**Journal of Intelligent Systems and Internet of Things**
**Vol. 09, No. 02, PP. 78-92, 2023**
**DOI:** https://doi.org/10.54216/JISIoT.090206

# Anomaly Detection in Complex Power Grid using Organic Combination of Various Deep Learning (OC-VDL)

**Tamarah Alaa Diame[1,*], Kadim A. Jabbar[2], Ahmed Taha[3], Naseer Ali Hussien[4], Sura Rahim Alatba[5], Mohammed Nasser Al-Mhiqani[6], Venkatesan Rajinikanth[7]**

[1]Technical Computer Engineering Department, Al-Kunooze University College,Basrah, Iraq
[2]Department of Computer Engineering techniques,National University of science and technology, Thi Qar, Iraq
[3]Medical instruments engineering techniques, Al-farahidi University, Baghdad, Iraq:
[4]Information and Communication Technology Research Group, Scientific Research Center, Al-Ayen University, Thi-Qar, Iraq
[5]Computer Technologies Engineering, Al-Turath University College, Baghdad, Iraq
[6] Keele University (KU), Keele, United Kingdom, Staffordshire, ST5 5AA
[7]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India

Emails: Tamarah.Alaa@kunoozu.edu.iq; kadim.jabber@nust.edu.iq; Ahmedtaha@uoalfarahidi.edu.iq; naseerali@alayen.edu.iq; sura.raheem@turath.edu.iq; Almohaiqny@gmail.com; v.rajinikanth@ieee.org
[*]Corresponding Author: Tamarah.Alaa@kunoozu.edu.iq

**Abstract**

The development of power industries creates impacts on the intelligent power grids. The power grids are more valuable for transmitting information over the network. Several intermediate activities influence the networks, which are interrupted by traffic, creating network security issues. Therefore, the threats highly influence power grids, and the number of attacks also increased gradually. Several conceptual approaches are introduced to overcome the security issues; however, computation complexity is still a significant problem while detecting network anomalies. This research problem is overcome by applying the Organic Combination of Various Deep Learning (OC-VDL) approach. The introduced method observes the industry standards with the help of the Innovative Blockchain Network (IBN). During this process, IBN observes the infrastructure using the communication protocol and Manufacturing Internet of Things (IoT). The collected information is processed with the help of the Intense Autoencoder Classifier Model (IACM), which manages bilateral traffic control and helps predict abnormal activities. The effective prediction of network traffic minimizes the intermediate activities and improves the overall security up to 98.8% accuracy.

**Received: February 22, 2023 Revised: May 21, 2023 Accepted: September 03, 2023**

**Keywords:** Power grids; Network Anomaly Detection; Deep Model; Intense Autoencoder Classifier Model .

## 1. Introduction

A network anomaly is a rapid and brief change in the network's typical behaviour [1]. Detection of unusual events, observations, or things that differ substantially from the norm is known as anomaly detection [2]. There are very few instances in which data shows an anomaly. Anomalies in data have distinct characteristics from regular occurrences [3]. Some hostile intruders purposefully produce anomalies like a denial-of-service assault on an IP address. Some are accidents like an overpass collapsing in the middle of a busy road network [4]. As the name implies, outlier analysis (or anomaly identification) is the process of looking for patterns in a dataset that deviates from the norm [5]. For example, a change in customer behaviour may indicate anomalous statistics. When a single data point differs significantly from the rest of the data, it is considered abnormal [6]. Identifying

fraudulent activity based on the "amount spent" illustrates this concept. Cooperative and real-time communication are key features of Cyber-Physical Systems (CPS) [6]. This is done internally and through external organizational services [7]. The system's architecture should ensure that permission relationships between contexts and trust implementations are incorporated to maintain that the concept of working based on minimal access is guaranteed [8]. Authorization means are burdensome for users, error-prone, and hinder the advancement of applications in secure environments. It should be considered [9]; hence, this design makes it possible to build a secure cloud platform for managing and completing necessary infrastructure transaction processing without requiring a single central authority to get involved [10]. As a result, extensive research has focused on creating automated Anomaly Detection (AD) systems to automatically detect abnormal patterns in the data [11].

### 1.1 Active learning (AL)

An active learning (AL) approach allows full advantage of guided learning models while reducing the time and effort required for human expert labeling [12]. For the AL challenge, different research groups have used and tested different data sets, including writing recognition and voice recognition, document classification, and protein engineering [13]. Nevertheless, AL had a worse start-up performance. It was quicker and smoother in stage 2 when a more significant number of labeled instances were available to reach high accuracy levels [14].To train their algorithms, managed machine learning models currently use a set of fully labeled data, which explains why this approach is popular [15]. Machine learning algorithms for automatic anomaly detection can't be widely adopted since labeling data is time-consuming [16]. Using Artificial technology (AI), an unsupervised anomaly detection approach was demonstrated on experimental and simulated data sets, including photos, thyroid medical data, and data identifying arrhythmia disorders [17]. Handwritten text recognition was a success with AL. Using an AL system with noisy data, some researchers look for anomalies of particular interest [18]. The approach has been tried in various domains and scales, including data from the spaceship technologist, abalone biology data, and extraordinarily high information [19].AL may be more difficult due to the imbalanced nature of the entire data set, with anomalies seldom appearing (0.1–10%) [20].

Furthermore, no research has been done to date on the effectiveness of AL in ecological AD applications. Environmental data differs from other types of data. It faces unique challenges, such as (a) seasonal variation at the annual, quarterly, weekend, sensor drift, semi, quasi, and complex nonlinear dynamics, which all play a role in the system's nonlinear dynamics [21]. However, no research has been done to back up these claims.

### 1.2 Deep learning

Secondary and primary data are both used in deep learning for training. Deep learning applications in the real world include voice assistants, sight for automated vehicles, money laundering, and face recognition, to name a few examples. In which deep learning is included, machine learning can be considered a subset [22]. It's a branch of computer science focusing on self-improvement through studying computer algorithms. Deep learning employs artificial neural networks to mimic the way people think and learn instead of machine learning's use of more straightforward concepts. Future studies should consider AL's integration with models that explicitly address temporal dynamics [23]. Recurrent neural networks and long short-term memory networks are examples of deep learning models. In machine learning, deep learning refers to algorithms that use multi-layered structural structures to learn. As a result of abstractions, intermediary representations, and feedback linkages, these networks can capture various operating levels while matching input data with desired network response times. This network's units each perform a conversion from one level of representation to another. Low-level characteristics tend to classify inputs, whereas features of a high level are broader and largely unmodified. It is to learn how to build proper intermediate representations and successfully provide their final estimations, artificial systems that imitate these functions are built [24].

### 1.3 Anamoly Detection

Anomaly detection technology is a critical part of the infrastructure for protecting the network from cyberattacks. In-depth network data analysis and deployment techniques for security solutions to safeguard computer systems' integrity, confidentiality, and dependability are all possible with this software. A significant percentage of network traffic data comprises various elements that are not unnecessary, hence significantly degrading detection accuracy in a cloud setting [25]. Any deviation from the typical behaviour of a dataset is detected using anomaly detection. This data mining stage discovers anomalous data points, events, or observations [26]. For example, a change in customer behaviour may indicate anomalous statistics. Anomaly detection is increasingly being automated using machine learning. A malware anomaly detection system is a network security component that monitors network and framework activity for malicious movements.

Inconsistency detection in malware shows how commonly used software detects attacks by looking for failure impacts [27].

