Indonesian Journal of Electrical Engineering and Computer Science
Vol. 38, No. 3, June 2025, pp. 1819~1829
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v38.i3.pp1819-1829

Deep learning-based secured resilient architecture for IoT-driven critical infrastructure

Srinivas A. Vaddadi[1], Rohith Vallabhaneni[1], Sanjaikanth E. Vadakkethil Somanathan Pillai[2], Santosh Reddy Addula[1], Bhuvanesh Ananthan[3]
[1]Department of Information Technology, University of the Cumberlands, Williamsburg, United States
[2]School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, USA
[3]Department of Electrical and Electronics Engineering, PSN College of Engineering and Technology, Tirunelveli, India

Article Info

Article history:

Received Mar 18, 2024
Revised Nov 21, 2024
Accepted Nov 30, 2024

Keywords:

Blockchain
Deep belief network
Improved crystal structure
Internet of things
Non-local means filter

ABSTRACT

While enabling remote management and efficiency improvements, the infrastructure of the smart city becomes able to advance due to the consequences of the internet of things (IoT). The development of IoT in the fields of agriculture, robotics, transportation, computerization, and manufacturing. Based on the serious infrastructure environments, smart revolutions and digital transformation play an important role. According to various perspectives on issues of privacy and security, the challenge is heterogeneous data handling from various devices of IoT. The critical IoT infrastructure with its regular operations is jeopardized by the sensor communication among both IoT devices depending upon the attacker targets. This research suggested a novel deep belief network (DBN) and a secured data dissemination structure based on blockchain to address the issues of privacy and security infrastructures. The non-local means filter performs pre-processing and the feature selection is achieved using the improved crystal structure (ICS) algorithm. The DBN model for the classification of attack and non-attack data. For the non-attacked data, the security is offered via a blockchain network incorporated with the interplanetary file system.

Corresponding Author:

Srinivas A. Vaddadi
Department of Information Technology, University of the Cumberlands
6178 College Station Drive, Williamsburg, KY 40769, USA
Email: Vsad93@gmail.com

1. INTRODUCTION

The modern world is changing with the inclusion of internet of things (IoT) devices, which make us lead an effortless life. These are used in many fields as healthcare, retail, and vertical markets. Implementation of enormous IoT devices takes away the big data concept and the flow of data in an unprecedented way. Since IoT devices are omnipresent, it is a challenging factor for the secured connection, which is necessarily important in the field [1]. More than that security is the root factor for any connection that has to be built. With encryption and decryption techniques, one can improve the security of the IoT infrastructure. In traditional information technology (IT) platforms, the security of the system can be obtained with the help of a common software platform that is not available in the IoT platform. The transition from IT to IoT requires challenging requirements.

The secured IoT devices or connections, enhance the system's scalability, which is the predominant factor in the IT infrastructure. Meanwhile, the implementation of security in the IoT system has various hardware and software. This might have led to integration challenges for the devices. For instance, the security also varies from low to higher base on the cost. The low-cost security provides basic security,

whereas as expensive one provides the best security. Moreover, the risk factors in low-level security are higher and lower in high-level security with complex production or design. The risk can be averted with software-based security techniques however, it elevates the complexities. The flexibility of software-based security is higher and so adopted for the final stages of any project.

The hardware-based security solutions are the best and are implemented at the endpoints of the board level. Since the complexity of the hardware-based security is higher with the employment of more hardware elements. The risk factor of this is lower and is utilized in the concept process of the projects. Deep learning (DL) and machine learning (ML)-based secured IoT-based infrastructures are offered by many researchers with less security and more complexity [2], [3]. Hence we proposed an innovative approach that provides resilience-based secured IoT infrastructure for the enhancement of the security in the critical infrastructure. For that, we have proposed an improved crystal structure (ICS) algorithm and deep belief network (DBN) with blockchain model for providing secured IoT infrastructures [4], [5].

The remaining part of this work is arranged like; the existing papers are discussed in section 2 and suggested architecture is presented in section 3. Section 4 investigates the investigational outputs and the whole article ends in section 5.

2. LITERATURE REVIEW

The multidisciplinary approach was suggested by [6] for resilience promotion and vulnerability detection. The IoT network's integrity and threat mitigation are important in the structure of multi-layered security. The privacy protocols and IoT security enhancement to the blockchain technology. Additional security layers are offered with immutability, transparency, and decentralization of inherent features in Blockchain. While compromising IoT systems, unauthorized entities are more difficult. According to IoT security, the best practices are promoted with security experts and collaborations fostering. While ensuring data safety and privacy, it ensures stakeholders build trust and also the reputations are protected thereby proving reliably and safely robust security measures.

