OPEN ACCESS JOURNALS
Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.20783401

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-06|Issue-03|2026

Neuromorphic Blockchain Framework for Secure and Energy-Optimized Outlier Detection in IoT-Driven Wireless Sensor Networks

Padmasree N[1], Dr. Malini M Patil[2]

RV Institute of Technology and Management (VTU Affiliated) Bangalore-560076

Article History
Received: 01.05.2026
Accepted: 11.06.2026
Published: 20.06.2026

Citation
Padmasree, N. & Patil, M. M. (2026). Neuromorphic Blockchain Framework for Secure and Energy-Optimized Outlier Detection in IoT-Driven Wireless Sensor Networks. *Indiana Journal of Multidisciplinary Research, 6*(3), 15-24.

Abstract: Wireless Sensor Networks (WSNs) are increasingly deployed in critical domains such as healthcare, environmental monitoring, and industrial automation, where secure and reliable data collection is essential. However, these networks face performance degradation and reduced network lifetime because they become susceptible to both unexpected system behaviour and intentional harmful attacks. The study presents a new framework that combines Spiking Neural Networks (SNNs) with a multi-layer block chain security system to solve these specific security challenges. The SNN model uses event-driven neural computation to find outliers with high precision while it maintains energy efficiency for nodes that have limited resources. The block chain component establishes data protection through decentralized validation which operates across multiple levels to maintain data security and permanent record. Experimental results show that the proposed method successfully reduces false detection rates while it improves trustworthiness of network transactions and extends system operational duration. The results demonstrate that the combination of neuromorphic intelligence and distributed ledger technologies creates a secure and energy-efficient anomaly detection system which scales to meet the demands of future IoT and WSN systems.

Keywords: Spiking Neural Networks (SNN), Block Chain-Enabled Outlier Detection in WSN, Neuromorphic Computing for IoT, Energy Efficient Anomaly Detection

INTRODUCTION

the growing use of Wireless Sensor Networks (WSNs) in both IoT applications and industrial environments has created two ongoing issues which require solutions: researchers need to develop methods for reliable anomaly detection and secure communication. Recent research has introduced multi-layer block chain frameworks which provide improved security and tamper resistance and privacy protection for IoT systems and WSN networks while maintaining low computational requirements[1]. The technological developments create trust among various sensor nodes which enable safe data sharing across networks that have limited resources. Spiking Neural Networks (SNNs) have become an effective tool for detecting anomalies through their operational capacity. The distributed and federated SNN variants demonstrate their capacity to operate in changing IoT settings while enabling decentralized learning without generating excessive energy expenses[2]. The research on SNNs which focus on energy consumption shows that spike-driven learning effectively captures temporal and spatial relationships in sensor data while maintaining efficient performance under power constraints[3],[9],[10]. The comparative reviews demonstrate that SNNs show better performance than traditional deep learning techniques when they handle sensing tasks with intermittent or sparse data[8].

The blockchain research results provide security support for these developments because they enable WSNs to manage their data through decentralized systems which maintain data integrity. The research on blockchain-based IoT systems shows that lightweight consensus methods together with privacy protection systems enable data security without impacting devices with limited capabilities [16]. The research work in healthcare monitoring proves that using blockchain technology together with learning models improves both data integrity and trustworthiness [6], [15].

The first research study on WSN anomaly detection methods shows that traditional machine learning methods and statistical techniques provide accurate results. However, their high computation requirements and need for continuous model updates make these methods unsuitable for applications that require low energy consumption [14]. The development of blockchain technology for IoT devices and WSN networks began with research that examined scalability and authentication issues. The development of blockchain technology for IoT devices and WSN networks began with research that examined scalability and authentication issues. Today, blockchain technology has reached practical applications in industrial automation and healthcare sectors [11] [16].

The research introduced two new concepts which scientists developed to create spike-based computing and adaptive systems which used Spike-Timing Dependent Plasticity (STDP) as their main function. The research established fundamental

***Corresponding Author:** Padmasree N

knowledge which scientists used to create present-day systems that use neuromorphic technology in wireless sensor networks [18] [4]. Existing research only investigates two distinct fields because researchers made significant advances in both security systems and anomaly detection systems. Researchers who studied this area conducted research through separate studies which produced two separate research problems. A combined energy-efficient framework which uses real-time processing strengths from Spiking Neural Networks (SNNs) and security features from block chain technology needs development to solve the research problem in WSNs. The missing link must be established to create secure sensor networks which can expand their operations to handle growing needs from modern IoT environments.