The significant contributions of this paper are:

1) An unique optimization technique based on the organic combination of various deep learning methods [OC-VDL] is needed to compete with the randomness of determination to overcome the threat and current security systems.

2) The introduction of Innovative Blockchain Network IBN architecture adheres to the industry standard; communication between the Industrial Internet of Things (IoT) modules will be safe.

3) The proposed smart contracts would use a qualified Intense Autoencoder Classifier Model (IACM) to establish a mutual traffic control agreement to identify quickly. Building a distributed platform that regulates and completes infrastructure transactions is important without partnering with a single central authority in this design.

Section 2 of the study included the remaining findings dealing with background study, analysis, and review of the existing models in the technology. The proposed concept of organic combination of various deep learning (OC-VDL) is illustrated in section 3; the result analysis is done by graphical representation specified in section 4. The conclusion and discussion are described in section 5.

**2. Background study**

Intelligent power network systems are the latest craze in power development, as traditional manual control methods have failed to satisfy the demands of power systems. Even though many systems are under the invention, the research practically enhances the existing scenarios.

Demertzis. et al. [28] proposed that the blockchain is an encoded, distributed archiving system to create unambiguously linked real-time log files. As a result, transactions are safe and transparent. A new approach to BlockchainSecurity Architecture (BCSA) is first introduced in this study. Industry 4.0 defines an industrial Internet - Of - Things (IIoT) network design that strives to ensure communication between traded devices and smart contracts built on deep learning.

Russo. et al. [29] phrased that natural anomaly detection in environmental monitoring is becoming increasingly important due to the growing amount of information collected from in-place sensors. The ineffectiveness of labeling data has made it difficult to use a machine learning approach for automated anomaly detection. A fully labeled training data set must be provided for today's supervised machine learning models (SML). This technique involves asking a specialist for the tags of a portion of the total data set rather than the entire set itself. This moment demonstrates that labeling takes less time and costs less money while still delivering similar or slightly similar anomaly detection capabilities as the previous method. Our findings suggest machine learning models with a variational classification boundary for environmental anomaly detection.

Hou. et al.[30] Identify personnel and detect smoke in the functional area of strength IoT equipment by suggesting a deep learning-based anomaly detection algorithm (DL- ADA). Methods such as using a multi-stream CNN to detect personnel in remote monitoring images or using a deep learning model to detect smoke from burning equipment have shown promise. It is a reference point for those interested in keeping tabs on image anomaly detection.

Garcia-Font. et al. [31] suggested wireless sensor networks (WSN), machine learning has proven effective in a wide range of fields, including detecting cyber-attacks. The problem with a smart city is that it is much more difficult to solve the WSN scenario, and whether these methods are equitably valid and effective must be assessed. Two machine learning algorithms (support vector machines) are compared in this study (SVM)in a lab that replicates a real-world smart city use case) to detect anomalies with a wide range of devices, protocols, algorithms, and network configurations. As a result, it allowed us to demonstrate that, despite the importance of these techniques for smart cities, they require additional. Certain factors must be considered for an attack detection system to be effective.

Nayak. et al. [32] elaborated a comprehensive analysis of the deep learning-based video anomaly detection methods (DL-VAD) reported in state-of-the-art. Weapons in a sensitive location and disused luggage should be automatically detected in time during abnormal activities like trying to fight, riots, vehicular rule violations, and stampedes. Although video anomalies can be detected, it's difficult because of the contradictory nature of the

anomaly, the variety of environmental conditions, and the complexity of human behavior. As video anomaly detection research is still in its infancy, a few studies are specifically dedicated to it. There is no comprehensive review covering all aspects of video anomaly detection, such as meanings, classifications, modeling, and performance evaluation methodologies.

As a result of these investigations, the existing BCSA, SML, DL-ADA, WSN, and DL-VDA methodologies have improved. Safety qualities such as energy efficiency, stability, durability, flexibility, security, and protection are highlighted in the OC-VDL model to help solve difficulties.

### 3. Deep Model In Complex Environment

Research in deep reinforcement learning, which can revolutionize artificial intelligence, has exploded recently. Many groundbreaking developments have been benchmarked against competitions and simple physical simulations. Creating more sophisticated learning systems to handle more challenging real-world situations is critical as the field develops. However, issues like catastrophic forgetting and critical capabilities like talent structure through coursework learning remain unresolved. Huge deep learning systems often clash with algorithms that can rapidly adjust to changed data. This dilemma may not exist in the meta-learning paradigm, which holds promise as a framework for supporting slow and fast learning in single learner's various deep learning (VDL) strategies such as blockchain network an autoencoder.

### 3.1 BlockChain Network

Intelligent power grid systems have replaced manual distribution transformer tracking because they could not keep up with the ever-increasing demands of electricity systems. Most monitoring devices can't respond quickly when the operating environment goes haywire, and an exact match can be made with potentially disastrous results. Generate unambiguously linked real-time log files; blockchain technology is an encoded, dispersed archiving system. Transparency and security are ensured as a result of this. An innovative Blockchain Security Architecture has never been built on Deep Learning Smart Contracts. Following Industry 4.0 aimed to ensure connectivity among tradable Manufacturing Internet of Things devices. To our knowledge, this is the first study to integrate AI as a structural element into the Blockchain network, essential to the network's completion rather than as a supporting framework for improving the network's abilities. It introduces a Blockchain Network Security for IIoT based on Deep Learning Smart Contracts, which is more specific still in this new study.

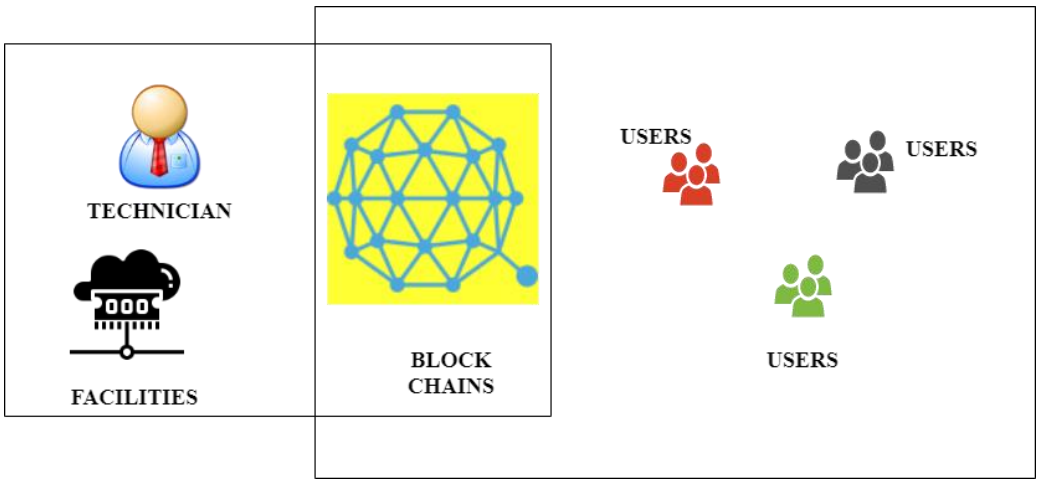



Figure 1: Structure of Blockchain

Figure 1. shows the chain's block structure in which maximum numbers of users are connected in the given one set of the framework. In other frameworks controlling departments for this blockchain are connected with which technicians and facilities are connected. Blockchains are connected in the middle of both frameworks. Despite its appearance, blockchain is quite simple in concept. A blockchain can be thought of as a new generation of the database. To comprehend blockchain, one must first grasp the concept of a database. A system is a database of digitally stored data on a computer network that can be accessed electronically. It makes finding specific information easier, and database information is typically organized in table format. One or a collection of people can use spreadsheets to manage and store limited data. On the other hand, a database is built to accommodate much larger amounts of data and allow multiple users to quickly and easily access, filter, and manipulate that data simultaneously.

