Vol. 06, No. 1 (2024) 241-250, doi: 10.24874/PES.SI.24.02.007

Proceedings on Engineering Sciences

www.pesjournal.net

UTILIZING A UNIQUE DEEP LEARNING TECHNIQUE FOR DETECTING ANOMALIES IN INDUSTRIAL AUTOMATION SYSTEMS

Ranganathaswamy Madihalli Kenchappa[1]
Rakesh Kumar Yadav
Alka Singh
Arvind Kumar Pandey

Received 30.11.2023.
Received in revised form 19.01.2024.
Accepted 29.01.2024.
UDC – 005.59

Keywords:

Industry, Stochastic Turbulent water flow optimization based restricted Boltzmann machine (STWFO-RBM), Anomalies, Real-time monitoring.

ABSTRACT

Industrial automation systems (IASs) are utilized in vital facilities to sustain society's fundamental services. As a consequence, protecting them against terrorist operations, natural catastrophes and cyber-threats is essential. The research on techniques for identifying cyber-attacks in IAS environments is lacking. The study proposed the Stochastic Turbulent water flow optimization based restricted Boltzmann machine (STWFO-RBM) to overcome the challenges. The proposed STWFO-RBM integrates anomaly detection into the fabric of industrial automation, enhancing system resilience and responsiveness. We collected datasets from the water industry and preprocessed them through min-max normalization, and then principal component analysis was used for feature extraction. The results show that the suggested technique applies to a real-world IAS situation, with state-of-the-art accuracy of 97%, F1 score of 96%, precision of 98%, recall of 95% and 6.1s of computational time. Our proposed method is better than the average of earlier endeavors.

1. INTRODUCTION

Industry automated methods are those that employ robotics or software for controllers to handle various equipment and procedures in a business with some sort of interaction between humans (Bayram et al., (2021)). They range in sophistication between basic electronic management methods through powerful modular logic controllers. Enhancing productivity, dependability and security during production and other business operations is the key goal of automation in industries (Hao et al., (2021)). The devices collect data from the real environment, such as location, pressure and temperature. Ethernet cables are used by automated factories to enable information transfer with multiple parts (Wang et al., (2020)). It is essential to identify abnormalities in automated factories to guarantee the dependable and seamless functioning of intricate production procedures. Finding departures beyond typical conduct is difficult but necessary job in the changing economic environment because equipment and procedures are interconnected (Genge et al., (2019)). If abnormalities are ignored, they can result in lost productivity along with greater upkeep expenses, or they could jeopardize the security of personnel and property (Lindemann et al.,

[1] Corresponding author: Ranganathaswamy Madihalli Kenchappa
Email: mk.ranganatha@jainuniversity.ac.in

(2020)). The emergence of revolutionary innovations like computer intelligence and the World Wide Web of Things presents fresh possibilities to improve the identification of anomalies in factories (Kim et al.,(2020)). Large volumes of information are produced by such machinery, providing a previously unheard-of chance to learn more about the complex internals of production procedures (Li et al., (2021)).

By evaluating such information, trends and patterns that represent typical behavior could be found, making it possible to spot abnormalities whenever departures from routine happen. Technologies for factories comprise a large number of networked actuators, sensing devices and controls (Demertzis et al., (2020)). Abnormalities can appear in a variety of shapes, such as deviations affecting impulses and abrupt surges in information from sensors. Sophisticated algorithms that can distinguish between safe variations and dangerous ones are needed to find such variations (De Vita et al., (2020)). Anomaly identification in automated factories includes the major issues that these sectors confront, the value of continuous surveillance and the contributions of novel innovations to the creation of reliable aberrations that detect the methods. Kim et al., (2022)). Identifying anomalies in automated factories includes the major issues that these sectors confront the value of continuous surveillance and the contribution of novel innovations toward the creation of reliable aberration-detecting methods (Huong et al., (2021)). The objective of the study is to get a thorough grasp of the technology and procedures used to identify abnormalities in automated factories. Through an examination of the difficulties in industrial facilities that are encountered and the possible repercussions of unnoticed irregularities, this study seeks to make a significant contribution to the subject. Abnormalities are varied beyond typical or anticipated trends that indicate possible problems, abnormalities, or openings.

These outliers can take a variety of shapes, such as sudden occurrences, economic upheavals, governmental modifications and technological developments (Ghazal et al., 2020;Leander et al., 2022). Companies and groups must identify and comprehend abnormalities to change, develop and reduce hazards. This investigation on industry irregularities explores an ever-changing and varied environment wherein unforeseen events have a significant influence on the past, there and destiny (Hsieh et al. 2019, Sapkota et al., (2020)). Abnormalities serve as hurdles and accelerators, forcing sectors to change and rethink their approaches to resiliency and equitable development (Liet al.,2021: Nawaratne et al., 2019). They could take the shape of social catastrophes or technical innovations. The complex structure of disparities draws focus on the impact on various sectors and the companies used to deal with and take advantage of this transformative potential (Choi et al., (2021)).

1.1 Contributions of the study

- It ensures the identification techniques that develop to meet new problems and adjust to modifications in manufacturing processes by promoting an environment for ongoing growth.
- Using anomaly recognition, one might find odd trends that can point to a vulnerability compromise.

The study proposed a Stochastic Turbulent water flow optimization based restricted Boltzmann machine (STWFO-RBM) to improve the industry settings over the safety stance.

2. RELATED WORKS

Rosa et al., (2021) discovered the concentration on each of the complete structures and fundamental neural network techniques. They suggested a comprehensive architecture for hacking anomaly recognition structure among several features and the essential anomalous detecting part at a situation processor level and specialized in detecting the sensors. Ding et al., (2020) explored the implementation of long short-term memory (LSTM) based fault detectors with an apparatus including 2 commercial robots. An LSTM predictor's information by intelligent analyzing the difference among the initial signals and its LSTM forecast utilizing both approaches, identification of errors was accomplished.