Kolhar and Aldossary [7], introduced a DL model to emphasize on smart networks and securing IoT Infrastructure. The voluminous datasets and handling complex sophisticated to employ intrusion detection. The subdivision's exact IoT implementations are safeguarded to present a novel IoT security model. The cyber-attacks with intricate patterns learned to manage huge datasets and demonstrate superior performance. The cyber-threats are identified to indicate the experimental results. By this investigation, the detection rate is 99.6% and 99.8% for InSDN and ToN-IoT datasets. In smart cities, an IoT system integrity is maintained based on the achieved track record.

Kelli *et al.* [8], presented blockchain and ML to provide a cyber-resilience framework. The essence is an intelligent healthcare model to monitor solutions. Required the appropriate measures to digitalize each health record. To maintain data, the insurance companies and hospitals based multiple organizations that integrate interoperable systems. For optimal patient assistance, the great important is describing access to health information. While demonstrating an effective security solution, the multi-layer tool with the featuring framework is presented. Based on a distributed way, the health data and authorized users to patient records with its access control are provided depending upon smart contracts.

According to IoT-based transportation networks, Pande *et al.* [9] presented a convolutional neural network (CNN) to detect resilient intrusion. In transportation networks, IoT generates a huge amount of information in which the useful characteristics are extracted automatically. The malicious and legitimate traffic patterns of large collections are based on CNN training in which the intrusion is identified and classified. A better rate of false positives is maintained with the system although consumers noticed various kinds of intrusions. Strong protection is offered with persistent intrusion detection. The infrastructure of energetic transportation is ensured and the network security was increased effectively.

DL uses a collection of well-known ML methods built on artificial neural networks, which enable one to mimic the information processing of organic nervous systems composed of different layers of perceptrons [10]. Although artificial neural networks have been around for a century, they have recently gained attention from the research community again because of advancements in computer power and computational efficiency. These advancements have made it possible for DL architectures, which consist of multiple related layers built up by hundreds or thousands of neurons each, to be used effectively and practically in a variety of application fields, such as computer vision [11], speech recognition [12], and health informatics [13]. The use of DL to IoT security is a current hot study field that has been expanding in the last several years, along with the two previously mentioned burgeoning research topics. There is still a lack of a specific systematic review in the relevant literature regarding DL approaches to IoT security, as the only one that mentions DL in the title [14] is not a proper systematic review (no evidence of the used databases, nor the applied queries, nor the numbers of retrieved papers are given) and is more focused on ML than DL.

Other recent evaluations exist in the literature, although they mostly target one or more of the following topics: generic ML approaches [15], [16], a particular security issue like intrusion detection [17], or none at all [18]-[21].

Research in DL-based secured resilient architectures for IoT-driven critical infrastructure is an evolving field, but several significant gaps remain [22], [23]. One major area that requires attention is real-time threat detection and response. IoT systems, especially those supporting critical infrastructure, demand rapid identification of threats and instantaneous responses to mitigate damage [24], [25]. However, existing DL models often struggle to balance accuracy with the real-time requirements of such systems. These models are computationally expensive and may introduce delays, which are unacceptable in scenarios where timing is critical.

Another challenge is the scalability and adaptability of these architectures. IoT networks are highly dynamic, with devices frequently joining or leaving the network, often with diverse types and capabilities. Many current DL models are not designed to adapt to these fluctuations, resulting in potential vulnerabilities. There is a need for research into scalable and adaptable architectures that can maintain robust security across a growing and diverse array of IoT devices while preserving system resilience.

Lastly, explainability and interpretability of DL models in critical infrastructure is a pressing concern. In such vital systems, it is not enough for the model to be accurate; stakeholders need to understand the decisions being made by these models. Current research lacks sufficient attention to making DL-based security architectures transparent, which is essential for gaining the trust of operators and ensuring that the system's actions can be effectively monitored and audited. Addressing these research gaps will be pivotal in developing a robust, scalable, and efficient DL-based secured architecture for IoT-driven critical infrastructure.

3. PROPOSED FRAMEWORKS

For IoT-based critical infrastructure, the secured data dissemination with deep neural network (DNN) and blockchain-based model is designed in this proposed architecture. The intrusion and non-intrusion data are categorized with the usage of a DNN classifier thereby maximizing the accuracy of classification data. The detailed model of the proposed work is discussed in the following sub-sections. Figure 1 depicts the illustration of the proposed schematic model.