### 3.1.1 Blockchain Technology

There are several ways in which blockchain technology addresses security and trust concerns. It is to begin; all new blocks are stored chronologically and linearly. To put it another way, they're always appended at the "very end" of the chain. A role on the chain is called a "height" assigned to each block in Bitcoin's Blockchain. Although the concept of blockchain appears to be complex, it is quite simple. It's nothing more than a special kind of database. In a blockchain, data is stored in an immutable, time-stamped record maintained by a distributed network of computers that are not currently owned by any one entity. Cryptographic principles secure and link all of these bits of information together (i.e., chain).

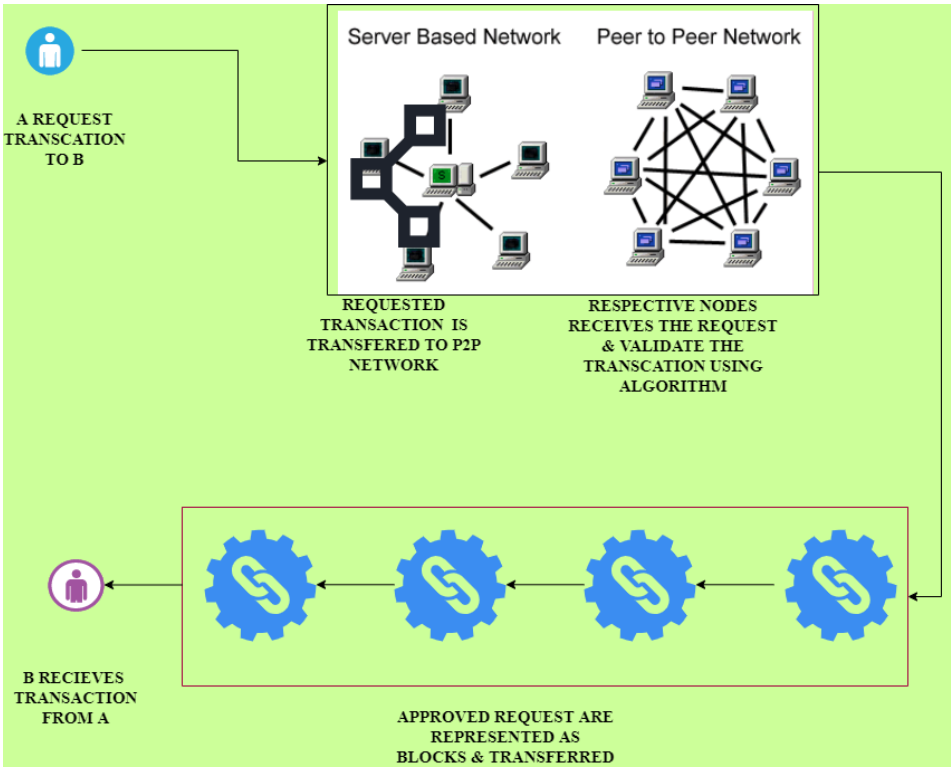



Figure 2: Implementation & Working of Blockchain Technology

Figure 2 above depicts how blockchain technology operates in action. Client A needs to send a transaction request to client B. The transaction is sent to a server-based and peer-to-peer network where the transaction is processed, sent to the p2p network, and validated over there using an algorithm. The same is transferred to a block where the nodes are represented as blocks, and the transaction is completed and accepted by client B.

### 3.1.2 Advantages of Blockchain

Due to its simplicity and transparency, blockchain has grown in popularity over the last few years. Most importantly, blockchain technology does not rely on any single entity. Because it's a publicly accessible, unalterable ledger, everyone has access to it. Due to its decentralized architecture, the blockchain is impervious to malware activity and system glitches. There isn't a point of failure because the database is replicated and stored in each node. It is nearly impossible to undo data storage in a blockchain once it has been made public. Because every transition is tracked and recorded on a public ledger, distributed ledger technology is perfect for storing financial data. Blockchain technology eliminates the need for a middleman by verifying transactions through mining. Total costs and transaction costs are reduced as a result of this.

### 3.2Anamoly Detection IoT

In anomaly detection (ADE), patterns are identified in a dataset that differs from expected. The objective is to keep false alarms minimal while detecting high levels of potential irregularities. Anomaly detection methods can be divided into three groups. Supervised ADE is the first type of supervised ADE in which techniques are tested using data from normal and extreme categories. Prediction models for normal and abnormal classes are generally used in these situations. Semi-supervised abnormal detection assumes that normal data has been

classified in the training set. To find anomalies in your test data, you'll need to use a standard approach that creates a basic outline responding to expected behaviour. This type of ADE does not require any preliminary data for training and is the most flexible. In this instance, the methodologies presumptively consider and test information have more vectors compared to the extreme one. This results in a significant portion of inaccurate estimates.

$$K = argmin \ (\max CP_{\partial} ( z = z|y_j)) \quad (1)$$

As equation (1)specifies the max $CP_{\partial} ( z = z|y_j)$ is the class probability at the supreme of specified $y_j$

**Energetic anomaly detection under supervision Algorithm**

The Algorithm shown below represents the active learning for anomaly detection

**Input**

$P^0$the first set of practice data

$\partial$ unknown repository of information

$N_{it}$the number of times something is repeated;

$\propto$ constant monitoring of mathematical modelling

$n$ quantity of randomly chosen data points that will be used in the query

**carrying out experimental tests:**

**For** k varying from 0 to $N_{it}$ do

use $P^K$ to put the classifier through its paces $\propto^k$

use $\propto^k$ to classify all of the data in a $\partial$

Select $N$ informative samples $\partial$ by calculating the most ambiguous value and consulting a specialist for labeling.

Remove all samples $\partial$ and replace them with the ones from $P^K$ new data records.

Until the criterion for stoppage is met

**End**

It is here proposing an anomaly detection algorithm that works according to deep neural networks from the point of view of identification and fire smoke recognition for the big data environment of strong IoT equipment operation. When used in the heavy machinery operating environment, the image detection method based on inter-CNN-based remote monitoring and the traffic detection technique based on deep convolutional neural networks have achieved good identification results for personnel and have successfully detected traffic from the image, respectively. It serves as a guide for keeping track of image anomaly detection. Malfunctioning power equipment may lead to significant economic and social consequences if not addressed quickly. It is crucial to keep an eye on the operational environment and permit electrical equipment to function smoothly to maintain a steady electricity supply. Therefore, it is crucial to research abnormality identification in images of power network equipment monitoring. During the anomaly detection process, poor stability and low-efficiency issues are overcome by applying the deep smoke convolution and multi-convolution neural network approach. Being able to distinguish anything by sight has enhanced the CNN network's ability to train optical data flow inside the personnel anomaly-detecting component. The efficiency of the technique in identifying human anomalies has

been tested. Finding an applicant's smoke region in a video frame is the initial stage in employing fire smoke detection. Once a smoking candidate zone has been discovered, rectified feature vectors are extracted from it using a deep learning model.