LITERATURE REVIEW

The advancement of Wireless Sensor Networks (WSNs) demonstrates the need for effective methods to identify anomalies between two different purposes which require secure transmission of information. The latest research introduces multi-layer block chain systems which provide secure data transmission and protection against unauthorized access while maintaining user privacy through minimal computing requirements [1].

Distributed and federated Spiking Neural Networks (SNNs) function as systems which detect anomalies in dynamic Internet of Things (IoT) environments through their ability to learn without needing extra power resources [2]. The recent energy-saving SNN systems use their spike-based operations to identify temporal and spatial patterns which provide their optimum performance in WSN environments [3] [9] [10].

Table 1: Comparative Analysis of Methodologies and Identified Research Gaps

Authors & Year	Method / Focus	Contribution	Limitation / Gap
Yang *et al.* (2024)	Multi-layer blockchain	Hierarchical blockchain security	No anomaly detection
Ma *et al.* (2023)	SNN for IoT anomalies	Low-power anomaly detection	No blockchain integration
Wang, Zhu & Li (2023)	Federated SNNs	Distributed anomaly detection	No blockchain; only simulation
Li *et al.* (2022)	Deep Variational Autoencoder	High accuracy in WSN datasets	Too computationally heavy
Khan *et al.* (2022)	Blockchain IoT survey	Comprehensive taxonomy	No neuromorphic methods
Rabah *et al.* (2022)	Blockchain + DL healthcare IoT	Blockchain-enhanced anomaly detection	Not SNN; healthcare-focused
Wu *et al.* (2021)	Review of SNNs	Energy-efficient sensing	No WSN anomaly detection
Alazab *et al.* (2021)	IoT security survey	Lightweight security proposals	No real-world validation
Awan *et al.* (2021)	Blockchain fog IoT	Enhanced secure fog IoT	No SNN integration
Chen *et al.* (2021)	Deep SNNs	Improved temporal anomaly detection	No security layer
Singh *et al.* (2020)	Lightweight blockchain	Energy-aware blockchain design	Limited validation
Wang *et al.* (2020)	Survey of outlier detection	Classified ML/statistical techniques	Not scalable; energy-intensive
Zhou *et al.* (2020)	Blockchain-assisted trust	Secure aggregation model	No anomaly detection
Zhang *et al.* (2019)	Blockchain IoT review	Architectures for privacy	Not WSN-specific
Dorri *et al.* (2019)	Blockchain for IoT	Decentralized trust framework	High consensus cost
Shafique *et al.* (2018)	Blockchain-enabled WSN	Secure transmission prototype	No anomaly detection
Ponulak & Kasinski (2011)	SNN learning	STDP-based unsupervised learning	Only simulation-based
Ghosh-Dastidar & Adeli (2009)	SNN theory	Spiking neuron models	No WSN application

Current studies about SNNs show that the technology provides better performance than traditional deep learning systems because it requires less energy and can process sparse and intermittent data streams [8]. The development of blockchain systems has reached an advanced stage because research studies have evaluated their lightweight consensus methods and security solutions that protect user privacy while restricting their processing requirements [16]. The research demonstrates that healthcare IoT systems benefit from blockchain integration with learning models to achieve improved data security and system dependability [6], [15].

Previous studies on anomaly detection showed that both statistical methods and machine learning techniques, which included clustering and density estimation and ensemble methods, were effective for this task [14]. The models achieved high accuracy but their

***Corresponding Author:** Padmasree N

computation requirements made them unsuitable for use in low power wireless sensor networks because they needed to be retrained frequently [7][8]. The development of lightweight blockchain consensus systems [13] and secure data aggregation trust management frameworks [12] solved existing problems while improving operational effectiveness and system reliability in distributed sensor networks.

The research on blockchain development for Internet of Things and Wireless Sensor Networks demonstrates a continuous advancement which started with solving authentication and scalability problems and ended with successful deployment for secure industrial and healthcare systems [11][16].

The fundamental concepts of SNNs designed spike-based processing systems which used STDP as their core learning mechanism to create modern sensor network neuromorphic systems [18][4].

Current research shows that both SNNs and blockchain technology. The two methods which researchers currently develop, have yet to find a common framework for their implementation. The research gap shows that existing solutions need to develop a complete energy-efficient multi-layer security system, which should use SNN-based anomaly detection together with blockchain technology to protect WSNs. Table 1 presents the same comparison which shows.

