Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Deep Learning and Metaheuristics based Cyber Threat Detection in Internet of Things Enabled Smart City Environment

Sonali Das
College of Agricultural Engineering and Technology,Odisha
Yugandhar Manchala
Vardhaman College of Engineering,Telangana
Saroja Kumar Rout (rout_sarojkumar@yahoo.co.in)
Vardhaman College of Engineering,Telangana
Sujit kumar Panda
Gandhi Institute for Technology,Odisha

Research Article

Keywords: Smart cities, Internet of Things, Threat detection, Cybersecurity, Deep learning

Posted Date: July 12th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3141258/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Deep Learning and Metaheuristics based Cyber Threat Detection in Internet of Things Enabled Smart City Environment

Sonali Das[1[0009-0007-5258-5978]], Yugandhar Manchala[2[0000-0001-9895-7940]], Saroja Kumar Rout[3*[0000-0001-9007-3665]], Sujit kumar Panda[4[0000-0001-6295-2750]]

[1]Computer Science and Applications, College of Agricultural Engineering and Technology, Odisha University of Agriculture and Technology, Bhubaneswar, Odisha, India.

[2]Department of Information Technology, Vardhaman College of Engineering (Autonomous), Hyderabad, Telangana, India.

[3]Department of Information Technology, Vardhaman College of Engineering (Autonomous), Hyderabad, Telangana, India.

[4]Department of Computer Science & Engineering, Gandhi Institute for Technology, Bhubaneswar, India.

[1]sonalidas80@gmail.com,[2] yugandhar1230@gmail.com, [3]rout_sarojkumar@yahoo.co.in, [4]mail2sulin@gmail.com

Corresponding Author: Mr. Yugandhar Manchala, yugandhar1230@gmail.com

Abstract

Recently, the extensive use of Internet of Things (IoT) applications has a stronger impact and greater contribution to the development of the smart city. A smart city (SC) uses IoT-based technologies, applications, and communications for maximizing operational efficacy and improving the service quality of providers and the living standard of people. With the development of SC networks, there also comes the augmented menace of cybersecurity attacks and threats. IoT gadgets within an SC network were linked to sensors connected to huge cloud servers and are vulnerable to malicious threats and attacks. Therefore, it is significant to formulate techniques for preventing such assaults and protecting IoT gadgets from failures. This article develops a new transient search algorithm with optimal stacked sparse autoencoder (TSA-OSSAE) based cyber threat detection in IoT-enabled SC applications. The presented TSA-OSSAE technique majorly focuses on the recognition of cyber threats to attain security in the SC. To attain this, the projected TSA-OSSAE system follows TSA based feature selection approach to reduce computational complexity. Besides, the TSA-OSSAE technique applies the SSAE model for cyber threat detection. At last, the hyperparameters of the SSAE approach are optimally chosen by utilizing of multi-versus optimizer (MVO) algorithm. The experimental result analysis of the TSA-OSSAE technique was performed by using the TON_IoT telemetry database. The simulation outcomes signify the promising performance of the TSA-OSSAE methodology over other existing techniques.

Keywords: Smart cities; Internet of Things; Threat detection; Cybersecurity; Deep learning

1. Introduction

Currently, the growth of the Internet of Things (IoT) is extensively rising in societies all over the world. In 2017, the count of connected IoT gadgets had touched twenty-seven billion and such IoT gadgets would be drastically increased in market demand, thereby the potentiality was expected to reach nearly 1,25 billion in 2030. Several SC applications will be connecting numerous IoT gadgets to real-time objects, which certainly have very significant advantages to day-to-day life [1]. But the enormous number of IoT gadgets over different types of devices, services, protocols, and technologies (e.g., Bluetooth, Wireless, Satellites, Cellular, Wired, etc.) results in the perplexity of controlling future IoT networks [2]. Thus, such integration protocols with the internet cause serious cybersecurity menaces and susceptibilities for assaulting the data of the everyday routines of individuals' lives [3]. The IoT paradigm has resulted in the invention of smart cities. Fig. 1 demonstrates the overview of IoT for smart cities.

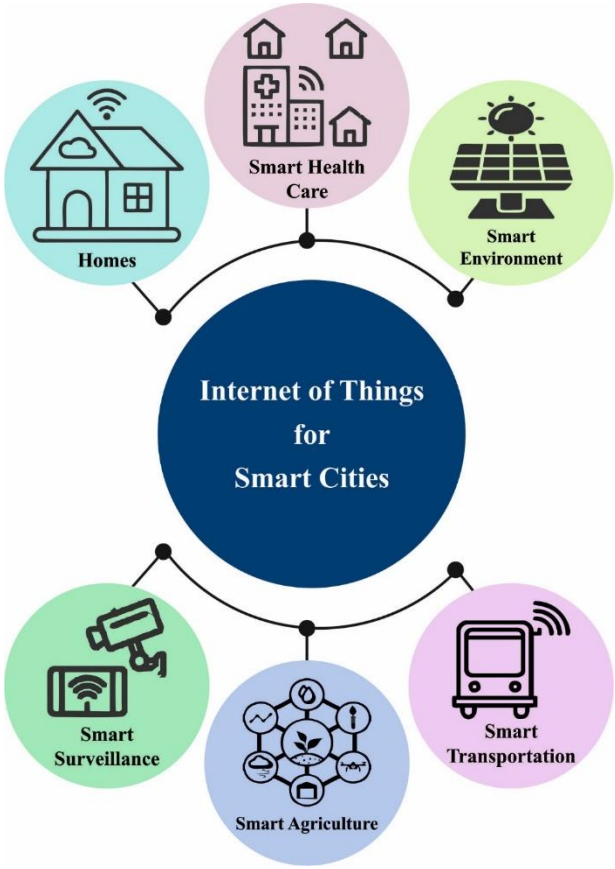

Fig. 1. Overview of IoT for smart cities

Smart cities work in real-time for promoting comfort and increasing the quality of life in cities [4]. The network traffic of smart cities through IoT systems has seen exponential growth and presents novel cybersecurity difficulties as these loT devices were linked to sensors that can be straightforwardly linked to enormous cloud servers. To mitigate such attacks, developers should advance novel methods to detect infected IoT gadgets [5]. The cyber threats could acquire unauthorized access to loT gadgets without the knowledge of the administrator or user (for example Miria botnet) [6]. The primary difficulty was how to find zero-day assaults since it occurs from various protocols of IoT gadgets in a cloud data center of SC, considering that the many assaults are hidden in IoT gadgets. Then the next challenge is how to detect a technique to intellectually identify cyberattacks from the IoT system formerly destructing smart cities [7].