### 3.3 CNN-based IoT Equipment with Deep Learning

Convolutional neural networks CNN have two basic structures: extraction of features and feature mapping. The previous layer's local acceptance domain is used to connect neurons for image retrieval. During the feature extraction process, the relationship between the features is extracted in the acceptance domain. It's possible to reduce the network's parameter size using a feature map and associated neurons with the same weight. Scene recognition methods can be categorized into object and scene-based methods which is done according to the CNN network. One method uses a CNN network based on object recognition and object models. It is done using scene training data; CNN networks constitute the second largest class of methods, and an image can better learn about the scene with a network of this type. The following are the steps involved in scene classification:

The average sampling for obtaining set $R = \{ r_1 , r_2, \ldots\ldots r_N \}$of image blocks, and obtain the semantic probability $S = \{ S_1 , S_2, \ldots\ldots S_N \}$ through the classification of the object. The feature is$F = \{ F_1 , F_2, \ldots\ldots F_N \}$ the center of the conceptual wheel is computed using equation (2).

$$\vartheta_m = \frac{1}{P_m} \sum_{j=1}^{P} S_j{}^m F_j \quad (2)$$

From equation (2),$S_j{}^m$ represents the $m$th measurement of $S_j$, $\vartheta_m$ is defined as the feature area layout, and Pm is denoted as the feature space layout which is computed using equation (3).

$$P_m = \sum_{j=1}^{P} S_m{}^j \quad (3)$$

$$\emptyset_m = \frac{P_m}{P} \quad (4)$$

The security is achieved from the above equation (3), and precision is calculated using equation (4), mentioning $\emptyset_m$as the m-th measurement site's mass.

$$\mu_m^2 = \frac{1}{P} \sum_{j=1}^{P} S_m{}^j \ (F_j - \vartheta_m)(F_j - \vartheta_m)^T \quad (5)$$

Equation (5) is an estimate of semantic deviation and through which privacy is obtained.

$$S_m = \frac{1}{\sqrt{\emptyset_m}} \sum_{n=1}^{N} S_n{}^m \frac{(F_t - \vartheta_n)}{\mu_m} \quad (6)$$

$$H_m = \frac{1}{\sqrt{\emptyset_m}} \sum_{n=1}^{N} S_n{}^m \left[ \frac{(F_t - \vartheta_n)^2}{\mu_m} - 1 \right] \quad (7)$$

The vector was utilized for encoding variance and mean in this data set, as shown in equations (6) and (7), where N is the amount of samples used to analyze durability. $[(S_1, H_1), (S_2, H_2), (S_3, H_3), \ldots\ldots\ldots (S_m, H_m)]$.

### 3.4 Dual Flow Configuration of CNN

Modeling behaviour in time and space domains is possible with vision anomaly detection. Optical flow fields are widely used in control because they can provide information on the speed and direction at which pixels are moving in the current image.

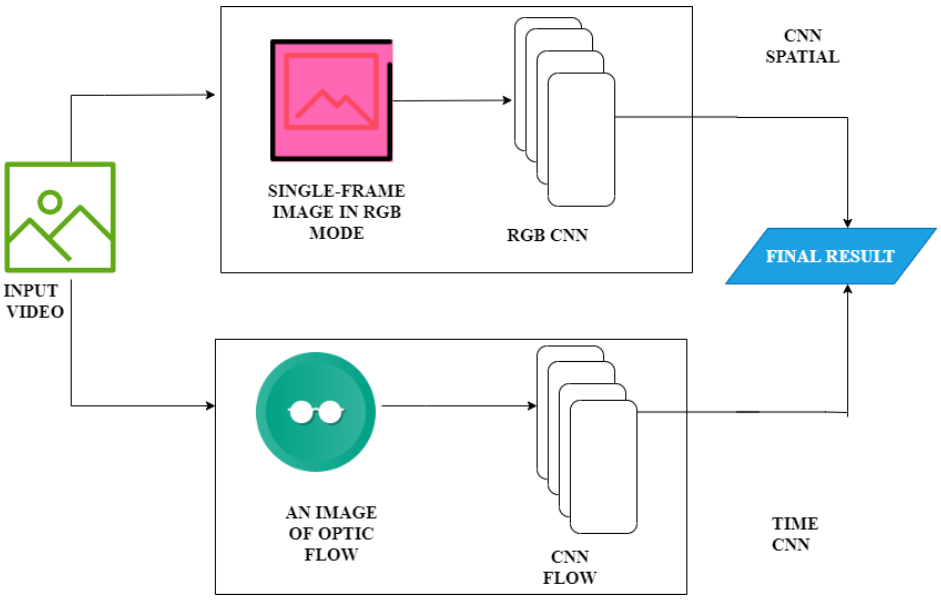



Figure 3: Image processing using CNN in a dual-flow configuration

The above figure 3 shows Image processing using CNN in a dual-flow configuration. Dual-stream CNN-based personnel detection uses CNN's learning capability to segment and classify color images and optical flow images. There are two CNN networks: one is built on RGB images, and the other is on optical flow images of CNN's original two-stream architecture diagram. The processing done by the spatial CNN can be seen in the upper branch. The spatial CNN follows the same network model for object detection and classification tasks.

The trained dataset is utilized for the network fine-tuning process before applying it to the full dataset. The model must anticipate each video frame in the data set for behaviour detection because it is made up of behavioural data recorded on video.

Spatial CNN has a provision of additional synthetic characteristics in data sets thanks to the superior learning capabilities of CNN. The next branch shows how the time CNN is processed. As shown by the features of the optical flow image, the amount of labeled visual information is extremely small, which poses a challenge for the training time CNN model. Calculating the optical image takes significantly longer than obtaining the RGB image. As a second point, the optical flow calibration is less precise than the RGB picture calibration.

Many activities or sports have parts that are duplicated elsewhere. The optical stream and the duration of the optical method influence CNN's learning ability has been suggested. With the help of keyframe extraction and video segmentation, CNN's learning ability for electro-optic flow information can significantly improve.