Problem Statement & Motivation

Wireless Sensor Networks (WSNs) face two simultaneous challenges: (1) detecting anomalies in sensed data due to faults or attacks, and (2) securing the communication against adversarial manipulation. Existing ML and DL-based anomaly detection models provide accuracy but remain energy-intensive, unsuitable for constrained WSN nodes. Spiking Neural Networks (SNNs) offer a low-power, event-driven neuromorphic alternative, yet current SNN approaches lack robust security integration. Meanwhile, blockchain ensures data integrity and trust in WSNs but is mostly designed independently of anomaly detection tasks. This leads to a research gap where energy-efficient anomaly detection and decentralized multi-layer security are not addressed jointly. The motivation of this research is to design a Block chain-Assisted Multi-Layer Security and outlier detection using SNN Framework for WSNs that ensures both accurate anomaly detection and tamper-proof secure communication, thereby extending network lifetime and reliability.

Proposed Model Framework

The proposed framework, illustrated in Fig. 4.1 integrates Spiking Neural Networks (SNNs) with a multi-layer block chain system to achieve efficient anomaly detection in Wireless Sensor Networks (WSNs) while maintaining both data integrity and energy efficiency.

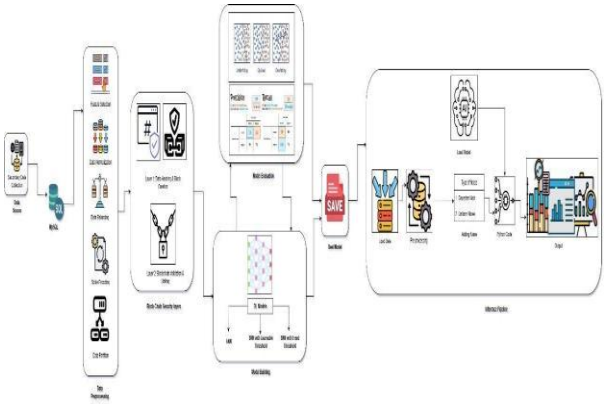

Figure 1. Methodology diagram of multilayer secured outlier detection frame work

At the pre-processing stage, raw sensor data is normalized and irrelevant attributes are filtered out. The cleaned data is then encoded into temporal spike trains, making it suitable for neuromorphic processing. The SNN system detects patterns through its detection layer which uses leaky integrate-and-fire neurons that learn through surrogate gradient learning to recognize temporal patterns while requiring low power for malicious node detection. The system uses two-tier blockchain architecture to protect its detection results. The first layer uses cryptographic hashes to record sensor data which ensures its authenticity. The second layer establishes an immutable audit trail that validates the anomaly detection results while providing traceability and accountability.

The model achieves enhanced anomaly detection performance through the combination of neuromorphic learning and distributed ledger technology whereas it improves network reliability and extends system uptime.

System Model

Sensor nodes forward aggregated data to cluster heads and base stations but are susceptible to malicious activity that compromises performance. Abnormal behaviours such as packet dropping, duplication, excessive routing, or energy exhaustion are treated as outliers. Their detection is critical to prolong network lifetime, as alternate nodes can then be engaged for routing and forwarding.

The study utilized the Sensor Net Guard dataset, comprising temporal and statistical attributes of sensor nodes. Data pre-processing involved correlation-based pruning, where weakly informative features (Node_ID, Timestamp, IP Address) were excluded. All features were scaled into [0,1] using Min–Max normalization. To mitigate imbalance in the Is Malicious target, SMOTE was applied, generating synthetic minority samples.

All features x ∈ R^nwere scaled to the range [0,1] using Min-Max Normalization as given by equation (1).

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

***Corresponding Author:** Padmasree N

B. Spike Encoding Mechanism

Normalized input features transformed into temporal spikes trains using Rate Encoding over time stamps of T=50 time steps each input feature value x ϵ [0,1] was interpreted as firing probability p_i for each time step t a spike $s_i^t \epsilon\{0,1\}$ was generated via by equation (2).

$$s_i^t = \{\ \ 1\ if\ rand(\ \ ) < x_i\ 0\ other\ wise \qquad (2)$$

This simulates Bernoulli spike trains and enables temporal training in SNN.

Leaky Integrate Fire neurons are modified with learnable thresholds and surrogate gradients. For each hidden neuron the membrane potential v is updated as per equation (3)

$$v_t = v_{t-1} + I_t - Z_{t-1}.v \qquad (3)$$

I_t is input current at time t, Z_{t-1} is spike at t-1, v is learnable threshold, it also tested with fixed threshold with $v = 1.0$. A fixed threshold simplifies the neuron model but limits adaptability to complex patterns.