Das et al., (2020) revealed the grim truth that hacks against industrial controllers with the intent to take down the related actual systems such as water treatment plants and electric grids were commonplace. It was critical to recognize and prevent abnormal activity, like assaults. Huang et al., (2021) examined the preventive repair scheduling along with prompt identification of possible manufacturing equipment breakdowns depending on effective identification of anomalies. A platform for identifying anomalies powered by virtual twins allowing for abnormality predictions as well as actual time manufacturing health of systems tracking. Mokhtari et al., (2021) assessed the Networking surveillance schemes that unusual activity identification gets employed to pinpoint security concerns in control systems used in factories. Hackers can confuse an intrusion detection system based on networks by mimicking its regular operations. In this study, they suggested a novel approach for solving this issue using oversight management along with the information collection method's metrics. The suggested method was known as measuring a security structure and it allowed the computer to identify any unusual behavior, regardless of whether the intruder attempts to cover up it in the administrative portion of the network. Ahmed et al., (2020) explored the defenses for critical assets like water treatment plants and the electrical system, data-driven methods have become more and more prevalent. Until these sensors can be confidently implemented in big electricity networks even city-scale organisms, there were several critical issues that need to be addressed, irrespective of the approach taken to develop these devices and the information utilized for the assessment of performance.

Haller et al., (2019) investigated the methodical approach for incorporating inexpensive algorithms for detecting anomalies in control systems for manufacturing was described. They indicated the way traffic-based disruptions can affect industry controls, namely the planning pace of applications used by customers. Wang et al., (2021) suggested that the nation's industry control mechanisms constitute its lifeblood. As such, industry control mechanisms communication recognition of anomalies constitutes a crucial undertaking. With immediate instruction, it can provide precise forecasts given unfamiliar or irregularly dispersed information. Li and Niggemann (2020) examined that the automated factories were becoming more and more sophisticated; methods involving machine learning were used extensively to identify anomalous conditions in these machines. In artificial intelligence (AI), identifying anomaly activities might be seen as one-class issues. For such issues, geometrical approaches can offer a clear solution. Possible mishaps and financial harm can be avoided by identifying irregularities utilizing these indications. Multimodal time series information presents a novel difficulty for recognizing anomalies since it necessitates taking seasonal and parameter correlations into account at the same moment. Wang et al., (2019) presented the study using AI approaches for identifying anomalies in automation systems. The current body of knowledge can be separated into two groups: industry network-specific instructional techniques and data-based instruction, depending on the characteristics that define controlling systems.

3. METHODOLOGY

The multifaceted task of identifying abnormalities in automated factories necessitates the application of advanced technology and approaches. The creation and application of efficient detection systems for anomaly detection is essential to maintain productivity, reduce interruptions and protect the confidentiality of manufacturing procedures as companies advance. Figure 1 depicts the flow of the suggested methodology

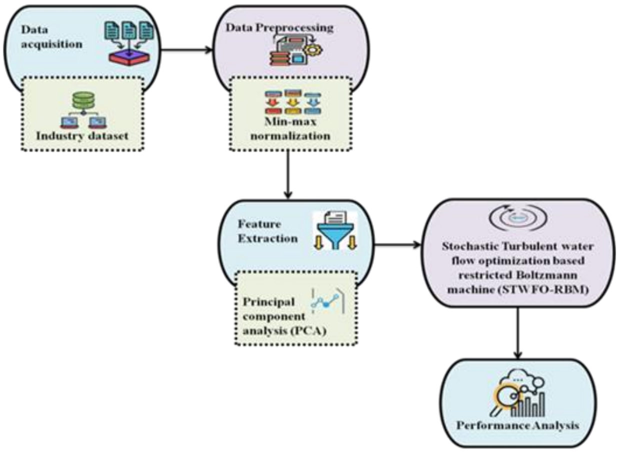
Data acquisition
Industry dataset
Data Preprocessing
Min-max normalization
Feature Extraction
Principal component analysis (PCA)
Stochastic Turbulent water flow optimization based restricted Boltzmann machine (STWFO-RBM)
Performance Analysis

Figure 1. Flow of methodology.

3.1 Dataset

The research consists of 9, 46,722 observations total from the complete SWaT database have fifty-one features classified into standard and attacking categories. That resulted in the collection of 4, 96,800 data during seven days of regular operations and 4, 49,919 data during a total of four days of continuous activity involving 32 assaults correspondingly. These four attacker circumstances: 1) lonely Staging Lone Points, 2) lonely Staging Multiple Pointed, 3) Multiple Staging Solo Pointed and 4) Multiple Phase Multiplied Points, yielded 54,584 attacker instances with varying dates (Krithivasan et al., (2020)).

3.2 Data preprocessing using min-max normalization

A linear modification is applied to the original set of data using the Min-Mix Normalization procedure. It maintains the connections between the original data. An easy method called min-max normalization allows information to be fitted in a predetermined border that has a predetermined border. Using the Min-Max normalization method as shown in Eq. (1)

$$B' = \left(\frac{B - value\ of\ B}{value\ of\ B - value\ of\ B}\right) * (C - D) + D \qquad (1)$$

Whereby B' contains one of the Min-Max normalized pieces of data. If $[C]$determines the predetermined border and if $B\ is$ an initial information area, B is newly translated information.