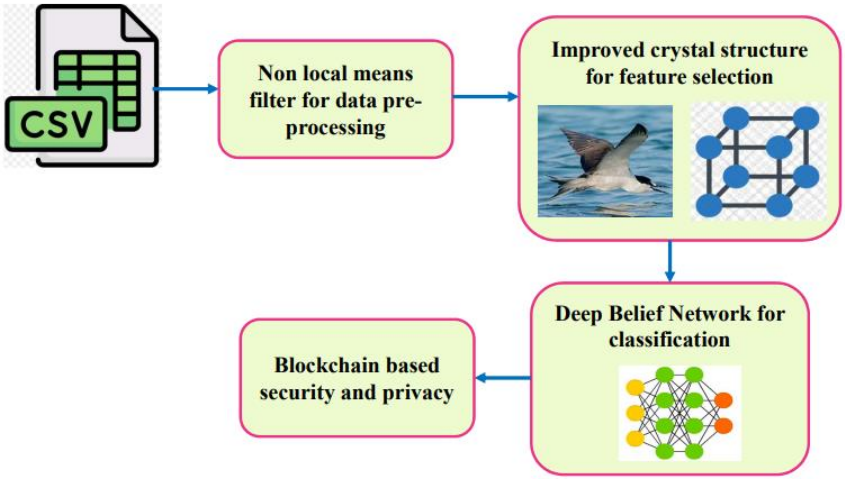

Figure 1. Illustration of the recommended schematic model

3.1. Collecting data

Different kinds of IoT infrastructures (IS_t) are nuclear power plants, and thermal and water treatment plants [10]. These critical infrastructures attach various kinds of IoT sensors. The data in CSV files are stored and the sensors are manipulated by one person among these operators. In the CSV file, store the data and the tempered data obtained from the critical infrastructure of the sensor. The poising attack is the manipulation activity of data type and this attack causes the classifier accuracy.

3.2. Data pre-processing

This step involved in an intelligence layer obtains the collected data file. From the collected data, the non-local means filter removes the noises, infinity values, and missing values. The below expression outlines the noise attenuated outputs [11].

$$\widetilde{M}(j,k) = \sum_{r=-S_D}^{S_D} \sum_{p=-S_D}^{S_D} \frac{\chi(r,p) M_{j,k}^{search}(r,p)}{M_F} \quad (1)$$

Based on the search window, (r,p) is the center and $S \times S$ matrix size is$M_{j,k}^{search}$. Calculate the M_F and χ.

$$M_F = \sum_{r=-S_D}^{S_D} \sum_{p=-S_D}^{S_D} \chi(r,p) \quad (2)$$

Define $\chi(r,p)$ and the noise level is H.

$$\chi(r,p) = \left\| M_{(r,p)}^{compare} - M_{(j,k)}^{compare} \right\|_{2,\delta}^{2} \quad (3)$$

The standard deviation is δ with the two matrices weight are $M_{(r,p)}^{compare}$ and $M_{(j,k)}^{compare}$. The noise removed also the infinity and missing values were neglected via non non-local means filter.

3.3. Feature selection

The ICS algorithm selects the features and minimizes the dimensionality of features [12]. The respective locations of lattice in atoms derive the principle of the CS algorithm. The below formula describes the infinite lattice shape depending upon the framework of periodic crystal features.

$$G = \sum e_j d_j \quad (4)$$

At jth sample, e_j and d_j are the integer and directions of crystallographic (G) principal linked to the shortest vector of features. According to the space for search, the mathematical modeling of a single crystal with its candidate solution is considered. The initialization formula for distributed crystals is as;

$$Str = \begin{bmatrix} Str_1 \\ Str_2 \\ . \\ . \\ . \\ Str_j \\ . \\ . \\ . \\ Str_e \end{bmatrix} \quad (5)$$

$$Str = \begin{bmatrix} w_1^1 & w_1^2 & \dots & w_1^i & \dots & w_1^D \\ w_2^1 & w_2^2 & \dots & w_2^i & \dots & w_2^D \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ w_j^1 & w_j^2 & \dots & w_j^i & \dots & w_j^D \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ w_m^1 & w_m^2 & \dots & w_m^i & \dots & w_m^D \end{bmatrix}, if \begin{cases} j = 1,2,\dots,e \\ k = 1,2,\dots,e \end{cases} \quad (6)$$

From this, D as the problem of dimensionality of features that implies the number of crystals and Strmain as the main crystal that deems the corner crystals. Where, A_C is selected crystals and Str_B is the optimal configuration of features. The simple cubicle, cubicle with best and mean crystal, and cubicle with best crystals are used to update the position with the random numbers r_1, r_2 and r_3.

The sooty tern algorithm with its exploitation behavior improves the best and mean crystal with the cubicle of CS algorithm [13]. Hence, the ICS model selects the feature subsets effectively.

$$Str_N = Str_O + r_1 Str_{main} + r_2 Str_B + r_3 A_C + q` \quad (7)$$

The exploration function of sooty terns is $q`$ with the old and new locations are Str_O and Str_N. The features are detected and also the dimensionality is reduced.