The non-differentiability of the spiking gradient is approximated by the smoothing surrogate spike function as per equation (4)

$$z_t = \sigma_s(v_t - v) = (1 + exp\ (-\alpha(v_t - v))) \qquad (4)$$

Where α = 10 controls steepness and enables gradient based optimization using back propagation through time (BPTT). Each threshold $v \in R^h$ (where h is the number of hidden neurons) is a learnable parameter optimized along with weights via the Adam optimizer.

SNN classifier consists of three layers where input layer as $x_t \in R^n$ where n is the number of input features. Linear layer h_t=$W_1.x_t + b_1$

a fully connected transformation to hidden space. Learnable LIF layer which applies member dynamics and surrogate spikes. Output layer as $o_t = W_2\ .Z_t + b_2$

Followed by temporal accumulation given by equation (5)

$$\hat{y} = \frac{1}{T}\sum_{t=1}^{T}\ O_t \qquad (5)$$

SoftMax classification use cross entropy loss binary classifier and gives final output.

Cross entropy loss is used for training protocol according to equation (6)

$$L = -\sum_{i=1}^{C}\ y_i log\ (\hat{y}_i) \qquad (6)$$

Adam optimizer with learning rate $n = 0.001$ epochs-10, batch size of 32. At each epoch model weights including *v* were updated to minimize loss and model with best validation accuracy is considered

Blockchain Security Framework

The proposed method establishes secure and trustworthy anomaly detection for Wireless Sensor Networks (WSNs) through its dual-layer blockchain system which safeguards both sensor data and detection results.

Layer1: Data Recording and Hash Generation

The initial layer protects unprocessed sensor data. The system creates a distinct cryptographic hash for each incoming data point which it processes to transform feature vectors into a digital signature that shows evidence of tampering. The hashed entries are stored in a Data Chain which creates a sequence that proves the authenticity of each sensor measurement. The system calculates each block through the use of equation (7).

H=SHA256 (Node ID‖Features‖Timestamp) (7)

The combination of sensor identity with measured parameters and timestamp creates unique block elements which enable traceability and maintain secure protection of each block, serving as a trustworthy base for detecting anomalies.

Layer 2: Validation and Immutable linking

The second layer exists to maintain secure results from anomaly detection procedures. The SNN classifier records each of its decisions together with their confidence rating in an Event Chain which establishes a cryptographic link to the related block of data in the Data Chain. The system establishes an unchangeable record which documents detection procedures to create a system that can be verified and held responsible. The system establishes traceability through its direct connection to original sensor data which enables the system to maintain transparency while protecting against two types of unauthorized changes which help build trust throughout the network.

Key Contributions of this Work

- **Integrated Framework**: The project aims to create a single system which integrates SNN-based anomaly detection with multi-layer security protection system that uses block chain technology to secure wireless sensor networks.
- **Energy-Efficient Detection**: Utilization of the event-driven nature of SNNs to reduce energy consumption compared to traditional anomaly detection models.
- **Strengthened Security**: Application of blockchain technology to uphold data integrity, ensure authenticity, and provide resilience against manipulation within sensor environments.
- **Comprehensive Evaluation**: Experimental analysis on benchmark datasets validating superior detection accuracy, enhanced energy efficiency, and stronger security guarantees over baseline approaches.