3.3 Feature extraction using Principal component analysis (PCA)

A popular approach to statistics for presenting information and minimizing dimensionality is the analysis of principal components. It enables to display of high-dimensional information in a lower-dimensional manner, allowing users to analyze as well as decipher the fundamental frameworks and trends. Finding the paths (principal parts) in the information across where the variation is the greatest constitutes PCA such main parts have no relationship because they're perpendicular to one another. With the first primary element describing the greatest amount of diversity of the available data, each subsequent item captures as much of the remaining variability as it possibly can. By relocating the initial information onto a fresh system of coordinates determined by the primary parts, PCA can reduce the dimensions of the information. The key components of the initial database are kept whereas the less significant ones are removed in the converted data. This decrease in dimensionality can be helpful for a variety of tasks, including data visualization, decreasing noise and accelerating future processes.

These modifications change the suggested value of the variables on an array from 0 to 1. The construction of a three-correlation matrix A for every selected normalization factor is necessary since the principal components rely on the relationship or similarity matrix. Since the weightings of every PC are derived through the eigenvalue of correlation matrices, As a result, the PCA values for this weight's nonlinear mixing don't consist of zeros or ones. The correlation matrices contain a collection of o eigenvectors:

$o\ \{f_1, f_2, \ldots . f_o\}$And o were parameters of$\{\lambda_1, \lambda_2, \ldots . \lambda_o\}$.

$$Z_1 = f_{11}V_1 + f_{21}V_2 + \cdots . f_{o1}V_o\ Z_2 = f_{12}V_1 + f_{22}V_2 + \cdots . f_{o2}V_o\ \cdots\cdots\cdots\cdots\cdots\cdots\ Z_o = f1oV_1 + f_{2o}V_2 + \cdots . f_{oo}V_o \tag{2}$$

It established the $PC\ z\ 1$ following every PC was created using its eigenvalue as the linear combination of measurements, resulting in the kth eigenvector$fk = (f1k, f2k, ok)$. They examine it since the variables in the problems $|B\ K| = 0$ provide problems with a trio of harmonics as a response, suggesting that options are feasible. The Eigen value that follows eigenvector B is those roots. Every single value of B has a matching scale position in the order of descending.

$$B = [V\ \ldots\ V\ \ \vdots \ddots \vdots\ \ \ldots\ ] \tag{3}$$

The eigenvalue of these Eigenvectors is driven by this matrices equation, which is calculated where all selected indications $(R\ K)\ =\ ek$ for wherein f is an eigenvector that corresponds to j with the characteristic that $e\ *\ e\ '\ =\ 1$ and where $e = [e_1, e_2 \ldots e_3]$. As a result, the eleven Eigenvectors $e1, e2, and\ e3$ maintain a relationship of 1 > 2 > 3. The next step is to calculate the eleven primary elements using the normalized indicator's weighted eigenvector with the associated eigenvalue of 1, 2 and 3.

$$O_{1I} = v_I e_1\ \cdots\cdots\ O_{9i} = v_i e_3 \tag{4}$$

For nation k, $e_i = [e_{I1}, e_{I2} \ldots e_3]$ is a standardized vector indication. The first main element exhibits the biggest difference in the initial indications, whereas the subsequent principal element exhibits the greatest variability in other signals. Maximizing variations makes it easier to get the greatest amount of data from all of the chosen variables. As it is practical, calculations are made of the total number of indicators of liquid vulnerability of liquid fuel accessibility, its total fluctuation, or its key components. The primary constituents of electricity are simultaneously orthogonal. Consequently instance $\lambda_I = var(O_I)$. It is important to note that J = var (PJ) and that $1\ +\ 2\ +\ 3\ =\ total$ variance in ETIPCA. As an outcome, the conclusion $J///J$ corresponds to the percentage of the overall variability that PJ accounts. The balanced total of the ETIPCA index is in 11 main elements, wherein the amount of weight is the variations of subsequent main elements that the last stage is done during the calculation. So, the sum is $1\ +\ 2\ +\ 3\ =\ 0$ variation is evaluated using Eq. (5).

$$FSJ_{ODB} = \frac{\lambda_1 O_{1I} + \lambda_2 I_2 O_{1I} + \lambda_3 3 O_3}{\lambda_1 + \lambda_2 + \lambda_3} \tag{5}$$

Since the weighted average of the normalized descriptions of each power indication makes it possible to calculate the ETIPCA ranking scores for this research, that balanced component's straightforward presentation of the various energy indications serves to demonstrate the comparative importance of every single energy indication. The present research uses range choice matrices to estimate energy efficiency, followed by PCA to quantify the impact of each of the energy trireme factors for purposes of ranking. The longevity of the results and the proximity given by the intermediary decision matrix plus PCA generate a pertinent indication for the decision-makers.

3.4 Stochastic Turbulent water flow optimization based restricted Boltzmann machine (STWFO-RBM)

3.4.1 Stochastic Turbulent Water Flow Optimization (STWFO)

Stochastic Turbulent water flow optimization (STWFO) presents possibilities and problems in a variety of applications, such as pipes, pathways, motors and monitoring of the atmosphere. It is distinguished by its turbulence and unpredictability. Figure 2 depicts the flowchart of the proposed STWFO. The nuances of this issue necessitate a sophisticated strategy to maximize effectiveness, minimize operating expenses and lessen the adverse environmental effects. When water rushes turbulently, it forms a circular shape and affects the effect of gravity, causing the fluid to follow a circular route. The angle of citation is shown in Eq. (6);

$$\delta_j^{new} = \delta_j + rand_1 * rand_2 * \pi \tag{6}$$

The waves that are the smallest weighted space among everything else were shown to simulate and determine the furthest and closest Whirlpools were shown in Eq. (7);