Many loT sensors were recently collecting every data which passes via the huge data that is identified in cloud servers [8]. At present, conventional IDS was not devised for IoT networking devices, since such gadgets contain limited sources and fewer functionalities (e.g., smart locks, smart watches, smart lamps, and so on.). Nowadays, deep learning (DL) can be extensively utilized on data gathered by research scholars. DL refers to a type of artificial intelligence (AI) and machine learning (ML) that mimics similarly with that of the human mind used to study a specific subject and contains several applications in smart cities [9]. DL could incessantly monitor and collect data and assist the system to adapt to novel spaces. DL can be considered a branch of AI that aids neural networks in ML [10]. Currently, a comparison is made with conventional ML techniques, computer vision programs made important advancements in robotics, natural language processing, and other areas.

This article develops a new transient search algorithm with optimal stacked sparse autoencoder (TSA-OSSAE) based cyber threat detection in the IoT-based SC applications. The presented TSA-OSSAE technique majorly focuses on the recognition of cyber threats to attain security in the SC. To attain this, the projected TSA-OSSAE system follows TSA based feature selection approach to reduce computational complexity. Besides, the TSA-OSSAE technique applies the SSAE model for cyber threat detection. At last, the hyperparameters of the SSAE approach are optimally chosen by using of multi-versus optimizer (MVO) algorithm. The experimental outcome investigation of the TSA-OSSAE technique is performed utilizing the TON_IoT telemetry dataset.

2. Related Works

In [11], an SC intrusion detection infrastructure dependent upon Restricted Boltzmann Machines (RBMs) was presented. RBMs were executed because of their capability for learning higher-level features in raw data from an unsupervised method and controlling real data representation created in smart meters and sensors. Baig et al. [12] examine an ML-based technique to detect hijacking, GPS signal jamming, and DoS attack which is applied to oppose a drone. A comprehensive ML-based classifier of drone databases to the DJI Phantom 4 method, cooperating with either normal or malicious signatures is performed. In [13], intrusion detection has been obtained with a 3-stage data traffic investigation, reduction, and classifier approach employed for identifying positive trusted service requests against false requests which can take place from intrusion attacks. The solution implements a decision tree and deep belief from ML processes utilized for data reduction and classifier drives correspondingly. The infrastructure is validated with simulations for demonstrating the efficiency of solutions concerning intrusion attack recognition.

Shafiq et al. [14] presented a novel infrastructure method and hybrid technique for solving this problem. Primarily, the BoT-IoT identify database was executed and their 44 effectual attributes are elected in the number of attributes to ML technique. Afterward, the 5 effectual ML technique was selected to detect malicious and anomaly traffic identification and even choose the broadly utilized performance evaluation metrics of the ML techniques. In [15], a hybrid DL technique was formulated to detect DDoS and replay attacks in a real-time smart city platform. The hybrid method's performance can be assessed with the help of real-time SC data (smart soil, environmental, and Smart River), whereas replay and DDoS attacks are simulated.In order to protect the sensor network, it is essential to safeguard the powerful node through which the network is secured, cost-effective, and energy-efficient because Moving the anchor node plays a significant function throughout the localization process. [16]. In [17], a DL-related technique with recent databases can be used to classify the assaults. A safeguard was presented for the reputation of the IoT network and to make sure that it is only accessible to appropriate users. A base to incorporate IDS as an IoT-related network as an application was

presented. The authors in [18] devise a botnet detection mechanism related to a two-level DL structure to discriminate legitimate and botnet behaviors semantically at the application layer of domain name system (DNS) services. At the fundamental level of a framework, a Siamese network related to an already-existing threshold was used to choose the common DNS data across Ethernet connections, which was used to find how similar the DNS requests. Coming to the second level of the structure, the domain generation method compared with DL architectures will be recommended to categorize abnormal and normal domain names. The computing to improve IoT solutions for smarter cities by resolving some of its current problems and limitations. Internet of Things and cloud computing will enable smart cities to develop novel and enhanced services by utilising large amounts of data stored in the cloud and analysing it in real-time. [19].

3. The Proposed Model

In this article, a novel TSA-OSSAE approach was formulated for the detection and classification of cyber threats in IoT-enabled SC applications. The presented TSA-OSSAE technique majorly concentrates on the recognition of cyber threats to attain security in the SC.

3.1. Process involved in TSA-FS Technique

In this article, the presented TSA-OSSAE method follows TSA based feature selection approach to reduce computational complexity. The TSA technique is based on the transient behaviors of circuits that involve energy storage elements in their configuration [20]. Those behaviors are based on the circuit order, either first- or second-order circuits. The circuit order is defined by the count of energy storage capacitors, components, and inductors in the circuit schematic. This transient behavior comprises steady-state and transient parts. For first-order circuits, the differential equation defining the aforementioned behavior is formulated by Eq. (1).

$$\frac{d}{dt}x(t) + \frac{x(t)}{\tau} = K \tag{1}$$

This formula is resolved for $x(t)$ as a function of time:

$$x(t) = x(\infty) + \big(x(0) - x(\infty)\big)e^{\frac{-t}{\tau}} \tag{2}$$

In Eq. (2), $x(t)$ characterizes the inductor current or capacitor voltage. τ represents the time constant. K denotes a primary condition-dependent constant. $\chi(\infty)$ indicates steady-state χ value.

$$\frac{d^2}{dt^2}x(t) + 2\alpha\frac{d}{dt}x(t) + \omega_0^2 x(t) = f(t) \tag{3}$$

The preceding second-order differential equation is resolved by the following expression:

$$x(t) = e^{-\alpha t}\big(B_1 cos(2\pi f_d t) + B_2 sin(2\pi f_d t)\big) + x(\infty) \tag{4}$$