3.4. Attack classification

The tarining and testing data are two sections of input datasets that are considered at an 8:2 ratio. The binary classes of 0 and 1 like intrusion and non-intrusion are classified by means of a DBN that contains layer-wise training with stacked restricted Boltzmann machines (RBMs). Over the past trained layer, RBM training is performed by utilizing RBM layers [14]. Based on a small number of labeled data, the fine-tuned and unlabeled data pertains to the auto-encoders and RBMs. At a time greedily, each layer is optimized and utilizes a greedy layer-wise model. All the layers apply combined supervised training. When implementing the softmax layer, an unsupervised model of the greedy layer trains the obtained features. The standard deviation is expressed as;

$$\varepsilon^* = \frac{\varepsilon - min_\varepsilon \mathrm{h}}{max_\varepsilon - min_\varepsilon \mathrm{h}}` \quad (8)$$

At jth visible unit is VS_j and the visible and hidden cells are and with the weight $\mathrm{h}_{j,k}$.

$$M = \{\mathrm{h}_{j,k} \in \mathrm{h}^{o,u}\} \quad (9)$$

The parameters are received by utilizing the probability function determination. The hidden layer node set with the overall condition acquires the visible layer node sets with its marginal distribution is $pr(\mu/\theta)$.

$$pr(\mu/\theta) = \frac{1}{X(\theta)} \sum_g e^{-F\left(\mu, g/\theta\right)} \quad (10)$$

Each hidden layer cells with enactment conditions are autonomous that describes the visible cell conditions. The jth hidden element initiation likelihood as;

$$pr(g_j = 1/\mu) = \varepsilon(B_j + \sum_j \mu_j M_{jk}) \quad (11)$$

The sigmoid function is ε. Figure 2 plots the graphical representaion of DBN to detect attacks. For Iot based critical infrastructures, the attack and non-attack data are classified by means of DBN.

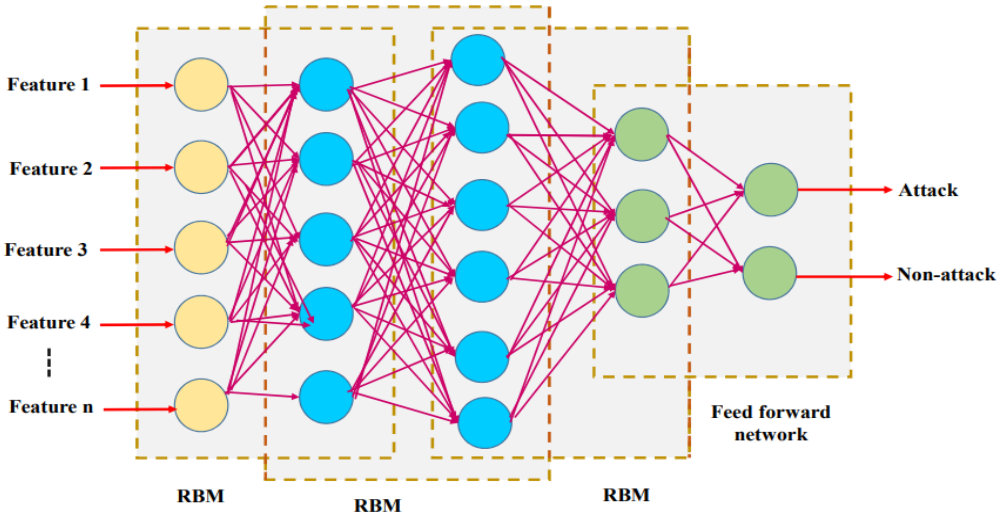

Figure 2. The attack detection model based on DBN

3.5. Privacy and security based on blockchain

Blockchain is the extending collection of blocks in organized entries which is the distributed database. The documentation of transactions is done with a simplified nature is unaltered and can be monitored inside the network. In our work, we adopted the blockchain layer for the secured infrastructure information [15]. The non-intrusion information from the intelligence layer is transferred to the blockchain layer and saved in a smart contract. Based on the user's agreement, the privacy of the non-intrusion data is maintained and executed in the solidity compiler v0.8.21. The smart contract is designed in a Sepolia testnet along with the Meta mask. A validation of the IoT-based non-intrusion data is executed by the smart contract. The IPFS is utilized for the facilitation of the storage of various versions in the elongated time. The value of hash to a non-intrusion information is generated with the secured hash algorithm. The blockchain stores the value of hash from the IPFS and is forwarded to the application layer thus enabling the accessing of information by the authorized user in the critical infrastructure.

The application layer involves various dangerous infrastructures like thermal and nuclear power plants with water treatment. For instance, from the blockchain, the data received while improving water quality. Pure water is provided to improve the human life quality. Human life is directly affected by obtaining non-malicious data from a blockchain network.

4. EXPERIMENTAL INVESTIGATION AND DISCUSSION

This section is for the investigation of the performances of the proposed technique incorporated with the comparative works such as MA [6], DL [7], ML [8], and CNN [9]. This section presents the dataset description and experimental setup for the simulation that is to be performed.

4.1. Experimental setup

For the experimental purpose, utilize the application of Google Colab along with the integrated development environment. The information for the feature selection and classification is obtained using the implementation of Google Colab. 128 GB RAM capacity-based PC is used for the implementation.

4.2. Dataset description

The dataset was collected from the IEEE dataport and is the intrusion classification dataset known as IEC 60870-5-104. The term IEC 60870-5-104 denotes the protocol used for the critical infrastructure of IoT. Various features and network configurations are included in this dataset such as bandwidth, packet size, and so on. 84 various features are employed with different numerical values in the dataset.