$$\Delta_s = e(Wh_s) * (Wh_s - sum(W_j)|^{0.5} \tag{7}$$

$$\Delta W_s = \cos\left(\delta_j^{new}\right) * rand(1, C) * \left(Wh_e - W_j\right) - \sin\left(\delta_j^{new}\right) * rand(1, C) * (Wh_x - W_j)) * (1 + |\,\mathrm{COS}\left(\delta_j^{new}\right) - \sin\left(\delta_j^{new}\right)|) \tag{8}$$

$$W_j^{new} = Wh_i - \Delta W_s \tag{9}$$

A centrifugal force is represented by the framework shown in (10) that happens at randomness in a single of the choice factors' dimensions. As seen in Eq. (10), a centrifugal force is calculated using the position created by the whirling and the item. If the resulting force exceeds an unknown amount in the interval [0, 1], the rotational activity is carried out in a predetermined dimension, which is illustrated in Eq. (11). In mathematics, the situation can be stated in the following manner:

$$FE_j = ((\cos(\delta_j^{new}))^2(\sin(\delta_j^{new}))^2)^2 \qquad (10)$$

$$W_{j.o} = W_o^{min} + rand * (W_o^{max} - W_o^{min}) \qquad (11)$$

The vortices clash and push against one another as well. These phenomena can be described in terms of how whirlpools affect things, with each Whirlpool tending to draw into additional whirlpools and exert centrifugal forces on them. Algorithm 1 denotes the procedure of STWFO. The nearest Whirlpools could be expressed by computing the minimal sum with the desired operations as seen in (12). After that, the location in the Whirl can be modified by (13) and (14):

$$\Delta_s = e(Wh_s) * |Wh_s - sum(Wh_s)| \qquad (12)$$

$$\Delta Wh_i = rand(1.C) * \left|\cos(\delta_j^{new}) + \sin(\delta_j^{new})\right| * (Wh_e - Wh_i) \qquad (13)$$

$$Wh_j^{new} = Wh_e - \Delta Wh_i \qquad (14)$$

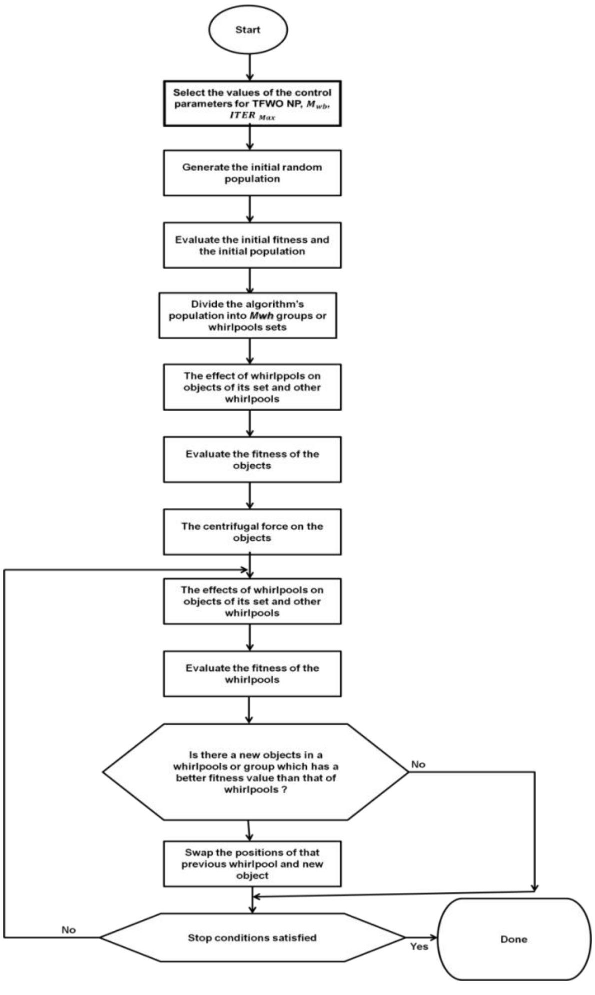
Start
Select the values of the control parameters for TFWO NP, M_{wb}, $ITER_{Max}$
Generate the initial random population
Evaluate the initial fitness and the initial population
Divide the algorithm's population into *Mwh* groups or whirlpools sets
The effect of whirlppols on objects of its set and other whirlpools
Evaluate the fitness of the objects
The centrifugal force on the objects
The effects of whirlpools on objects of its set and other whirlpools
Evaluate the fitness of the whirlpools
Is there a new objects in a whirlpools or group which has a better fitness value than that of whirlpools ?
No
Swap the positions of that previous whirlpool and new object
No
Stop conditions satisfied
Yes
Done

Figure 2. Flowchart of proposed STWFO.

Algorithm 1: STWFO

```
#Apply the turbulence formulas to assess the intended value
#Determine which people are suitable for procreation
#utilizes crossovers and mutations to establish a completely novel population
#Analyze the freshly created population's viability
#Change out the current demographic for the one that came before
#Iterations indicator with increments
#Give back the finest resolution you were able to find
```