In Eq. (4), α indicates the damping coefficient, ω_0 and f_d represents the resonant and damped frequencies. B_1 and B_2 denotes an arbitrary constant. Like other optimization techniques, the primary step in the TSA is to set a random agent whose value lies between predetermined limits as follows:

$$Y = lb + rand \times (ub - lb) \tag{5}$$

Then, it examines the optimum solution employing the exploitation and exploration phases. The exploration stage was stimulated by the oscillatory response of the second-order circuit. Lastly, it obtains the optimum solution after a predetermined amount of iterations. Furthermore, the exploitation stage depends on the exponential decay of the first-order circuit and it is mathematically formulated by the subsequent equation:

$$Y_{l+1} = \begin{cases} Y_l^* + (Y_l - C_1.Y_l^*)e^{-T} & r_1 < 0.5 \\ Y_l^* + e^{-T}[cos(2\pi T) + sin(2\pi T)]|Y_l - C_1.Y_l^*| & r_1 \geq 0.5 \end{cases} \quad (6)$$

$$T = 2 \times a \times r_2 - a \quad (7)$$

$$C_1 = k \times a \times r_3 + 1 \quad (8)$$

$$a = 2 - 2\left(\frac{l}{L_{\max}}\right) \quad (9)$$

Now T, C_1, r_1, r_2, and r_3 indicates random numbers. Y_l and Y_l^* denotes the population and better population until the $l\text{-}th$ iterations, correspondingly k indicates the counter that begins from 0. The ending condition is that once the iteration reaches $L_{\max}$. Y_l^* corresponding to (∞). Furthermore, $B_1 = B_2 = |Y_l - C_1.Y_l^*|$. 'T' denotes a parameter that ranges from -2 to 2, which is utilized for balancing the exploitation and exploration procedures.

The fitness function (FF) used in the proposed method was created to achieve a balance between the maximum classifier accuracy attained by using minimal attributes and features, Eq. (10) denotes the FF for assessing solutions.

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \quad (10)$$

whereas $\gamma_R(D)$ indicates the classifier error rate of given classifiers, $|R|$ was the cardinality of the designated subset and $|C|$ was the total number of attributes in the data, α, and β were 2 variables respective to the import of classifier quality and subset length. $\in$ [1, 0] and $\beta = 1 - \alpha$.

3.2. SSAE based Cyber Threat Detection

At this stage, the TSA-OSSAE technique applies the SSAE model for cyber threat detection. The SSAE is a NN involved in numerous SAEs linked in end-to-end ways [21]. Higher-level feature representation of the input dataset has been achieved mainly due to the application of the findings of the previous layer's sparse self-encoder as the input of the next layer of self-encoding. In order to retrieve the optimised relation weight and bias values for the entire SSAE network, the greedy layer-by-layer pre-trained model was used to train all of the SSAE's layers sequentially. The error BP method was then designed to optimise the SSAE, although the achieved error function between the input and output information meets the predictable conditions, for receiving an optimal parameter as follows:

$$\frac{\partial}{\partial w_{ij}^r} J_{sparse}(W,b) = \frac{1}{2n_r}\sum_{r=1}^{n_r}\frac{\partial}{\partial w_{ij}^r} J_{sparse}\big(W,b,X(n),Y(n)\big) + \lambda w_{ij}^r \quad (11)$$

$$\frac{\partial}{\partial b^r} J_{sparse}(W,b) = \frac{1}{2n_r}\sum_{r=1}^{n_r}\frac{\partial}{\partial b^r} J_{sparse}\big(W,b,X(n),Y(n)\big) \quad (12)$$

Consequently, the upgraded method of the weight and bias were given below:

$$w_{ij}^k = w_{ij}^k - \eta\,\frac{\partial}{\partial w_{ij}^k} J(W,b) \quad (13)$$

$$b^r = br - \eta\,\frac{\partial}{\partial b^r} J(W,b) \quad (14)$$

From the expression, $X(n)$ and $Y(n)$ are denoted by the $n\text{-}th$ actual vector and reformation vector, and η represents the upgraded learning rate. Fig. 2 demonstrates the framework of SSAE model.

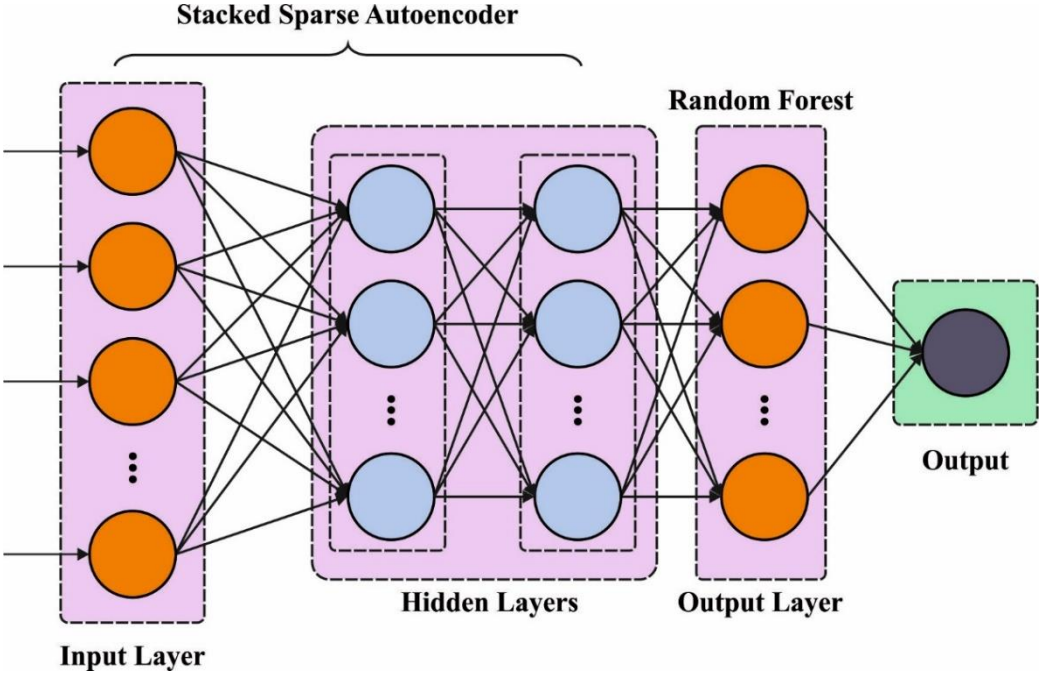

Fig. 2. Architecture of SSAE

Assuming sparse constraints in the SSAE approach, it is indispensable applied several rates of learning for different variables as diminishing frequency. However, the classic Gradient Descent (GD) system has mini-batch GD and SGD which apply undistinguishable learning rate for network parameter that should upgrade which generate the complexity for simply gaining the local minima and selecting the appropriate rate of learning.