4.3. Evaluation of parameters

The evaluation of parameters is effectuated in this section. This is a comparative study of various methods such as MA [6], DL [7], ML [8], and CNN [9] along with the proposed technique. The intrusion detection of the proposed technique is analyzed with parameters such as accuracy, precision, and recall. The execution of the blockchain is analyzed with the term execution time and the overall security is analyzed with the security analysis parameter.

Analysis of blockchain is effectuated with the execution time and the execution of time of our proposed work is lower than the other techniques. The inclusion of blockchain decreases the execution time and the graphical plot is illustrated in Figure 3. The execution time of the proposed technique and other previous works is shown. The execution time of the proposed work when the iteration number of 300 is 160s and the other techniques includes MA [6], DL [7], ML [8], and CNN [9] take more time of about 263 s, 365 s, 390s, and 400s respectively which might have produce higher computational time and make the use of our proposed technique.

The evaluation of accuracy in terms of number of iterations for various techniques such as proposed and MA [6], DL [7], ML [8], and CNN [9] are visually plotted in Figure 4. For the evaluation we have observed the values from the starting of iteration to the end of the iterations that is from 0 to 300 and plotted the values for each 50 iterations. The accuracy of the proposed technique when the iteration is about 300 is 98% while the rest of the works such as MA [6], DL [7], ML [8], and CNN [9] ensure the accuracy of at 300th iteration of about 82%, 87%, 92%, and 97% respectively. This is how the classification and detection of intrusion in the system is made.

The evaluation of precision for different number of iterations are established and plotted in Figure 5. The precision of the recommended method is higher due to the higher accuracy and the selection better techniques. As per other parameters the proposed work is associated with the existing works like MA [6], DL [7], ML [8], and CNN [9]. The number of iterations taken are 300 and at 300th iteration the precision of the proposed work is 97% and other techniques such as MA [6], DL [7], ML [8], and CNN [9] ensure the precisions of 84%, 86%, 90%, and 95% respectively.

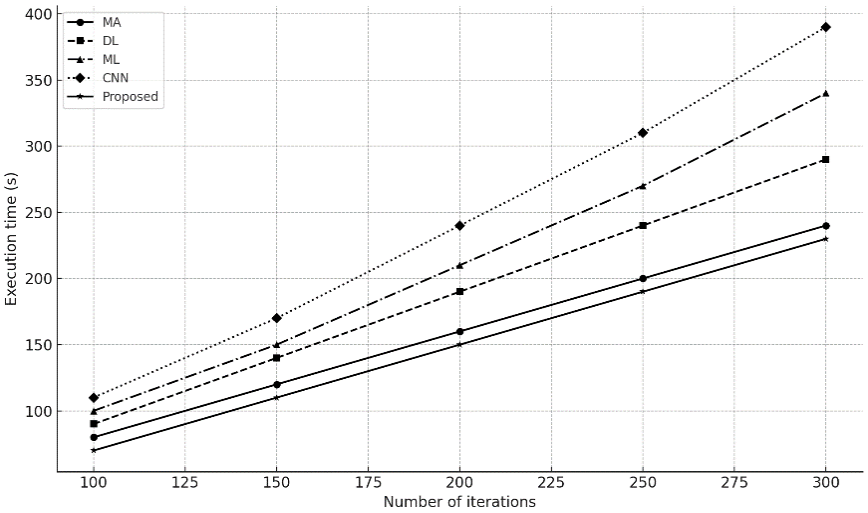

Figure 3. Validation of performance in terms of execution time (s) vs. number of iterations

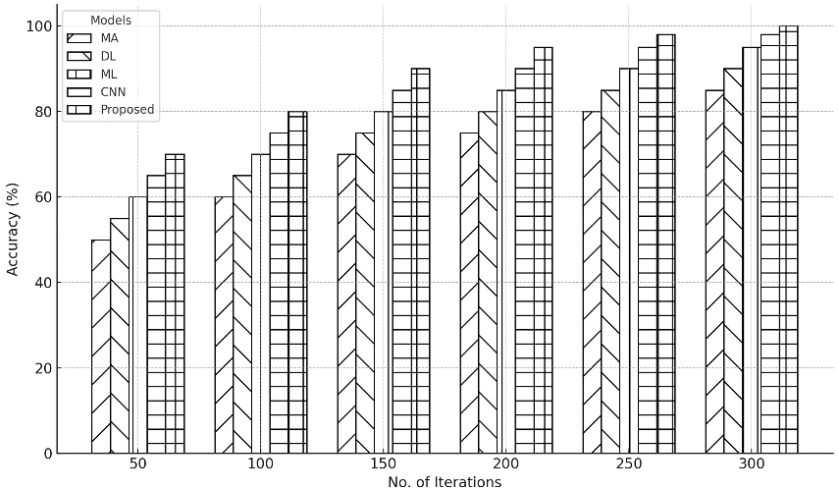

Figure 4. Validation of performance in terms of accuracy (%) vs. number of iterations