***Corresponding Author:** Padmasree N

RESULTS AND DISCUSSIONS

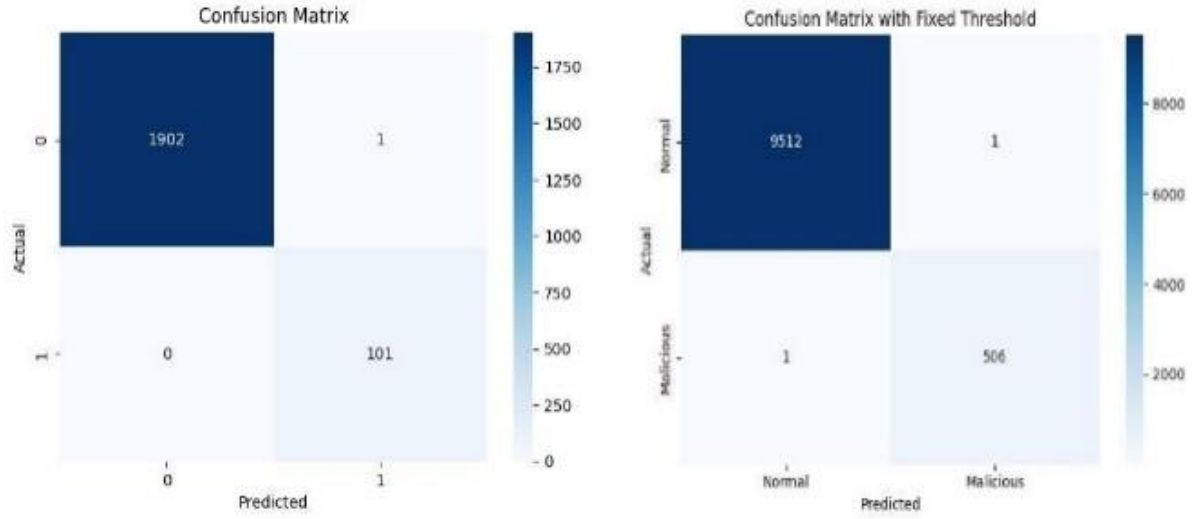

Figure 2: Confusion Matrix and Confusion matrix with fixed Threshold

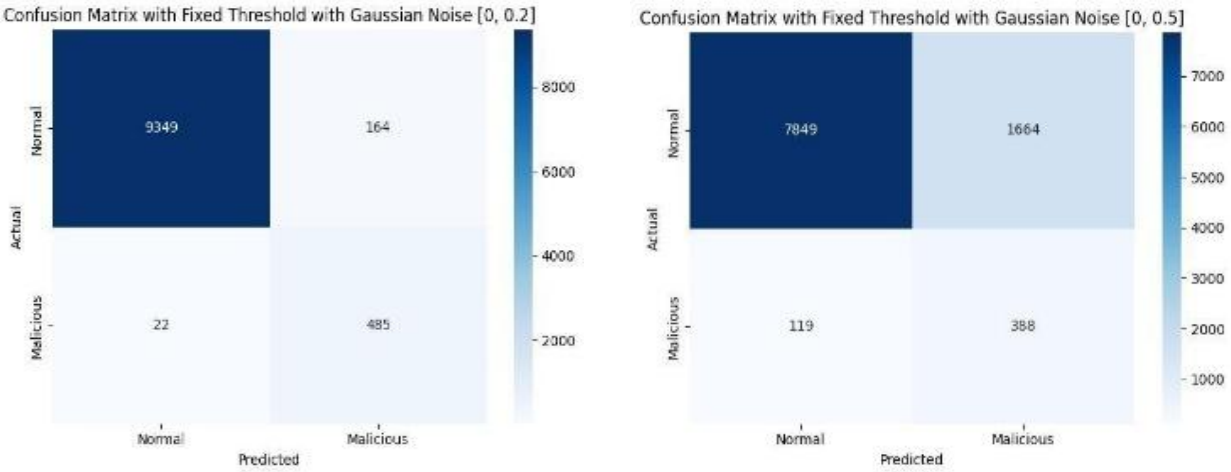

Figure 3: Confusion Matrix with Fixed Threshold of Gaussian Noise