3.3. Hyperparameter Tuning using MVO Algorithm

Finally, the hyperparameters of the SSAE algorithm are optimally selected by utilizing the MVO approach. The MVO algorithm is called a growing metaheuristic approach which tries to stimulate the laws of the multi-verse concept [22]. To upgrade the answer utilizing these methods, the rate of travel (TDR) and probability of wormhole existence (WEP) should be initially calculated. This parameter determines the magnitude and frequency of solution changes in the optimization algorithm as follows:

$$WEP = a + t \times \left(\frac{b-a}{T}\right) \tag{15}$$

The overall iteration number is T, equivalent to the minimal, b to the maximal, and t to the existing iteration.

$$TDR = 1 - \frac{t^{\frac{1}{P}}}{T^{\frac{1}{P}}} \tag{16}$$

p denotes the exploitation accuracy. P is the most important TDR measure. The emphasis on exploitation rises as the value of choice increases.

Update the solution position as follows:

$$x_i^j \begin{cases} \begin{cases} \chi_j + TDR + ((ub_j - lb_j) * r_4 + lb_j) & if r_3 < 0.5 \\ \chi_j - TDR + ((ub_j - lb_j) * r_4 + lb_j) & if r_3 \geq 0.5 \end{cases} & if\ r_2 < WEP \\ x^j_{roulette\ Wheel}\ if\ r_2 \geq WEP \end{cases} \tag{17}$$

In Eq. (17), χ_j is set to be $j\text{-}th$ elements from the best-predetermined individuals, WEP, TDR represents coefficients, lb_i and ub_i indicates the lower and upper limits of the $j\text{-}th$ elements, r_2, r_3, r_4 indicates arbitrary number ranges from [0,1], x_i^j signifies the $j\text{-}th$ variable in $i\text{-}th$ individuals, and $x_{roulette\ Wheel}^j$ does the roulette wheel selection model for picking the $j\text{-}th$ component of the solution. This formula is utilized for computing a novel solution location and compared to the best-in-class participant in WEP. If r_3, If a random value within [0,1], is lesser than 0.5, then the optimum solution value for $j\text{-}th$ parameter needs a solution. By rising WEP in the process of optimization, MVO rises the usage of the best solution.

The MVO method will improve a fitness function (FF) for attaining greater classifier outcomes. It resolves a positive value for designating the best performance of candidate results. In this study, the decreased classifier rate of errors was signified as the FF, as presented in Eq. (18).

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{no.of\ misclassified\ instances}{Total\ no.of\ instances} * 100 \quad (18)$$

4. Results and Discussion

The experimental validation of the TSA-OSSAE method was tested by exploiting the TON-IoT dataset [23]. Table 1 showcases a detailed description of the dataset.

Table 1 Details of the dataset

Label	Attack Type	No. of Records
A1	Backdoor	1000
A2	DDoS	1000
A3	DoS	1000
A4	Injection	1000
A5	MITM	1000
A6	Password	1000
A7	Ransomware	1000
A8	Scanning	1000
A9	XSS	1000
N	Benign	1000
Total Number of Attacks		**10000**

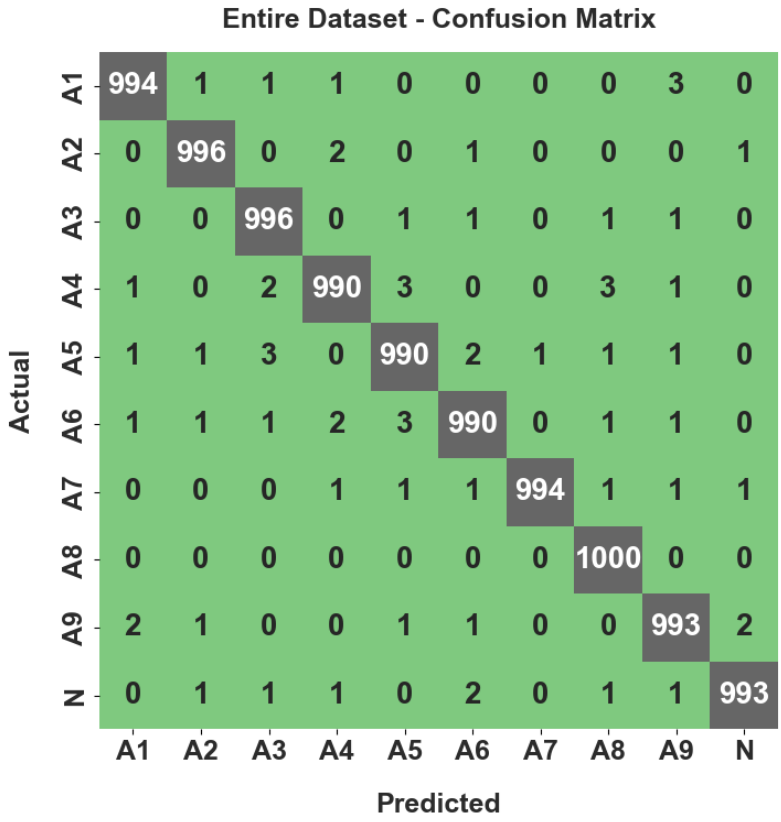

Fig. 3. Confusion matrix of TSA-OSSAE algorithm on the Entire database

The confusion matrices created by the presented TSA-OSSAE technique on the entire dataset are reported in Fig. 3. The figure demonstrated that the TSA-OSSAE method has categorized all the classes of cyber threats effectively and accurately.

Table 2 and Fig. 4 demonstrate an overall cyber threat classification performance of the TSA-OSSAE methodology on the entire database. The simulation values represented that the TSA-OSSAE approach has revealed enhanced performance under all classes. For sample, on class A1, the TSA-OSSAE algorithm has provided $accu_y$ of 99.89%, $prec_n$ of 99.50%, $reca_l$ of 99.40%, F_{score} of 99.45%, and MCC of 99.39%. Meanwhile, in class A5, the TSA-OSSAE technique has offered $accu_y$ of 99.81%, $prec_n$ of 99.10%, $reca_l$ of 99%, F_{score} of 99.05%, and MCC of 98.94%. Eventually, in class A9, the TSA-OSSAE method has rendered $accu_y$ of 99.84%, $prec_n$ of 99.10%, $reca_l$ of 99.30%, F_{score} of 99.25%, and MCC of 99.11%.