3.5 **Multi-Flow Configuration of CNN**

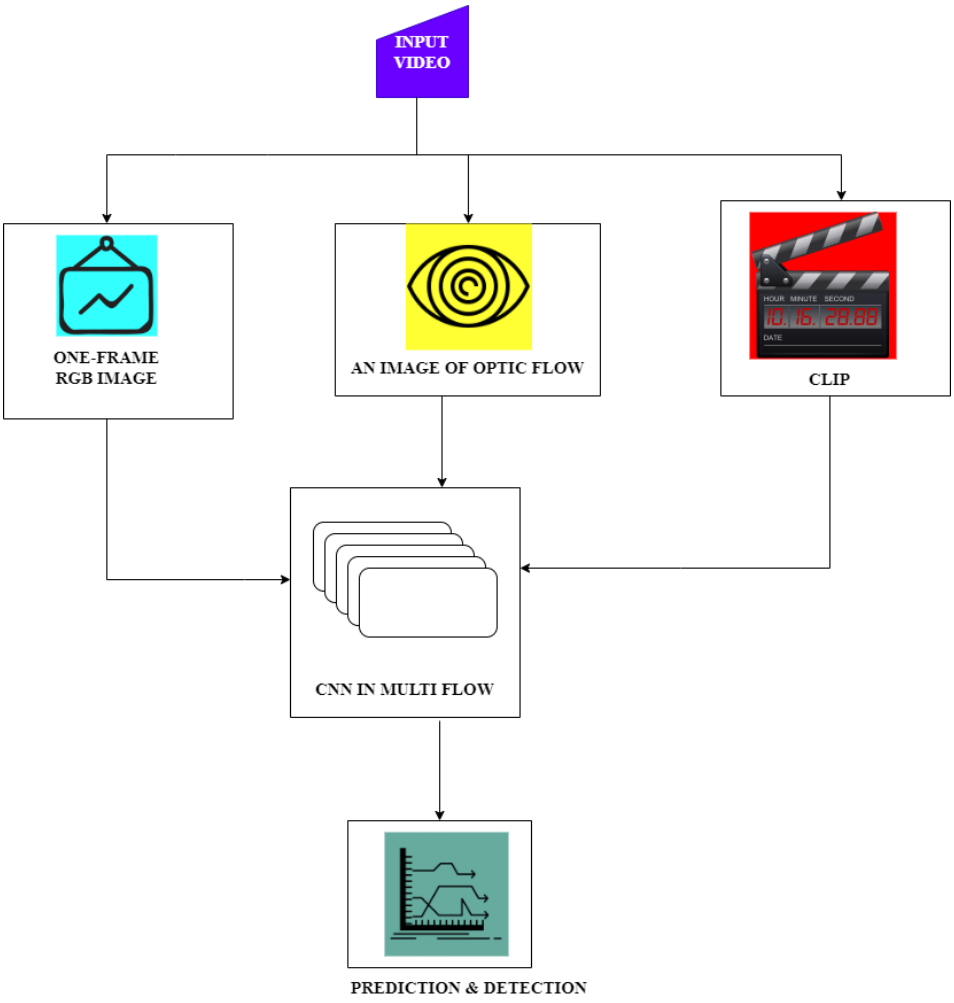



Figure 4: Image processing using CNN in a Multi-flow configuration

As per Figure 4, recognizing a scene serves as the input unit for CNN, which predicts what will happen next in the current video scene and makes predictions by cutting the video into individual frames one at a time. The image of optical flow serves as per the framing methodology. One frame RGB image is directed to join at Multiflow CNN model and finally prediction, detection takes place in which the image is detected and predicted.

**3.6 Auto Encoder Module**

It is necessary to identify fraudulent internet traffic and glitches in general, and the proposed system uses Deep learning to detect malicious activity among IIoT devices. The contract stipulates that the extract and intelligent commentary will be performed using a trained Auto Encoder type Neural Network (NN) and network traffic features between vending machines.

The Neural Network is divided into two network connections in an autoencoder: an encoder and a decoder. Four major components make up an autoencoder.

Encoder: It is where the system knows how to compress the input data and reduce its dimensions.

Bottleneck: which surface contains the information data's condensed representation. The input data has been shrunk to its smallest possible size.

Decoding: Data reconstruction from an encoded representation is known as decoding, and it is the process whereby the model is trained on how to do it.

Reconstruction loss: Decoder performance can be evaluated by measuring how closely the output signal matches the input signal.

This network takes an input and refines it so that the second converter system can use it to bring the original input back to its original form.

When using, first deform the input data into a response time representation and then reconstruct the output from that. They gain knowledge to compress the original input data into an abstract sense, which is then decompressed by transforming it into something that matches the original input data in size and format. As a result, it is compelled to decrease the initial problem's dimensions and learn how to overlook noise. To put it another way, the autoencoder has three layers such as input, hidden, and output which are interconnected with each other. The encoder networks according to the multilayer perceptron network that used to predict the output Q by processing the input P. The input layer processes the P processed by the hidden layer and the output network produces the output Q. Then the transmission of the encoder and decoder of input is defined using the below equations.

$y : Y -> W$

$y^0 : W \rightarrow Y$ (8)

$$y, y^0 : \{|Y - (y^0 * y)|Y\}^2$$

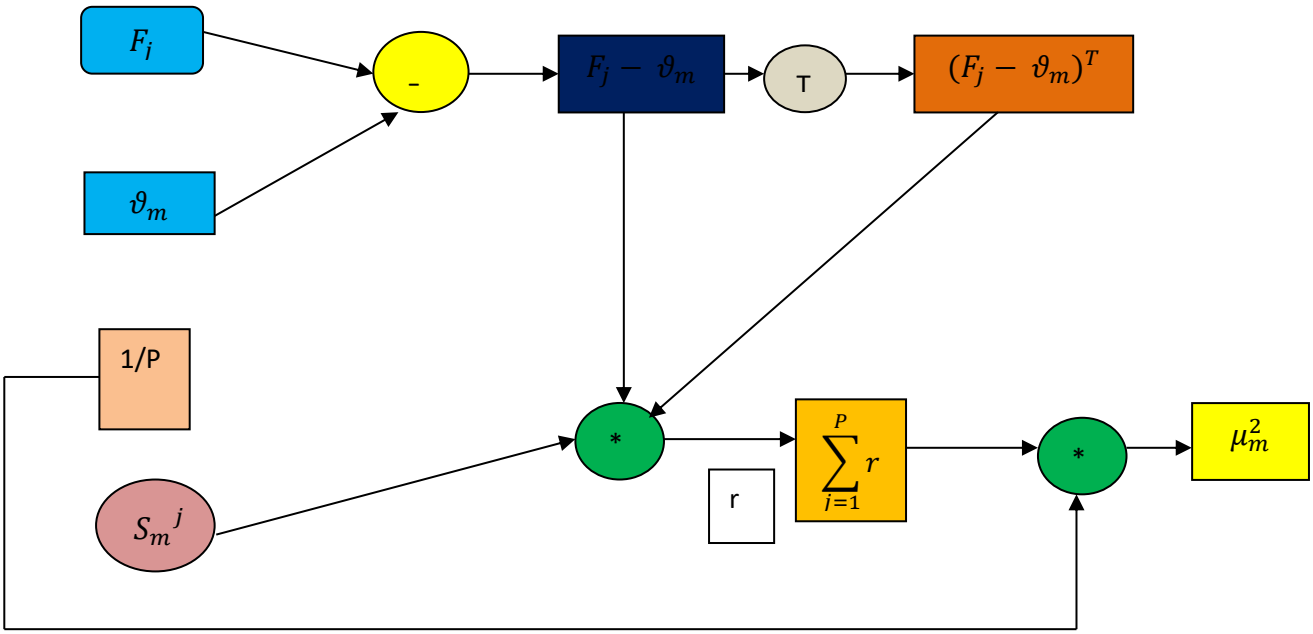
An objective function is optimized throughout the learning process to compute the deviation of input (y) and reconstructed value (y0). Compared to other models, the above equation provides a solution for top-performance efficiency. The encoder gets the input vector $y \in F^{S_y}$ and produces a vector

$w \in F^{S(1)}$ is defined in the below equation.

$w = j^{(1)}(K^{(1)}y + c^{(1)}$ (9)

$y^0 = j^{(2)}(K^{(2)}y + c^{(2)}$ (10)

It is clear from the equation that (8) relates to the network starting level (9). Equations (9) help efficiently attain the performance (10).




Type equation here.

Figure 5: Encoder's Node Count Diagram

The above figure 5 shows the path diagram of equation(5) semantic deviation. The encoder's node count decreases as it advances through the levels, while the decoder's node count increases. Decoders are typically symmetrical in design in aspects of the layer structure to the encoder. Because of this, the current network anomaly detection algorithm presented in this paper and blockchain technology, CNN-based deep learning, helps enhance security, durability, versatility, and network traffic protection using a deep model of the complex environment.

**4. Results & Discussion**

The proposed OC -VDL model's security, precision, privacy, durability, performance, and effectiveness were all considered during the simulation analysis. The responses to each section are shown in the graphs below.