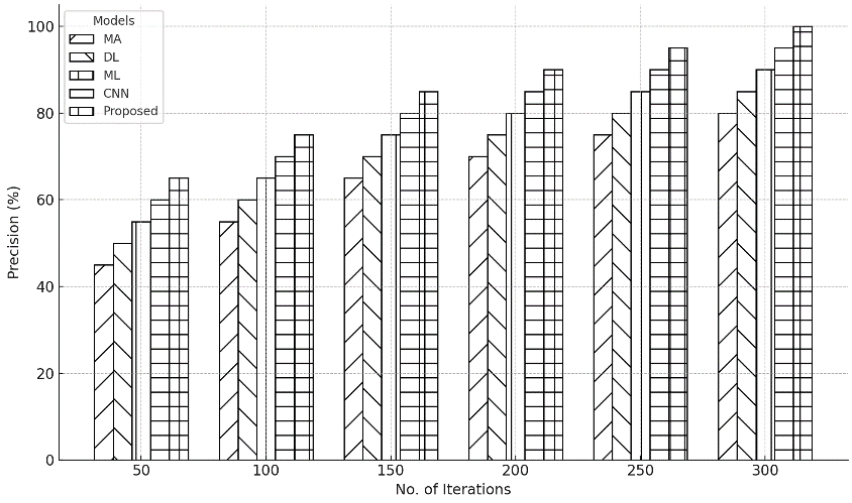

Figure 5. Validation of performance in terms of precision (%) vs. number of iterations

The recall of the recommended technique and comparison techniques such as MA [6], DL [7], ML [8], and CNN [9] are plotted in Figure 6. This evaluation ensures the effectiveness of the classification of attacks and non-attacks information and for our proposed work the recall is 96% at 300th iterations and for other techniques such as MA [6], DL [7], ML [8], and CNN [9] ensure the recall of 87%, 88%, 89%, and 93% correspondingly. The next parameter is security analysis which ensures the security of the techniques. Since our proposed system utilizes the blockchain it has higher security level and others have lower security levels. The security analysis for various techniques and proposed techniques are tabulated in Table 1. When the number of iterations is equal to 300 the security of the recommended work is 98% that becomes superior to other techniques such as MA [6], DL [7], ML [8], and CNN [9] with the security of 83%, 88%, 90%, and 94% respectively and is prone to attacks.

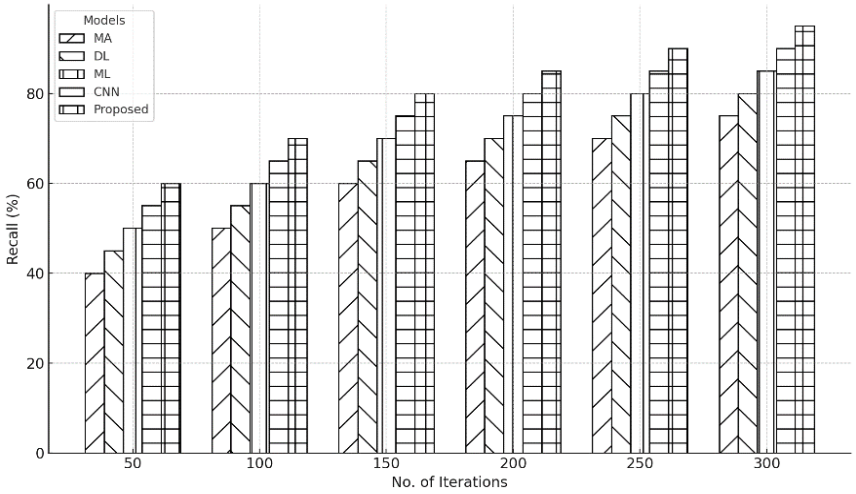

Figure 6. Validation of performance in terms of recall (%) vs. number of iterations

Table 1. Security analysis vs. number of iterations for various techniques

Methods	Iterations					
	50	100	150	200	250	300
MA	56	62	67	71	78	83
DL	45	54	61	69	75	88
ML	48	55	64	73	79	90
CNN	64	69	75	82	88	94
Proposed	72	76	80	87	94	98

The practical impacts of DL-based secured resilient architectures for IoT-driven critical infrastructure are significant, enhancing security, scalability, and operational efficiency. These architectures enable real-time threat detection and decision-making, preventing cyberattacks and reducing downtime in critical sectors such as energy, healthcare, and transportation. By continuously learning from data, DL models adapt to evolving threats, improving resilience and reducing system failures. They also enhance privacy by incorporating techniques like federated learning, ensuring compliance with data regulations while safeguarding sensitive information.