Table 2 Classification analysis of the TSA-OSSAE algorithm with different classes on the entire database

Entire Dataset					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	**MCC**
A1	99.89	99.50	99.40	99.45	99.39
A2	99.91	99.50	99.60	99.55	99.50
A3	99.88	99.20	99.60	99.40	99.33
A4	99.83	99.30	99.00	99.15	99.05
A5	99.81	99.10	99.00	99.05	98.94
A6	99.82	99.20	99.00	99.10	99.00
A7	99.93	99.90	99.40	99.65	99.61

A8	99.92	99.21	100.00	99.60	99.56
A9	99.84	99.10	99.30	99.20	99.11
N	99.89	99.60	99.30	99.45	99.39
Average	**99.87**	**99.36**	**99.36**	**99.36**	**99.29**

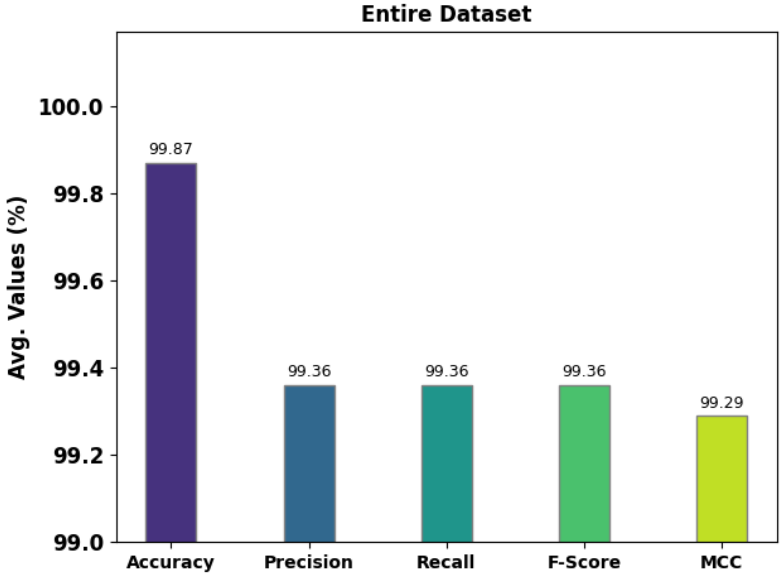

Fig. 4. Average outcome of TSA-OSSAE algorithm on the entire dataset

The confusion matrices produced by the proposed TSA-OSSAE technique on 70% of TRS have been revealed in Fig. 5. The figure illustrated the TSA-OSSAE system had classified every class of cyber threats accurately and effectively.

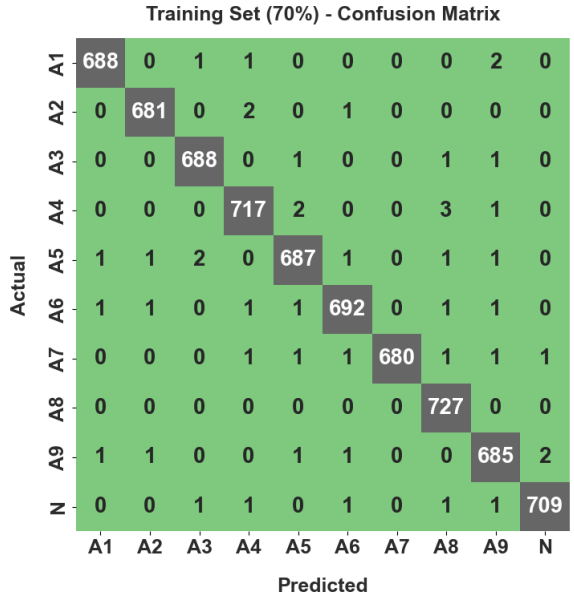

Fig. 5. Confusion matrix of TSA-OSSAE algorithm on 70% of TRS

Table 3 and Fig. 6 portray a complete cyber threat classification performance of the TSA-OSSAE system on 70% of TRS. The simulation values signified the TSA-OSSAE algorithm has displayed enhanced performance in every class. For example, in class A1, the TSA-OSSAE system has presented $accu_y$ of 99.90%, $prec_n$ of 99.57%, $reca_l$ of 99.42%, F_{score} of 99.49%, and MCC of 99.44%. In the meantime, on class A5, the TSA-OSSAE algorithm has rendered $accu_y$ of 99.81%, $prec_n$ of 99.13%, $reca_l$ of 98.99%, F_{score} of 99.06%, and MCC of 98.96%.

Finally, in class A9, the TSA-OSSAE approach has offered $accu_y$ of 99.80%, $prec_n$ of 98.85%, $reca_l$ of 99.13%, F_{score} of 98.99%, and MCC of 98.88%.

Table 3 Classifier outcome of TSA-OSSAE methodology with distinct classes under 70% of TRS

Training Set (70%)					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	**MCC**
A1	99.90	99.57	99.42	99.49	99.44
A2	99.91	99.56	99.56	99.56	99.51
A3	99.90	99.42	99.57	99.49	99.44
A4	99.83	99.17	99.17	99.17	99.07
A5	99.81	99.13	98.99	99.06	98.96
A6	99.84	99.28	99.14	99.21	99.12
A7	99.91	100.00	99.13	99.56	99.51
A8	99.89	98.91	100.00	99.45	99.39
A9	99.80	98.85	99.13	98.99	98.88
N	99.89	99.58	99.30	99.44	99.38
Average	**99.87**	**99.35**	**99.34**	**99.34**	**99.27**