**4.1 SecurityAnalysis**

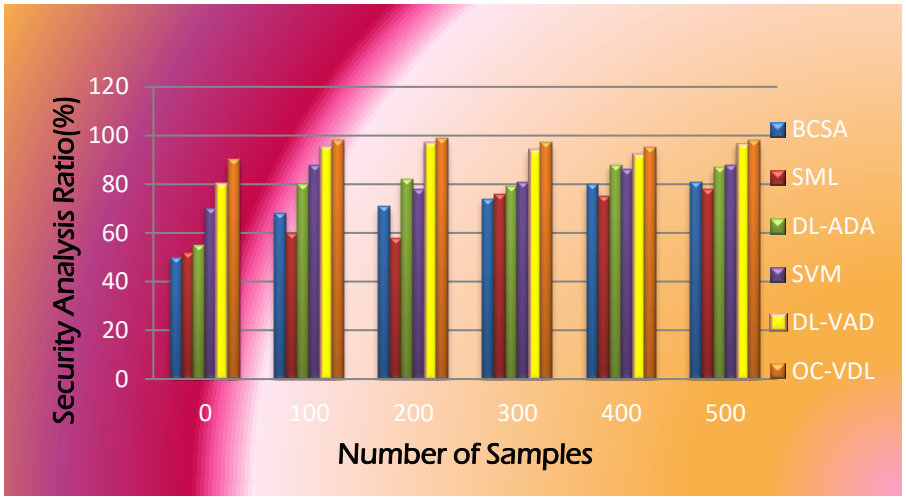



Figure 6: Security Analysis

Each job/task is broken down into key training sequences that identify safety elements at each step and coach employees about avoiding unsafe conditions.

Using Security Analytics, a proactive approach to cybersecurity can be developed by analyzing large amounts of data. Monitoring network traffic, for example, could be used to spot signs of compromise before they become a real threat. This process is systematic. It is achieved from equation (3).

**4.2 Precision Analysis**

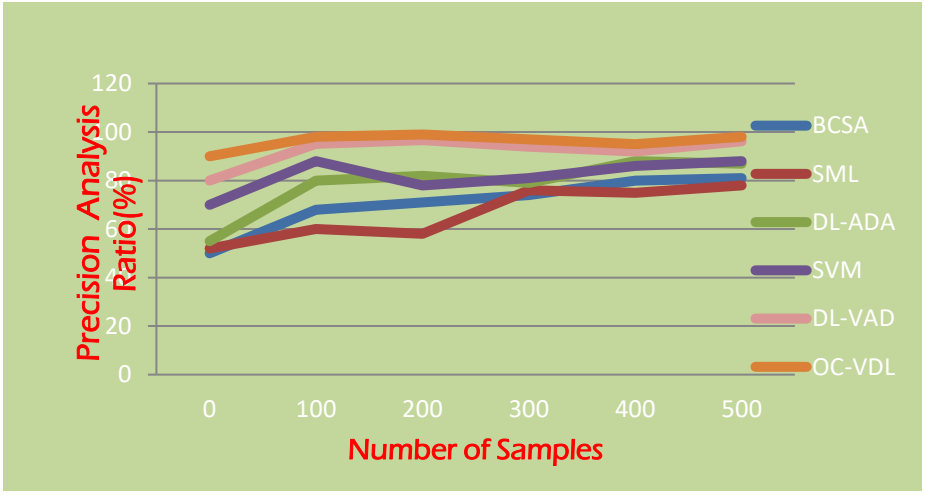



Figure 7: Precision Analysis

As a sample, Figure 7 depicts the precision analysis for the model proposed. Precision refers to how close a quantification is to a standard or ideal quantity. It is a measure of honesty, and the reverse is true, observed from equation (4). This term describes how closely an observed or calculated amount corresponds to a valid (actual) quantity. Accuracy and precision have a great deal in common, yet they are two very different things.

**4.3Privacy Analysis**

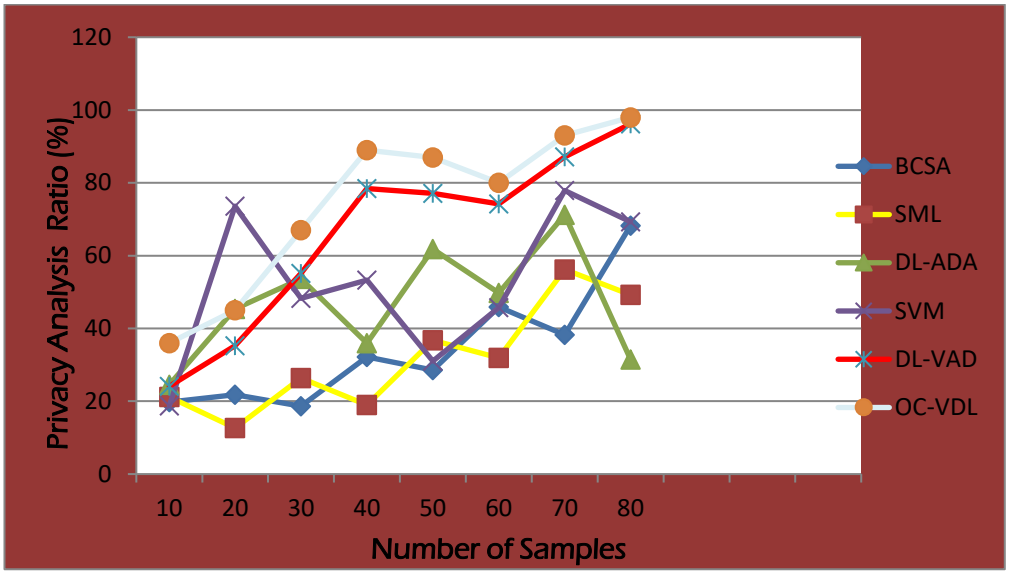



Figure 8: Privacy Analysis

Figure 8 reveals the privacy analysis. Two methods are there to be considered for in-network traffic. There are two types of traffic-analysis attacks: passive and active. It's possible to conduct a passive traffic-analysis attack by searching for specific characteristics in one part of the system's traffic and then stealing them from another. Network analysis can approximate complicated relationship patterns, and the entire network can be analyzed to reveal the network's core features. Results: There is a wide range of interactions between the items, as seen from the network structure. The network was divided into three groups, which can be achieved through equation (5).

**4.4 Durability Analysis**

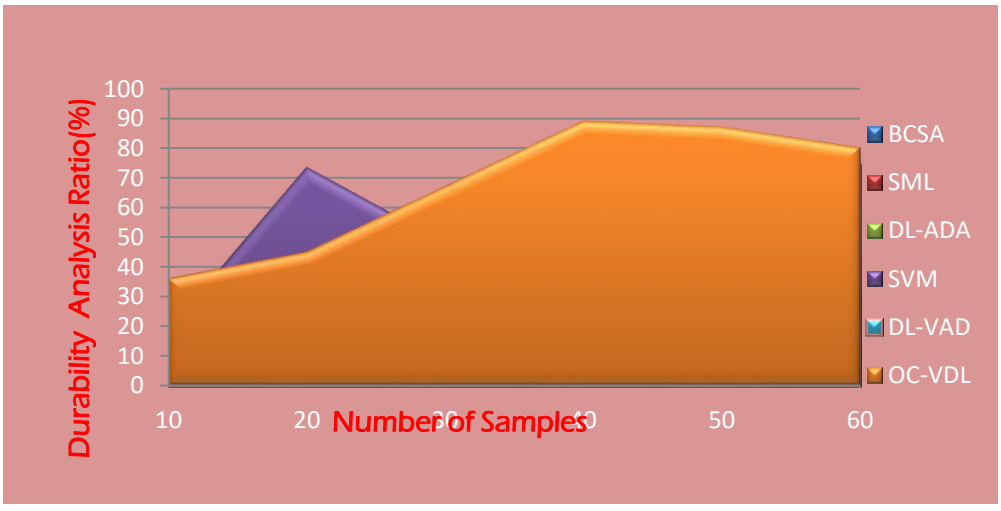



Figure 9: Durability Analysis

Figure 9 represents durability analysis, an investigation, test, or measurement procedure's ability to produce consistent results over time. The degree to which a study's design produces reliable and secure results is known as the reliability of the researcher. If a measurement consistently yields the same results repeatedly when used on the same thing, it's considered precise data. This is achieved through equation (6).