3.4.2 Restricted Boltzmann machine (RBM)

Every layer vertices have links to one another however nodes interconnections inside a particular layer do not exist. The durability of links among levels is determined by the pounds assigned to them. RBMs analyze information and identify trends by using a stochastic methodology. To identify root causes and correlations, the framework modifies the weightings in learning according to the information that is provided. Figure 3 depicts the graphical model of RBM linkages employing symmetrical weighting among hiding as well as transparent entities. Reducing the disparity between the information drawn from the simulator and the exists is a key component of the procedure for learning. RBM-related temperature significance of RBM appears to be allocated functions;

$$F(u,h) = g^S Xu - u^S a^u - g^S a^g \qquad (15)$$

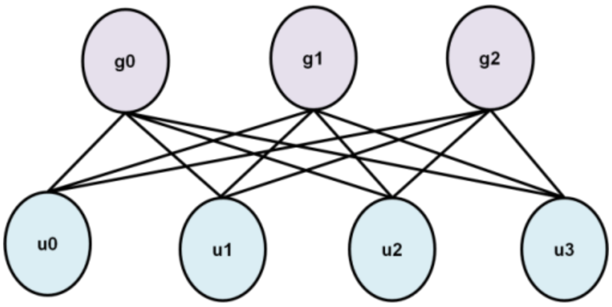

Figure 3. Graphical model of RBM

The aforementioned energy function defines likelihood distributions across exposed as well as concealed variables.

$$O(u,h) = \frac{1}{y} f^{-F(u,g)} \qquad (16)$$

With,

$$Y = \sum_{u' \epsilon\, v} \sum_{g' \epsilon \mathrm{H}} f^{-F(u',g')} \qquad (17)$$

Through exclusionary across any potential concealed vector arrangements one can determine the chance distributions for a transparent direction. The tractability of the residual denominator represents particular features of the RBM.

$$O(u) = \frac{1}{y} \sum_{g' \epsilon H} f^{-F(u',g')} = \frac{1}{Y} f^{-E(u)} \qquad (18)$$

With

$$E(u) = -u^S a^u - \sum_{j=1}^{1} Soft_{+}(X_j\, u + a_j^g) \quad (19)$$

As computational models, RBMs are sometimes trained to place an elevated likelihood (lower cost) on teaching data and a small likelihood on non-training information. Reducing the median to a negative logarithm probability given a group of cases constitutes a single strategy.

$$e(\ominus, C) = \frac{1}{M}\sum_{m=1}^{M} -In\; o(u_m) \quad (20)$$

$$\nabla_p e(\ominus, C) = \frac{1}{M}\sum_{n=1}^{M} \nabla_\theta E(u_m) - \sum_{u' \epsilon V} O(u')\nabla_\theta\, E(u') \quad (21)$$

Where

$$\nabla_x E(u) = -F[g|u]u^S = -\overset{\frown}{g}\,(u)u^S \quad (22)$$

$$\nabla_{ag} E(u) = \; -F[g|u] = -\overset{\frown}{g}\,(u) \quad (23)$$

$$\nabla_{au} E(u) = -u \quad (24)$$

It makes sense that the optimistic stage increases the likelihood that instances come from the training materials we provide and the adverse stage decreases the likelihood that instances be produced through the algorithm. The adverse phases become insurmountable, comparable to the division formula.

$$\nabla_p e(\ominus, C) = \frac{1}{M}\sum_{n=1}^{M} \nabla_\theta E(u_m) - \frac{1}{T}\sum_{t=1}^{T} \nabla E(\acute{u}_t) \quad (25)$$

Additionally, mini-batch training is usual, which entails changing the initial positive mean after every practice iteration with an additional one across a tiny portion of the exercise batch.

4. RESULTS

Anomalies in industrial automation systems are identified through real-time monitoring and analysis of operational data, utilizing machine learning algorithms to detect deviations from normal behavior, ensuring early intervention and system reliability. In this paper, we have used STWFO-RBM as a proposed method and existing methods are support vector machine random forest (SVM-RF) (Anton et al., (2019)), long short-term memory (LSTM) (Lindemen et al., (2020)) and convolutional neural network (CNN) (Hu et al., (2019)).

An elevated accuracy of proportion suggests the algorithm has done a good job of differentiating between typical and unusual behaviors. Certainty, however, cannot be the sole variable to be considered regard, particularly if working with imbalanced collections that contain a significant amount of common scenarios along with anomalies. Accuracy is an essential measure for assessing the effectiveness of computerized buildings' unusual behavioral detection techniques, but it's essential to consider additional parameters, particularly while utilizing incomplete information. Figure 4 and Table 1 depict the value of STWFO-RBM occurred at 97% in accuracy which is higher than the SVM-RF obtained at 80%, LSTM revealed at 90% and CNN occurred at 92%.

Table 1. Numerical outcomes of accuracy.

Methods	Accuracy (%)
SVM - RF	80
LSTM	90
CNN	92
STWFO-RBM (Proposed Methods)	97

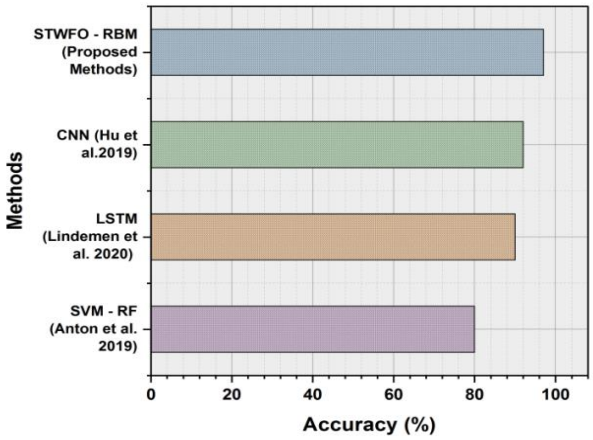

Figure 4. Performance analysis of accuracy.

The F1 score is relevant for examining the ratio of normal to abnormal events. Regular operating trends tend to be more common than aberrant incidents in a manufacturing environment. As a result, while a simulation that labels everyone as typical can attain a high F1 score, it can lose significant abnormalities. The F1 score takes into account either inaccurate results or fake negatives, allowing for rectifying that disparity. Table 2 and figure 5 illustrate the value of STWFO-RBM in an F1 score obtained 96%, SVM-RF 85%, LSTM presented 80% and CNN obtained 90%.