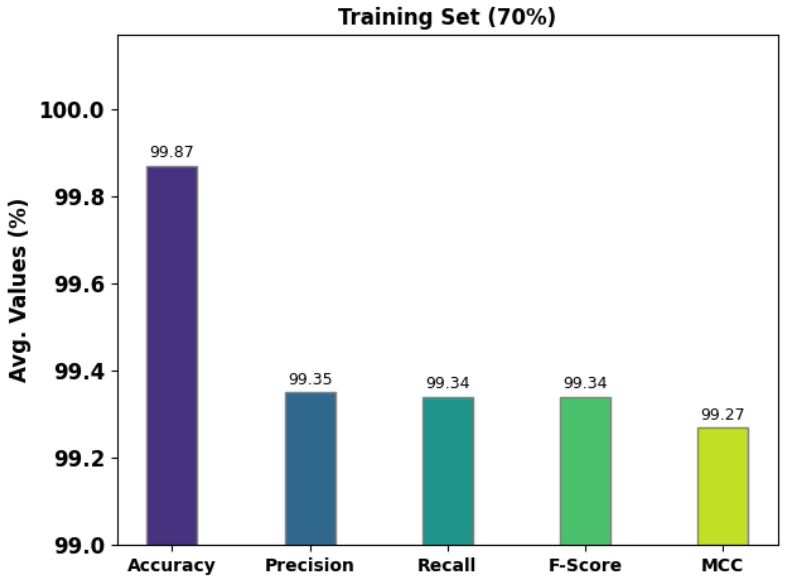

Fig. 6. Average outcome of TSA-OSSAE system on 70% of TRS

The confusion matrices generated by the presented TSA-OSSAE system on the 30% of TSS are given in Fig. 7. The figure designated the TSA-OSSAE methodology classified every class of cyber threats accurately and effectively.

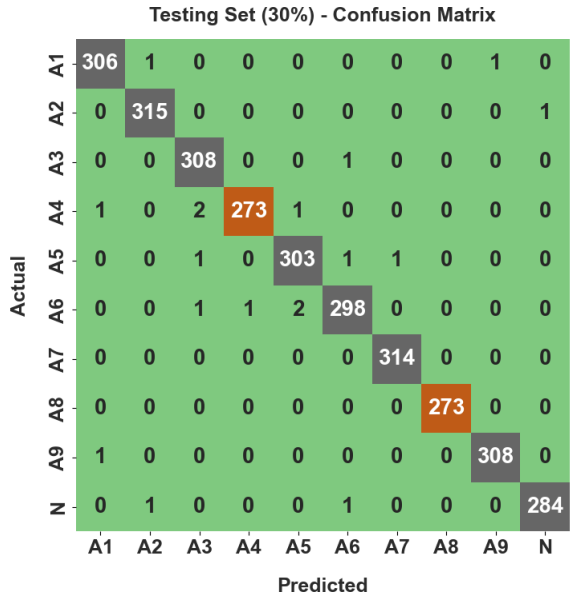

Fig. 7. Confusion matrix of TSA-OSSAE algorithm on 30% of TSS

Table 4 and Fig. 8 establish a complete cyber threat classification performance of the TSA-OSSAE approach on 30% of TSS. The simulation values represented by the TSA-OSSAE system have demonstrated improved performance in distinct classes. For example, in class A1, the TSA-OSSAE approach has projected $accu_y$ of 99.87%, $prec_n$ of 99.35%, $reca_l$ of 99.35%, F_{score} of 99.35%, and MCC of 99.28%. In the meantime, in class A5, the TSA-OSSAE methodology has presented $accu_y$ of 99.80%, $prec_n$ of 99.02%, $reca_l$ of 99.02%, F_{score} of 99.02%, and MCC of 98.91%. Finally, in class A9, the TSA-OSSAE method has offered $accu_y$ of 99.93%, $prec_n$ of 99.68%, $reca_l$ of 99.68%, F_{score} of 99.68%, and MCC of 99.64%.

Table 4 Classifier outcome of TSA-OSSAE scheme with various class labels on 30% of TSS

Testing Set (30%)					
Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	**MCC**
A1	99.87	99.35	99.35	99.35	99.28
A2	99.90	99.37	99.68	99.53	99.47
A3	99.83	98.72	99.68	99.19	99.10
A4	99.83	99.64	98.56	99.09	99.00
A5	99.80	99.02	99.02	99.02	98.91
A6	99.77	99.00	98.68	98.84	98.71
A7	99.97	99.68	100.00	99.84	99.82
A8	100.00	100.00	100.00	100.00	100.00
A9	99.93	99.68	99.68	99.68	99.64
N	99.90	99.65	99.30	99.47	99.42
Average	**99.88**	**99.41**	**99.39**	**99.40**	**99.34**