### 4.5 Performance Analysis

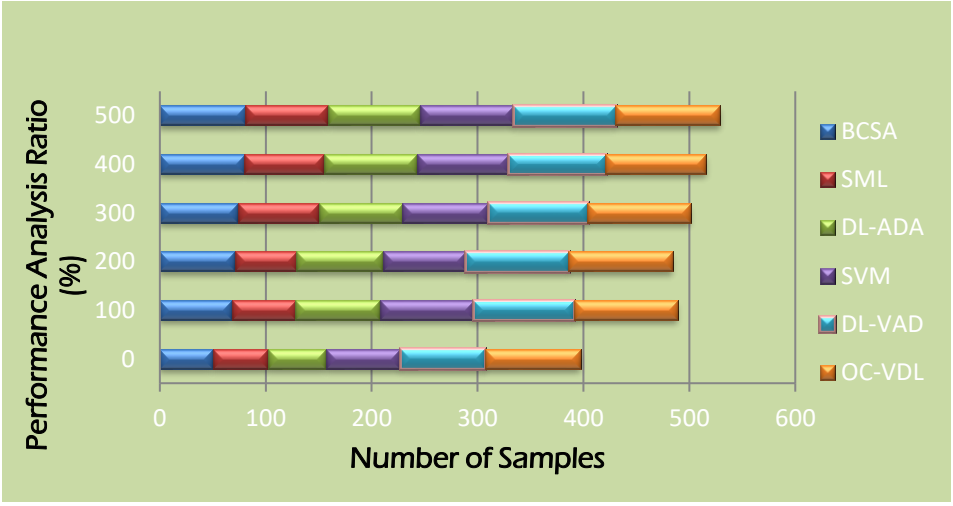



Figure 10: Performance Analysis

Figure 10 depicts the performance analysis shown by a graph plotting against the existing proposed algorithms and other methods with many data sets. For example, the OC-VDL approach has a 98.9 % performance rating in the suggested model, compared to different ways, with a lower performance rating that the equation anomaly detection algorithm satisfies.

### 4.6 Efficiency Analysis

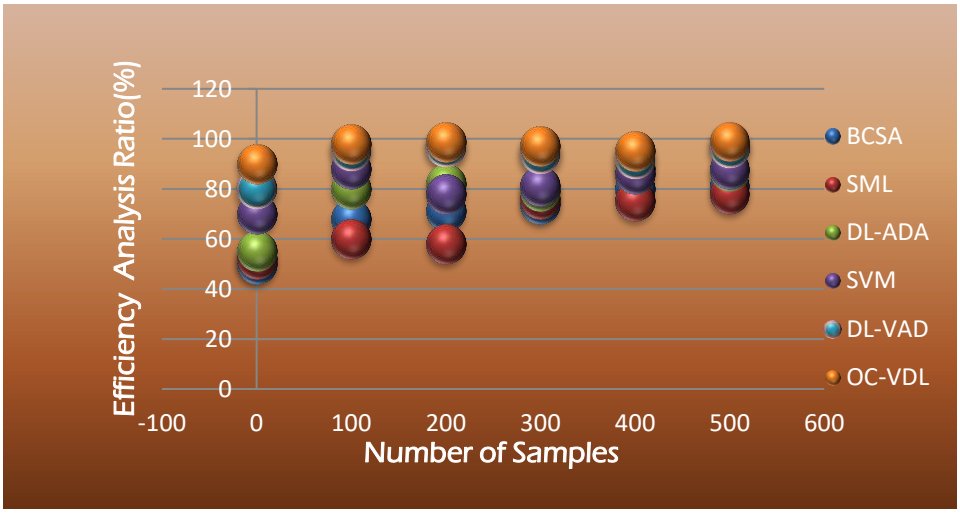



Figure 11: Efficiency Analysis

On the other hand, efficiency means using as many resources as possible while still producing as much. Regarding efficiency, using fewer resources, like individual time and energy, achieves a specific result. Often, the quickest and most convenient method of completing the procedure is chosen instead, and the highest levels of efficiency are achieved using (7),(8). Figure 11 depicts the results of the efficiency test.

Compared to existing models such as BCSA, SML, DL-ADA, SVM, and DL-VAD, the proposed model OC-VDL is superior in performance, accuracy, efficiency, safety, and security. This new technology was developed to resolve the competing issues mentioned in the paper.

## 5. Conclusion

An intelligent information security tracking, modeling, and management system combines architecture and design normalization and implementation of the project outlier detection via OC-VDL smart contracts. It's based on clever techniques that our researchers have frequently employed. Smart Contracts and Blockchain network features provide a two-way joint declaration for this scheme, which enforces advanced anomaly detection functions. As a result, even the most efficient and effective network interaction between trading devices in the IIoT ecosystem is guaranteed. The proposed Deep Learning Smart Contract uses a cutting-edge Deep Autoencoder to provide an intelligent mechanism for accurately classifying risky oddities in IIoT exchanges, most of which are cyber-attacks. The system's primary goal is to improve critical infrastructure security protocols, and the proposal does that. With the help of a multifaceted dataset of high complexity, the proposed system was evaluated for its performance in comparisons, controls, and tests. The dataset was developed after thorough research into the operation of IIoT devices. This research presented a novel way to detect anomalies in the Blockchain network using advanced computational intelligence methods that are dependable, constrained, and extremely effective. Therefore artificial intelligence (AI), as a building element of the Blockchain network, is the proposed system's most significant innovation he strengthening the network's Blockchain. The Deep Autoencoder variables should be further optimized for future system improvement and expansion. In this way, the proposed technique will become a classification process that is more precise, efficient, and quick and that can separate IIOT system states with even greater precision.

Further optimization of the Deep Autoencoder parameters should focus on any system development or future improvement suggestions. The new approach will be a classification process that can separate IIOT system states even more precisely while faster and more efficient. Additionally, the proposed framework should be improved by automatically incorporating self-improvement techniques and redefining its parameters.

## References


[1] Gao, J., Wang, H., & Shen, H. (2020, August). Machine learning-based workload prediction in cloud computing. In *2020 29th international conference on computer communications and Networks (ICCCN)* (pp. 1-9). IEEE.

[2] Liu, B. H., Nguyen, N. T., Pham, V. T., & Lin, Y. X. (2017). Novel methods for energy charging and data collection in wireless rechargeable sensor networks. *International Journal of Communication Systems*, *30*(5), e3050.

[3] Jaber, M.M., Ali, M.H., CB, S., Asaad, R.R., Agrawal, R., Bizu, B., and Sanz-Prieto, I., 2023. Future smart grids creation and dimensionality reduction with signal handling on smart grid using targeted projection. *Sustainable Computing: Informatics and Systems*, 39.