Table 2. Numerical outcomes of F1 score.

Methods	F1 score (%)
SVM - RF	85
LSTM	80
CNN	90
STWFO-RBM (Proposed Methods)	96

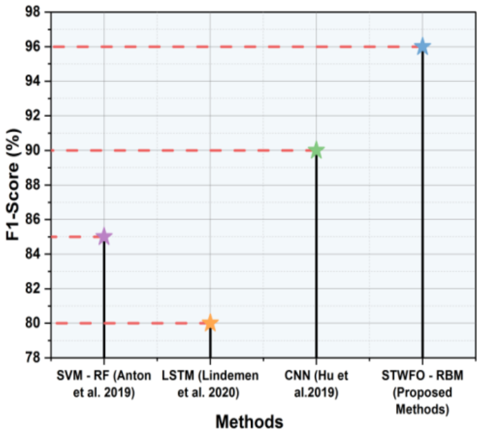

Figure 5. Performance analyses of F1 score.

When referring to the reliability of the approach to anomaly detection in recognizing positive results amongst the occurrences as it identifies for deviations, sharpness in the setting of recognizing irregularities in automated processes is used. Precision was an important indicator since it evaluates the equipment's dependability as a means of reducing false alarms. Reaching excellent precision is necessary to guarantee that anomalies reported by the computer system are real problems that need to be fixed. Conversely, poor precision can cause false warnings, which would use resources and increase costs for upkeep and unavailability. The value of precision in STWFO-RBM obtained 98% efficiently then the SVM-RF obtained 87%, LSTM revealed 93% and CNN occurred 90% as shown in Table 3 and figure 6.

Table 3. Numerical outcomes of precision.

Methods	Precision (%)
SVM - RF	87
LSTM	93
CNN	90
STWFO-RBM (Proposed Methods)	98

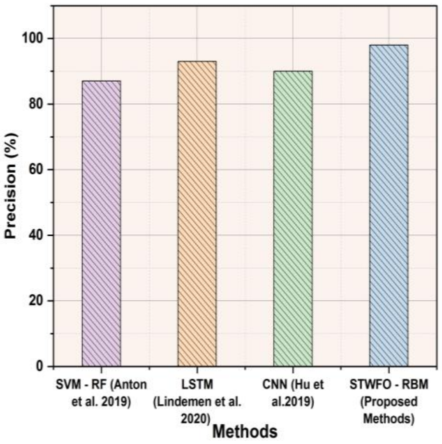

Figure 6. Performance analysis of precision.

The capacity of an organization to recognize and recover cases of abnormalities or unusual activity amongst every one of the actual cases of abnormalities for the framework is referred as anomaly recalls of identifying irregularities in automation systems for industry. It serves as an essential statistic for assessing how well anomalous detectors are working, particularly in sectors wherein losing their abnormalities or inaccurate results might have dire repercussions. Table 4 and figure 7 depict the value of recall for STWFO-RBM observed at 95%, SVM-RF explored at 86%, LSTM presented at 90% and CNN obtained at 80%.

Table 4. Numerical outcomes of recall.

Methods	Recall (%)
SVM - RF	86
LSTM	90
CNN	80
STWFO-RBM (Proposed Methods)	95

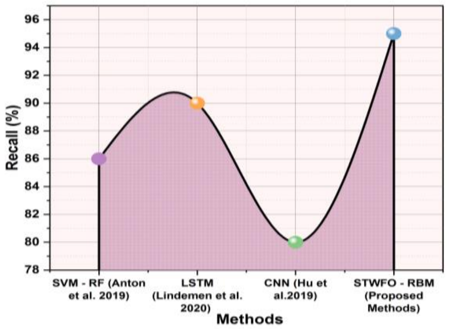

Figure 7. Performance analysis of recall.

In a production setting, a variety of instruments and sensors produce enormous volumes of data, which must be monitored and analyzed to identify irregularities in the system's operation. So this sense, computing effort means the amount of effort needed for processing and analyzing the information to find anomalies or departures from the anticipated pattern. For factories to continue operating reliably, safely, as well as efficiently, finding anomalies must be done effectively. Table 5 and figure 8 illustrate the value of computational time for STWFO-RBM obtained at 6.1s, SVM-RF demonstrated at 8.6s, LSTM presented at 10.0s and CNN occurred at 8.5s.

Table 5. Numerical outcomes of computational time.

Methods	CT
SVM - RF	8.6s
LSTM	10.0s
CNN	8.5s
STWFO-RBM (Proposed Methods)	6.1s

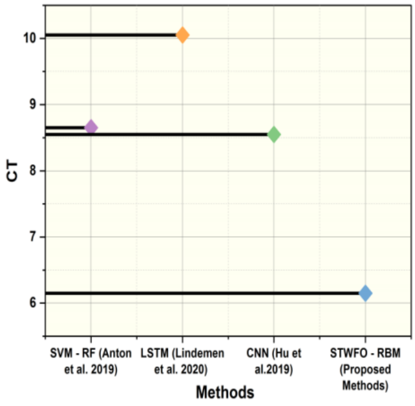

Figure 8. Performance analysis of computational time.