5. CONCLUSION

According to IoT oriented critical infrastructure, this work provided the secured and DBN based intrusion detection. The critical infrastructures like thermal and nuclear power with water treatment plants by utilizing standard dataset. The proposed architecture with its overall performance is enhanced using non local means filters for data pre-processing. The bulky datasets with less important features causes computation overhead, which are reduced by means of feature selection model called ICS algorithm. An accurate intrusion detection results are categorized via DBN. From the dataset feature space, anomalous data is identified for anomaly detection. A critical data infrastructure with secure storage is offered by utilizing an IPFS-based blockchain system. The simulation results show that the proposed system achieved a classification and

detection accuracy of 98.2%, precision of 97%, and recall of 96%. Further, the execution time of the proposed work is lower and ensures faster attack detection and secured system. Furthermore, the security level of the proposed system is about 98%. Future research in DL-based secured resilient architecture for IoT-driven critical infrastructure offers several promising directions. One key area is the development of real-time, low-latency DL models that can handle the growing complexity of IoT environments while ensuring rapid threat detection and response. There is also a need for scalable and adaptable architectures that can manage diverse and heterogeneous IoT devices in dynamic networks. Energy-efficient DL models are crucial, particularly for resource-constrained IoT devices in critical infrastructure.

ACKNOWLEDGEMENTS

The Author with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

FUNDING INFORMATION

No funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Srinivas A. Vaddadi	✓		✓	✓	✓	✓		✓		✓			✓	
Rohith Vallabhaneni		✓				✓		✓	✓	✓	✓	✓		
Sanjaikanth E. Vadakkethil Somanathan Pillai	✓		✓	✓			✓			✓	✓		✓	✓
Santosh Reddy Addula	✓	✓	✓	✓			✓	✓	✓	✓				
Bhuvanesh Ananthan			✓	✓	✓	✓			✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [S.A.V], upon reasonable request

REFERENCES

[1] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," *In 2017 19th International Conference on Advanced Communication Technology (ICACT), IEEE*, pp. 464-467, 2017, doi: 10.23919/ICACT.2017.7890132.
[2] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: how do IoT devices use AI to enhance security?," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, 2018, doi: 10.1109/MSP.2018.2825478.
[3] S. U. Aswathy, T. Jarin, R. Mathews, L. M. Nair, and M. Rroan, "CAD systems for automatic detection and classification of COVID-19 in nano CT lung image by using machine learning technique," *International Journal of Pharmaceutical Research*, vol. 2, pp. 1865-1870, 2020, doi: 10.31838/ijpr/2020.12.02.247.
[4] B. Deepanraj, R. Muniraj, T. Jarin, and J. Kohila, "Modern multilevel inverter for application of drive with grid connected renewable energy sources," *In 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), IEEE*, pp. 150-155, 2023, doi: 10.1109/ICACRS58579.2023.10405229.
[5] V. Sivaraman, H. H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: security and privacy implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71-79, 2018, doi: 10.1109/MTS.2018.2826079.
[6] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, and C. U. Asonze, "IoT security in the era of ubiquitous computing: a multidisciplinary approach to addressing vulnerabilities and promoting resilience," *Asian Journal of Research in Computer Science*, vol. 16, no. 4, 2023, doi: 10.9734/ajrcos/2023/v16i4397.
[7] M. Kolhar and S. M. Aldossary, "A deep learning approach for securing IoT infrastructure with emphasis on smart vertical networks," *Designs*, vol. 7, no. 6, pp. 139, 2023, doi: 10.3390/designs7060139.

