (2021)https:// doi: 10.38094/jastt20165.