5. CONCLUSION

The efficient identification of irregularities in automated manufacturing technologies is crucial for guaranteeing the seamless functioning, dependability, along security of production procedures. The speed at which the equipment can quickly and precisely detect departures from usual conduct is affected by the effectiveness of those computing operations. The numerical outcomes of STWFO-RBM work efficiently and give better results than the other existing methods, STWFO-RBM occurred 97% in accuracy, obtained 96% of F1 score, discovered 98% of precision, revealed 95% of recall and presented 6.1s of computational time. In commercial environments, when quick reactions to irregularities can reduce possible dangers, avoid machinery breakdowns and improve the system's general efficiency, immediate time tracking of anomalies is important. It is challenging to develop and implement methods that blend computation speed with accuracy, in rapidly evolving sectors. The expenditures of installing computing facilities learning and upgrading designs as well as getting and keeping detectors play a part in the deployment and upkeep of an efficient detectable anomaly system. For certain commercial purposes, those costs can be prohibitive, especially among startups. Upcoming anomaly identification solutions are going to use algorithms that use AI collaborating alongside humans as part of a people-machine partnership. Further advances and integrations will bring the creation of sophisticated sensors that are able to provide information that becomes more varied and detailed. Technologies for detecting anomalies will develop so they may anticipate possible problems ahead of them that arise in addition to recognizing present abnormalities.

References:

Ahmed, C.M., MR, G.R. and Mathur, A.P. (2020, October). Challenges in machine learning based approaches for real-time anomaly detection in industrial control systems. In Proceedings of the 6th ACM on cyber-physical system security workshop (pp. 23-29). doi:https://doi.org/10.1145/3384941.3409588

Anton, S.D.D., Sinha, S. and Schotten, H.D., (2019, September). Anomaly-based intrusion detection in industria data with SVM and random forests. In 2019 International conference on software, telecommunications and computer networks (SoftCOM) (pp. 1-6). IEEE. doi:https://doi.org/10.23919/SOFTCOM.2019.8903672

Bayram, B., Duman, T. B., & Ince, G. (2021). Real time detection of acoustic anomalies in industrial processes using sequential autoencoders. Expert Systems, 38(1), e12564.doi:https://doi.org/10.1111/exsy.12564

Choi, K., Yi, J., Park, C. and Yoon, S., (2021). Deep learning for anomaly detection in time-series data: review, analysis, and guidelines. IEEE Access, 9, pp.120043-120065. doi:https://doi.org/10.1109/ACCESS.2021.3107975

Das, T.K., Adepu, S. and Zhou, J., (2020). Anomaly detection in industrial control systems using logical analysis of data. Computers & Security, 96, p.101935. doi:https://doi.org/10.1016/j.cose.2020.101935

De Vita, F., Bruneo, D. and Das, S.K., (2020, April). A novel data collection framework for telemetry and anomaly detection in industrial iot systems. In 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 245-251). IEEE. doi:https://doi.org/10.1109/IoTDI49375.2020.00032

Demertzis, K., Iliadis, L., Tziritas, N. and Kikiras, P., (2020). Anomaly detection via blockchained deep learning smart contracts in industry 4.0. Neural Computing and Applications, 32, pp.17361-17378. doi:https://doi.org/10.1007/s00521-020-05189-8

Ding, S., Morozov, A., Vock, S., Weyrich, M. and Janschek, K., (2020). Model-based error detection for industrial automation systems using lstm networks. In Model-Based Safety and Assessment: 7th International Symposium, IMBSA 2020, Lisbon, Portugal, September 14–16, 2020, Proceedings 7 (pp. 212-226). Springer International Publishing. doi:https://doi.org/10.1007/978-3-030-58920-2_14

Genge, B., Haller, P. and Enăchescu, C., (2019). Anomaly detection in aging industrial internet of things. IEEE Access, 7, pp.74217-74230. doi:https://doi.org/10.1109/ACCESS.2019.2920699

Ghazal, M., Basmaji, T., Yaghi, M., Alkhedher, M., Mahmoud, M. and El-Baz, A.S., (2020). Cloud-based monitoring of thermal anomalies in industrial environments using AI and the internet of robotic things. Sensors, 20(21), p.6348. doi:https://doi.org/10.3390/s20216348

Gupta, K., & Muzakkir, S. M. (2023). A Model for Prediction of Outer Race Defects of Rolling Contact Bearing based on Vibration Data Using Machine Learning Algorithms. Tribology in Industry, 45(4), 676–685. https://doi.org/10.24874/ti.1540.09.23.11

Gupta, K., & Muzakkir, S. M. (2023). Prediction of Gearbox oil degradation based on online sensor data and machine learning algorithms. Tribology in Industry, 45(3), 487–502. https://doi.org/10.24874/ti.1491.06.23.08

Haller, P., Genge, B. and Duka, A.V., (2019). On the practical integration of anomaly detection techniques in industrial control applications. International Journal of Critical Infrastructure Protection, 24, pp.48-68. doi:https://doi.org/10.1016/j.ijcip.2018.10.008

Hao, W., Yang, T. and Yang, Q., (2021). Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems. IEEE Transactions on Automation Science and Engineering. doi:https://doi.org/10.1109/TASE.2021.3073396

Hsieh, R.J., Chou, J. and Ho, C.H., (2019, November). Unsupervised online anomaly detection on multivariate sensing time series data for smart manufacturing. In 2019 IEEE 12th conference on service-oriented computing and applications (SOCA) (pp. 90-97). IEEE. doi:https://doi.org/10.1109/SOCA.2019.00021

Hu, Y., Zhang, D., Cao, G. and Pan, Q., (2019, October). Network data analysis and anomaly detection using CNN technique for industrial control systems security. In 2019 IEEE International conference on systems, man and cybernetics (SMC) (pp. 593-597). IEEE. doi:https://doi.org/10.1109/SMC.2019.8913895

Huang, H., Yang, L., Wang, Y., Xu, X. and Lu, Y., (2021). Digital twin-driven online anomaly detection for an automation system based on edge intelligence. Journal of Manufacturing Systems, 59, pp.138-150. doi:https://doi.org/10.1016/j.jmsy.2021.02.010