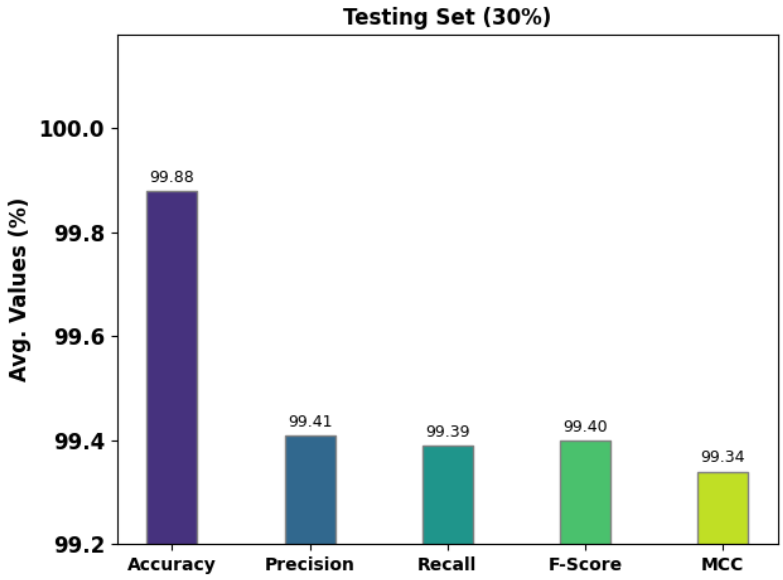

Fig. 8. Average outcome of TSA-OSSAE algorithm on 30% of TSS

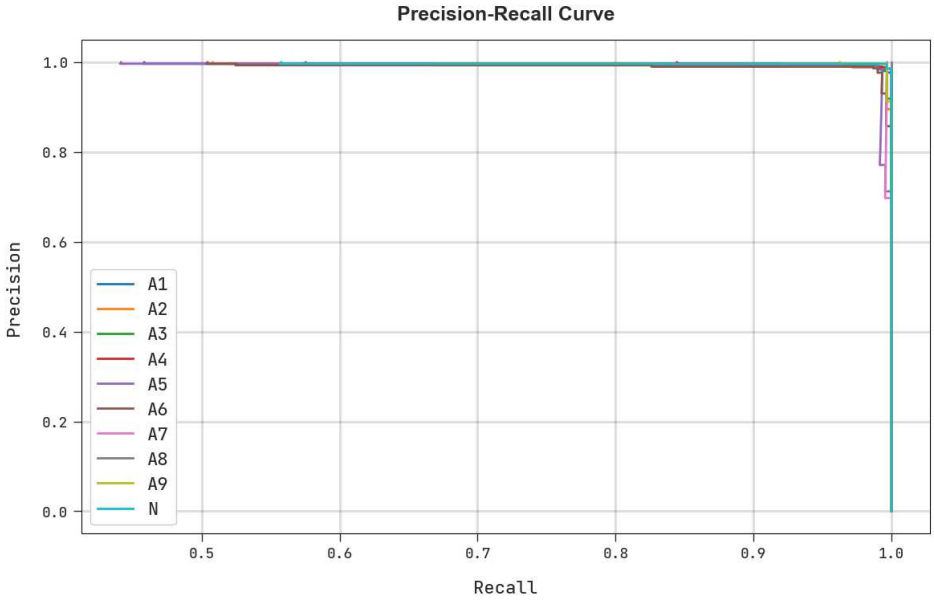

Fig. 9. Precision-recall curve analysis of the TSA-OSSAE approach

An obvious precision-recall (PR) assessment of the TSA-OSSAE system in the test database is given in Fig. 9. The figure designated the TSA-OSSAE system has resulted in improved values of PR values in distinct classes.

Table 5 Comparative outcome of TSA-OSSAE method with recent methodologies

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
TSA-OSSAE	99.88	99.41	99.39	99.40
Voting Classifier-SMOTE	99.69	98.15	96.40	97.13
ANN	90.12	94.32	99.08	93.44
1D-CNN	83.69	88.70	83.51	89.71
Random Forest	99.35	97.56	98.24	98.36

Deep Random Neural Network	99.50	99.18	99.09	99.16

Table 5 renders an overall outcome investigation of the TSA-OSSAE model with recent models [16]. A comparative investigation of the TSA-OSSAE algorithm with existing methods is given in Fig. 10. From the outcomes, it is apparent that the 1D-CNN method has shown minimal performance over other existing techniques. Also, the ANN model has reached slightly improved results whereas the RF model has reached even increased outcomes. Although the Voting classifier-SMOTE and DRNN models have resulted in reasonable performance, the TSA-OSSAE approach has demonstrated higher outcomes over other approaches.

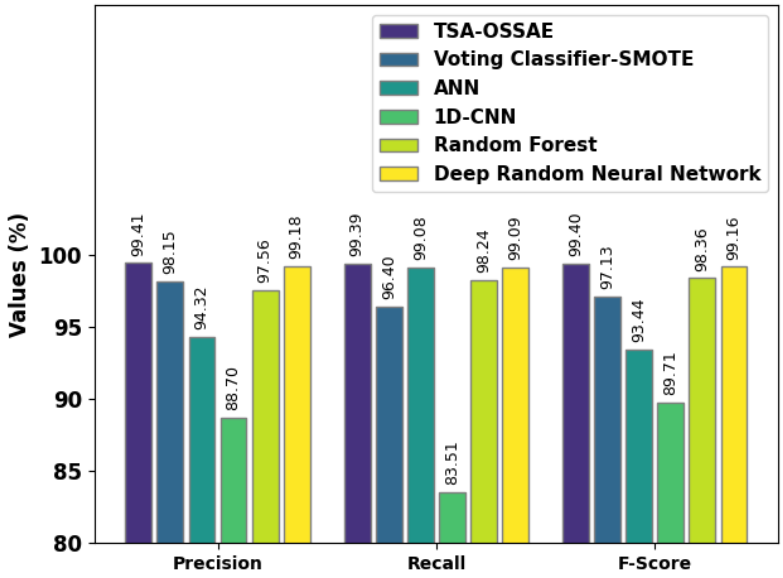

Fig. 10. Comparative analysis of the TSA-OSSAE system with recent methodologies

Lastly, a detailed $accu_y$ examination of the TSA-OSSAE methodology with existing approaches occurs in Fig. 11. The experimental values represented by the TSA-OSSAE methodology have resulted in increased $accu_y$ of 99.88% whereas the voting-classifier-SMOTE, ANN, 1D-CNN, RF, and DRNN models have accomplished reduced $accu_y$ of 99.69%, 90.12%, 83.69%, 99.35%, and 99.50% respectively. Thus, the TSA-OSSAE model can be applied for enhanced cyber threat detection performance.

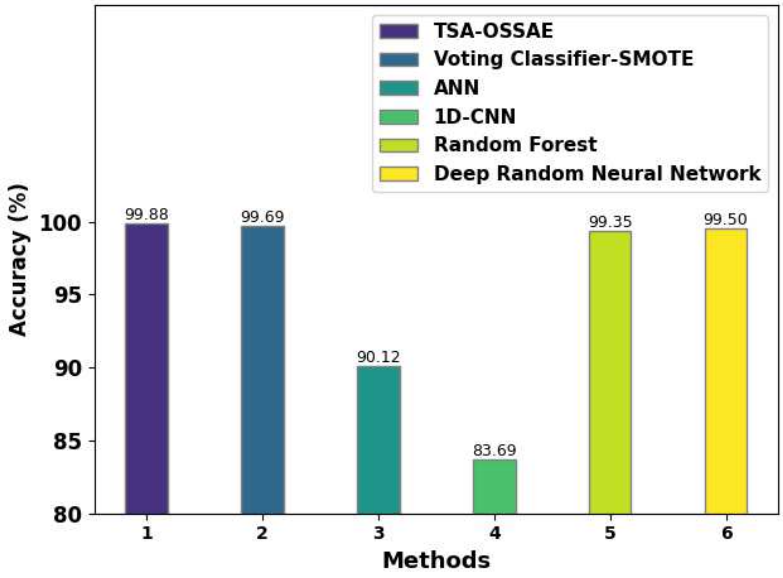

Fig. 11. $Accu_y$ the outcome of TSA-OSSAE methodology with recent methodologies

5. Conclusion

In this article, a novel TSA-OSSAE system has been projected for the detection and classification of cyber threats in IoT-enabled SC applications. The presented TSA-OSSAE algorithm majorly focuses on the detection of cyber threats to attain security in the SC. To attain this, this TSA-OSSAE approach follows TSA based feature selection approach to reduce computational complexity. Besides, the TSA-OSSAE technique applies the SSAE model for cyber threat detection. At last, the hyperparameters of the SSAE approach are optimally chosen by using the MVO technique. The experimental result investigation of the TSA-OSSAE technique was performed by making use of the TON_IoT telemetry dataset. The experimental outcomes establish the optimal performance of the TSA-OSSAE system to other recent methodologies. In the future, the performance of the TSA-OSSAE methodology was improvised by the outlier removal process.