[4] Javed, A. R., Rehman, S. U., Khan, M. U., Alazab, M., & Khan, H. U. (2021). Betalogger: Smartphone sensor-based side-channel attack detection and text inference using language modeling and dense MultiLayer neural network. *Transactions on Asian and Low-Resource Language Information Processing*, *20*(5), 1-17.

[5] A. Lakhan, M.A. Mohammed, K.H.Abdul kareemetal.,Secure blockchain assisted internet of medical things architecture for data fusion enabled cancer workflow, Internet of Things(2023),doi:https://doi.org/10.1016/j.iot.2023.100928.

[6] Hussein, A.F., ALZubaidi, A.K., Habash, Q.A., and Jaber, M.M., 2019. An adaptive biomedical data managing scheme based on the blockchain technique. Applied Sciences (Switzerland), 9(12).

[7] Pallavi Goel,Sarika Chaudhary, Maximizing Anomaly Detection Performance in Next-Generation Networks, Journal of Cybersecurity and Information Management, Vol. 12 , No. 2 , (2023) : 36-51` (Doi : https://doi.org/10.54216/JCIM.120203)

[8] Abidi, M. H., Alkhalefah, H., Moiduddin, K., Alazab, M., Mohammed, M. K., Ameen, W., &Gadekallu, T. R. (2021). Optimal 5G network slicing using machine learning and deep learning concepts. *Computer Standards & Interfaces*, *76*, 103518.

[9] Hammad, M., Alkinani, M. H., Gupta, B. B., &Abd El-Latif, A. A. (2021). Myocardial infarction detection based on deep neural network on imbalanced data. *Multimedia Systems*, 1-13.

[10] Naeem, M. A., Nguyen, T. N., Ali, R., Cengiz, K., Meng, Y., &Khurshaid, T. (2021). Hybrid Cache Management in IoT-based Named Data Networking. *IEEE Internet of Things Journal*.

[11] Billah, M. F. R. M., Saoda, N., Gao, J., & Campbell, B. (2021, May). BLE Can See: A Reinforcement Learning Approach for RF-based Indoor Occupancy Detection. In *Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)* (pp. 132-147).

[12] Hussein, A.F., ALZubaidi, A.K., Habash, Q.A., and Jaber, M.M., 2019. An adaptive biomedical data managing scheme based on the blockchain technique. Applied Sciences (Switzerland), 9(12).

[13] Guo, Z., Tang, L., Guo, T., Yu, K., Alazab, M., &Shalaginov, A. (2021). Deep graph neural network-based spammer detection under the perspective of heterogeneous cyberspace. *Future Generation Computer Systems*, *117*, 205-218.

[14] Sedik, A., Hammad, M., Abd El-Latif, A. A., El-Banby, G. M., Khalaf, A. A., Abd El-Samie, F. E., &Iliyasu, A. M. (2021). Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities. *IEEE Access*, *9*, 94780-94788.

[15] Nguyen, N. T., Liu, B. H., Chu, S. I., &Weng, H. Z. (2018). Challenges, designs, and performances of a distributed algorithm for minimum-latency of data-aggregation in multi-channel WSNs. *IEEE Transactions on Network and Service Management*, *16*(1), 192-205.

[16] Waleed Abd Elkhalik,Ibrahim Elhenawy, Semi-supervised Transformer Network for Anomaly Detection in Cellular Internet of Things, International Journal of Wireless and Ad Hoc Communication, Vol. 4 , No. 1 , (2022) : 56-68 (Doi : https://doi.org/10.54216/IJWAC.040106).

[17] Asghar, M. Z., Subhan, F., Ahmad, H., Khan, W. Z., Hakak, S., Gadekallu, T. R., &Alazab, M. (2021). Senti-eSystem: A sentiment-based eSystem-using hybridized fuzzy and deep neural network for measuring customer satisfaction. *Software: Practice and Experience*, *51*(3), 571-594.

[18] Khan, W. U., Javed, M. A., Nguyen, T. N., Khan, S., &Elhalawany, B. M. (2021). Energy-efficient resource allocation for 6G backscatter-enabled NOMA IoV networks. *IEEE Transactions on Intelligent Transportation Systems*.

[19] Rauf, H. T., Gao, J., Almadhor, A., Arif, M., &Nafis, M. T. (2021). Enhanced bat algorithm for COVID-19 short-term forecasting using optimized LSTM. *Soft Computing*, 1-11.

[20] Rezaee, K., Savarkar, S., Yu, X., & Zhang, J. (2022). A hybrid deep transfer learning-based approach for Parkinson's disease classification in surface electromyography signals. Biomedical Signal Processing and Control, 71, 103161.

[21] Rehman, A., Rehman, S. U., Khan, M., Alazab, M., & Reddy, T. (2021). CANintelliIDS: detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU. *IEEE Transactions on Network Science and Engineering*.

[22] Saeed, V. A. (2024). A Framework for Recognition of Facial Expression Using HOG Features. International Journal of Mathematics, Statistics, and Computer Science, 2, 1–8. https://doi.org/10.59543/ijmscs.v2i.7815

[23] Salman, O. H., Taha, Z., Alsabah, M. Q., Hussein, Y. S., Mohammed, A. S., & Aal-Nouman, M. (2021). A review on utilising machine learning technology in the fields of electronic emergency triage and patient priority systems in telemedicine: Coherent taxonomy, motivations, open research challenges and recommendations for intelligent future work. Computer Methods and Programs in Biomedicine, 209, 106357.

[24] Xie, G., Yang, L. T., Yang, Y., Luo, H., Li, R., &Alazab, M. (2021). Threat Analysis for Automotive CAN Networks: A GAN Model-Based Intrusion Detection Technique. *IEEE Transactions on Intelligent Transportation Systems*.

[25] Zhang, X., & Wang, Y. (2021). Research on intelligent medical big data system based on Hadoop and blockchain. EURASIP Journal on Wireless Communications and Networking, 2021(1), 1-21.

[26] Ghanbari Ghoushchi, N. ., Ahmadzadeh, K., & Jafarzadeh Ghoushchi, S. (2023). A New Extended Approach to Reduce Admission Time in Hospital Operating Rooms Based on the FMEA Method in an Uncertain Environment. Journal of Soft Computing and Decision Analytics, 1(1), 80-101. https://doi.org/10.31181/jscda11202310

[27] Demertzis, K., Iliadis, L., Tziritas, N., &Kikiras, P. (2020). Anomaly detection via blockchained deep learning smart contracts in industry 4.0. Neural Computing and Applications, 32(23), 17361-17378.

[28] Ahmed Abdelmonem, Nehal N. Mostafa, Interpretable Machine Learning Fusion and Data Analytics Models for Anomaly Detection, Fusion: Practice and Applications, Vol. 3 , No. 1 , (2021) : 54-69 (Doi : https://doi.org/10.54216/FPA.030104)

[29] Hou, R., Pan, M., Zhao, Y., & Yang, Y. (2019). Image anomaly detection for IoT equipment based on deep learning. *Journal of Visual Communication and Image Representation*, *64*, 102599.

[30] Garcia-Font, V., Garrigues, C., &Rifà-Pous, H. (2018). Difficulties and challenges of anomaly detection in smart cities: A laboratory analysis. *Sensors*, *18*(10), 3198.

[31] Nayak, R., Pati, U. C., & Das, S. K. (2020). A comprehensive review on deep learning-based methods for video anomaly detection. *Image and Vision Computing*, 104078.