Huong, T.T., Bac, T.P., Long, D.M., Luong, T.D., Dan, N.M., Thang, B.D. and Tran, K.P., (2021). Detecting cyberattacks using anomaly detection in industrial control systems: A federated learning approach. Computers in Industry, 132, p.103509. doi:https://doi.org/10.1016/j.compind.2021.103509

Kim, G.Y., Lim, S.M. and Euom, I.C., (2022). A study on performance metrics for anomaly detection based on industrial control system operation data. Electronics, 11(8), p.1213. doi:https://doi.org/10.3390/electronics11081213

Kim, S., Jo, W. and Shon, T., (2020). APAD: Autoencoder-based payload anomaly detection for industrial IoE. Applied Soft Computing, 88, p.106017. doi:https://doi.org/10.1016/j.asoc.2019.106017

Krithivasan, K., Pravinraj, S. and VS, S.S., (2020). Detection of cyberattacks in industrial control systems using enhanced principal component analysis and hypergraph-based convolution neural network (EPCA-HG-CNN). IEEE Transactions on Industry Applications, 56(4), pp.4394-4404. doi:https://doi.org/10.1109/TIA.2020.2977872

Kumar, V., Tewari, R. P., Pandey, R., & Rawat, A. (2023). Triboinformatic modeling of wear in total knee replacement implants using machine learning algorithms. Journal of Materials and Engineering, 1(3), 97–105. https://doi.org/10.61552/jme.2023.03.001

Leander, B., Marković, T., Čaušević, A., Lindström, T., Hansson, H. and Punnekkat, S., (2022, October). Simulation environment for modular automation systems. In IECON 2022–48th Annual Conference of the IEEE Industrial Electronics Society (pp. 1-6). IEEE. doi:https://doi.org/10.1109/IECON49645.2022.9968835

Li, P. and Niggemann, O., (2020). Non-convex hull based anomaly detection in CPPS. Engineering Applications of Artificial Intelligence, 87, p.103301. doi:https://doi.org/10.1016/j.engappai.2019.103301

Li, Z., Zhao, Y., Han, J., Su, Y., Jiao, R., Wen, X. and Pei, D., (2021, August). Multivariate time series anomaly detection and interpretation using hierarchical inter-metric and temporal embedding. In Proceedings of the 27th ACM SIGKDD conference on knowledge discovery & data mining (pp. 3220-3230). doi:https://doi.org/10.1145/3447548.3467075

Lindemann, B., Jazdi, N. and Weyrich, M., (2020, August). Anomaly detection and prediction in discrete manufacturing based on cooperative LSTM networks. In 2020 IEEE 16th International Conference on Automation Science and Engineering (CASE) (pp. 1003-1010). IEEE. doi:https://doi.org/10.1109/CASE48305.2020.9216855

Mokhtari, S., Abbaspour, A., Yen, K.K. and Sargolzaei, A., (2021). A machine learning approach for anomaly detection in industrial control systems based on measurement data. Electronics, 10(4), p.407. doi:https://doi.org/10.3390/electronics10040407

Nawaratne, R., Alahakoon, D., De Silva, D. and Yu, X.,(2019). Spatiotemporal anomaly detection using deep learning for real-time video surveillance. IEEE Transactions on Industrial Informatics, 16(1), 393-402. doi:https://doi.org/10.1109/TII.2019.2938527

Rosa, L., Cruz, T., de Freitas, M. B., Quitério, P., Henriques, J., Caldeira, F. and Simões, P., (2021). Intrusion and anomaly detection for the next-generation of industrial automation and control systems. Future Generation Computer Systems, 119, 50-67. doi:https://doi.org/10.1016/j.future.2021.01.033

Sapkota, S., Mehdy, A. K. M., Reese, S. and Mehrpouyan, H., (2020). Falcon: Framework for anomaly detection in industrial control systems. Electronics, 9(8), 1192. doi:https://doi.org/10.3390/electronics9081192

Wang, C., Wang, B., Liu, H.andQu, H., (2020). Anomaly detection for industrial control system based on autoencoder neural network. Wireless Communications and Mobile Computing, 2020, 1-10. doi:https://doi.org/10.1155/2020/8897926

Wang, Q., Chen, H., Li, Y. and Vucetic, B., (2019). Recent advances in machine learning-based anomaly detection for industrial control networks. In 2019 1st International Conference on Industrial Artificial Intelligence (IAI), (pp. 1-6), IEEE. doi:https://doi.org/10.1109/ICIAI.2019.8850828

Wang, W., Wang, Z., Zhou, Z., Deng, H., Zhao, W., Wang, C. and Guo, Y., (2021). Anomaly detection of industrial control systems based on transfer learning. Tsinghua Science and Technology, 26(6), 821-832. doi:https://doi.org/10.26599/TST.2020.9010041

Ranganathaswamy Madihalli Kenchappa
JAIN (Deemed-to-be University),
Ramanagara District, Karnataka,
India
mk.ranganatha@jainuniversity.ac.in
ORCID 0000-0001-7387-839X

Rakesh Kumar Yadav
Maharishi University of Information
Technology, Uttar Pradesh,
India
rkymuit@gmail.com
ORCID 0000-0002-0151-4981

Alka Singh
Noida Institute of Engineering
&Technology, Greater Noida, Uttar
Pradesh, India
alka@niet.co.in
ORCID 0009-0004-4891-436X

Arvind Kumar Pandey
Arka Jain University, Jamshedpur,
Jharkhand, India
dr.arvind@arkajainuniversity.ac.in
ORCID 0000-0001-5294-0190