Author Contributions: Conceptualization, S.D., Y.M. ,S.K.R. and S.K.P; writing—original draft preparation, S.D.,Y.M. and S.K.R.; investigation, S.D.,Y.M.,S.K.P; methodology, Y.M. and S.K.R.; Results and discussion , S.D., S.K.R. Writing—review and editing, S.K.R, Y.M. and S.K.P. All authors have read and agreed to the published version of the manuscript.

Conflict of Interest

The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated during the current study.

Ethics approval

This article does not contain any studies with human participants performed by any of the authors.

Consent to Participate

Not applicable.

Funding details

None.

Informed Consent

All the authors well aware submission of manuscript.

References

[1] Chen, D., Wawrzynski, P. and Lv, Z., 2021. Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities and Society*, *66*, p.102655.

[2] Rashid, M.M., Kamruzzaman, J., Hassan, M.M., Imam, T. and Gordon, S., 2020. Cyberattacks detection in iot-based smart city applications using machine learning techniques. *International journal of environmental research and public health*, *17*(24), p.9347.

[3] Elsaeidy, A.A., Jagannath, N., Sanchis, A.G., Jamalipour, A. and Munasinghe, K.S., 2020. Replay attack detection in smart cities using deep learning. *IEEE Access*, *8*, pp.137825-137837.

[4] Ma, C., 2021. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, *7*, pp.7999-8012.

[5] Ahmed, S., Hossain, M., Kaiser, M.S., Noor, M.B.T., Mahmud, M. and Chakraborty, C., 2021. Artificial intelligence and machine learning for ensuring security in smart cities. In *Data-driven mining, learning and analytics for secured smart cities* (pp. 23-47). Springer, Cham.

[6] Mehta, S., Bhushan, B. and Kumar, R., 2022. Machine Learning Approaches for Smart City Applications: Emergence, Challenges and Opportunities. *Recent Advances in Internet of Things and Machine Learning*, pp.147-163.

[7] Kumar, P., Gupta, G.P. and Tripathi, R., 2021. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *Journal of Systems Architecture*, *115*, p.101954.

[8] Duraisamy, A., Subramaniam, M. and Robin, C.R.R., 2021. An optimized deep learning based security enhancement and attack detection on IoT using IDS and KH-AES for smart cities. *Stud Inf Control*, *30*(2), pp.121-131.

[9] Duraisamy, A., Subramaniam, M. and Robin, C.R.R., 2021. An optimized deep learning based security enhancement and attack detection on IoT using IDS and KH-AES for smart cities. *Stud Inf Control*, *30*(2), pp.121-131.

[10] Singh, S.K., Azzaoui, A.E., Kim, T.W., Pan, Y. and Park, J.H., 2021. DeepBlockScheme: A deep learning-based blockchain driven scheme for secure smart city. *Hum.-Centric Comput. Inf. Sci*, *11*, p.12.

[11] Elsaeidy, A., Munasinghe, K.S., Sharma, D. and Jamalipour, A., 2019. Intrusion detection in smart cities using Restricted Boltzmann Machines. Journal of Network and Computer Applications, 135, pp.76-83.

[12] Baig, Z., Syed, N. and Mohammad, N., 2022. Securing the Smart City Airspace: Drone Cyber Attack Detection through Machine Learning. Future Internet, 14(7), p.205.

[13] Aloqaily, M., Otoum, S., Al Ridhawi, I. and Jararweh, Y., 2019. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks, 90, p.101842.

[14] Shafiq, M., Tian, Z., Sun, Y., Du, X. and Guizani, M., 2020. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. Future Generation Computer Systems, 107, pp.433-442.

[15] Elsaeidy, A.A., Jamalipour, A. and Munasinghe, K.S., 2021. A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City. IEEE Access, 9, pp.154864-154875.

[16] Rout, S.K., Rath, A.K. and Bhagabati, C., 2016, September. Energy efficient and cost effective secure node localization with key management in wireless sensor networks. In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 515-520). IEEE.

[17] Saba, T., Khan, A.R., Sadad, T. and Hong, S.P., 2022. Securing the IoT System of Smart City against Cyber Threats Using Deep Learning. Discrete Dynamics in Nature and Society, 2022.

[18] Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q.V., Padannayil, S.K. and Simran, K., 2020. A visualized botnet detection system based deep learning for the internet of things networks of smart cities. IEEE Transactions on Industry Applications, 56(4), pp.4436-4456.

[19] Rout, S.K., Sahu, B., Mohapatra, P.K., Mohanty, S.N., Sharma, A.K. (2023). IoT and an Intelligent Cloud-Based Framework to Build a Smart City Traffic Management System. In: Ahad, M.A., Casalino, G., Bhushan, B. (eds) Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities. Springer, Cham.

[20] Qais, M.H., Hasanien, H.M. and Alghuwainem, S., 2020. Optimal transient search algorithm-based PI controllers for enhancing low voltage ride-through ability of grid-linked PMSG-based wind turbine. *Electronics*, *9*(11), p.1807.

[21] Mienye, I.D. and Sun, Y., 2021. Improved heart disease prediction using particle swarm optimization based stacked sparse autoencoder. *Electronics*, *10*(19), p.2347.
[22] Abualigah, L. and Alkhrabsheh, M., 2022. Amended hybrid multi-verse optimizer with genetic algorithm for solving task scheduling problem in cloud computing. *The Journal of Supercomputing*, *78*(1), pp.740-765.
[23] N. Moustafa, "TON-IoT dataset," 2020, https://cloudstor. aarnet.edu.au/plus/s/ds5zW91vdgjEj9i.