[8] V. Kelli, P. Sarigiannidis, V. Argyriou, T. Lagkas, and V. Vitsas, "A cyber resilience framework for NG-IoT healthcare using machine learning and blockchain," *In ICC 2021-IEEE International Conference on Communications, IEEE*, pp. 1-6, 2021, doi: 10.1109/ICC42927.2021.9500496.
[9] S. P. Pande, S. Chaudhary, P. R. Satav, U. P. Thakur, and N. Parati, "IoT-enabled transportation networks for resilient intrusion detection using deep learning," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 10s, pp. 49-58, 2023, doi: 10.1109/tits.2022.3188671.
[10] L. Deng and D. Yu, "Deep learning: methods and applications," *Foundations and Trends in Signal Processing*, vol. 7, no. 3–4, pp. 197–387, 2014, doi: 10.1561/2000000039.
[11] A. S. Lundervold and A. Lundervold, "An overview of deep learning in medical imaging focusing on MRI," *Zeitschrift für Medizinische Physik*, vol. 29, no. 2, pp. 102–127, 2019, doi: 10.1016/j.zemedi.2018.11.002.
[12] H. M. Fayek, M. Lech, and L. Cavedon, "Evaluating deep learning architectures for speech emotion recognition," *Neural Network*, vol. 92, pp. 60–68, 2017, doi: 10.1016/j.neunet.2017.02.013.
[13] G. H.-J. Kwak and P. Hui, "DeepHealth: deep learning for health informatics," *ArXiv preprint*, arXiv:1909.00384, 2019, doi: 10.48550/arXiv.1909.00384.
[14] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *ArXiv preprint*, arXiv:1807.11023, 2018, doi: 10.1109/COMST.2020.2988293.
[15] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," *ArXiv preprint*, arXiv:1904.05735, 2019, doi: 10.1109/COMST.2020.2986444.
[16] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167-185, 2024, doi: 10.1016/j.iotcps.2023.12.003.
[17] A. Aleesa, B. Bahaa, A. Zaidan, and N. Sahar, "Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions," *Neural Computing and Applications*, pp. 1–32, 2019, doi: 10.1016/j.cosrev.2021.100389.
[18] D. Berman, A. Buczak, J. Chavis, and C. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, 2019, doi: 10.3390/info10040122.
[19] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine learning for security and the internet of things: the good, the bad, and the ugly," *IEEE Access*, vol. 7, pp. 158126–158147, 2019, doi: 10.1109/ACCESS.2019.2948912.
[20] T. Nguyen *et al.*, "Guest editorial: deep learning assisted visual IoT technologies for critical infrastructure protection," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 10-12, 2022, doi: 10.1109/MIOT.2022.9889269.
[21] H. Ai *et al.*, "Modified non-local means: a novel denoising approach to process gravity field data," *Open Geosciences*, vol. 15, no. 1, pp. 20220551, 2023, doi: 10.1515/geo-2022-0551.
[22] S. Talatahari, M. Azizi, M. Tolouei, B. Talatahari, and P. Sareh, "Crystal structure algorithm (CryStAl): a metaheuristic optimization method," *IEEE Access*, vol. 9, pp. 71244-71261, 2021, doi: 10.1109/ACCESS.2021.3079161.
[23] M. A. Saleem, N. Thien Le, W. Asdornwised, S. Chaitusaney, A. Javeed, and W. Benjapolakul, "Sooty tern optimization algorithm-based deep learning model for diagnosing NSCLC tumours," *Sensors*, vol. 23, no. 4, pp. 2147, 2023, doi: 10.3390/s23042147.
[24] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in internet of medical things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396-77404, 2020, doi: 10.1109/ACCESS.2020.2986013.
[25] T. Rathod *et al.*, "AI and blockchain-based secure data dissemination architecture for IoT-enabled critical infrastructure," *Sensors*, vol. 23, no. 21, pp. 8928, 2023, doi: 10.3390/s23218928.

BIOGRAPHIES OF AUTHORS

Srinivas A. Vaddadi is a dynamic and forward-thinking professional in the field of Cloud and DevSecOps. With a solid educational foundation in computer science, he embarked on a journey of continuous learning and professional growth. His relentless pursuit of knowledge and commitment to staying at the forefront of industry advancements has earned him recognition as a thought leader in the Cloud and DevSecOps space. He can be contacted at email: Vsad93@gmail.com.

Rohith Vallabhaneni is a dedicated worker with a strong work ethic in leading teams to solve organizational issues. He is capable of learning all aspects of information within a company and using the technical knowledge and business background to effectively analyze security measures to determine their effectiveness in order to strengthen the overall security posture. He has great work ethic and outstanding team leadership skills and seek to accomplish organizational goals, while growing in knowledge and experience. He can be contacted at email: rohit.vallabhaneni.2222@gmail.com.

Sanjaikanth E. Vadakkethil Somanathan Pillai (Senior Member, IEEE) holds an MS in software engineering from The University of Texas at Austin, Texas, USA, and a BE from the University of Calicut, Kerala, India. Currently pursuing a Ph.D. in computer science at the University of North Dakota, Grand Forks, North Dakota, USA, his research spans diverse areas such as mobile networks, network security, privacy, location-based services, and misinformation detection. He is a proud member of Sigma Xi, The Scientific Research Honor Society, underlining his commitment to advancing scientific knowledge and research excellence. He can be contacted at email: s.evadakkethil@und.edu.

Santosh Reddy Addula a senior member of IEEE, is a research scholar at the University of the Cumberlands. His educational qualifications include a Ph.D. and a Master of Science in information technology. With extensive experience in the IT industry, he has demonstrated expertise across multiple domains. He is an innovator who has made significant contributions to academic research through his articles as an author and co-author. Additionally, he serves as a reviewer for esteemed journals, demonstrating his commitment to advancing knowledge and upholding high standards in scholarly publications within his field. He can be contacted at email: santoshaddulait@gmail.com.

Bhuvanesh Ananthan received the B.E. degree in electrical and electronics engineering from Anna University in 2012, M.Tech. in power system engineering from Kalasalingam University in 2014 and Ph.D. degree from Faculty of Electrical Engineering of Anna University in 2019. He has published more than 100 papers in reputed international journals, 75 papers in international conferences and 20 books. He is a life time member of International Society for Research and Development and International Association of Engineers. He can be contacted at email: bhuvanesh.ananthan@gmail.com.