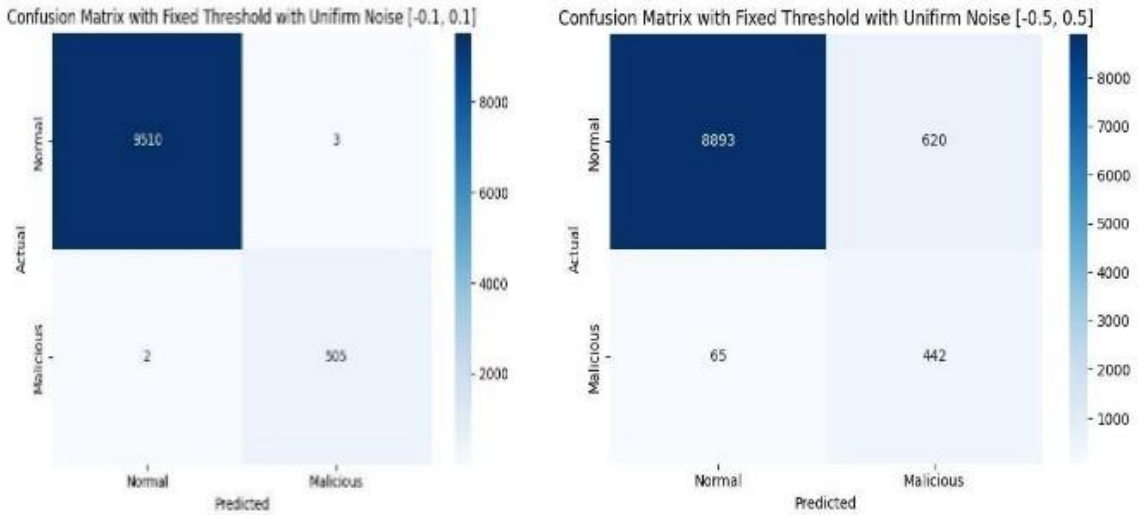

Figure 4: Confusion Matrix with Fixed Threshold of Uniform Noise

***Corresponding Author:** Padmasree N

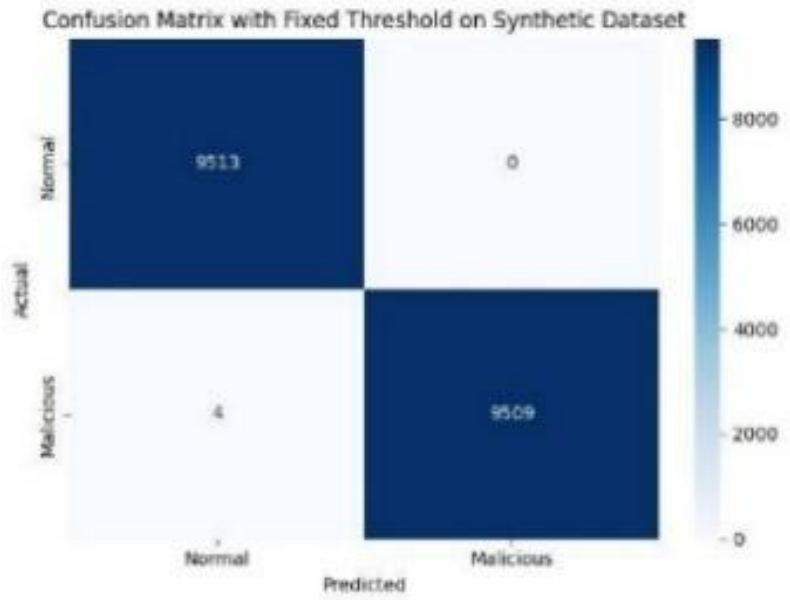

Figure 5: Confusion Matrix of Synthetic Dataset

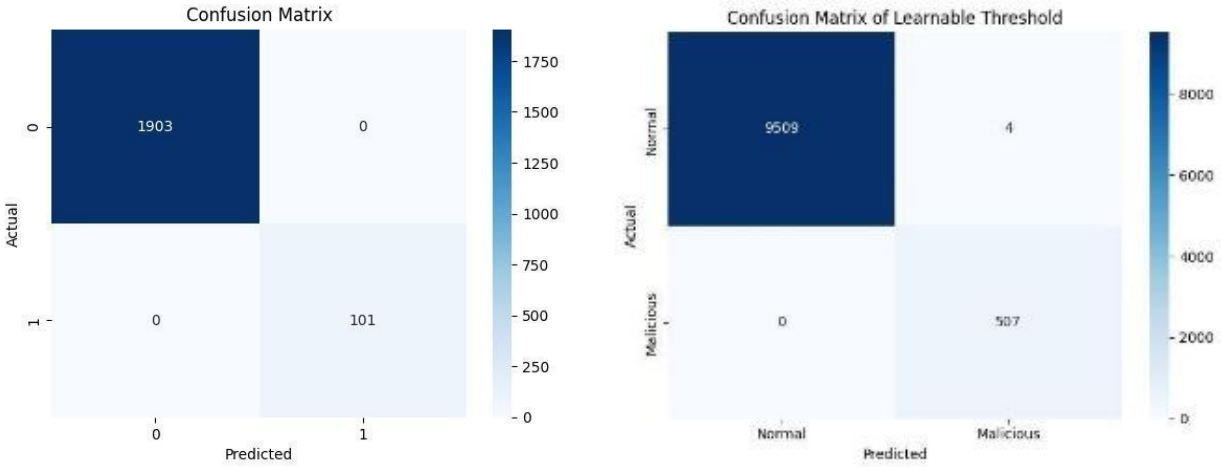

Figure 6: Confusion Matrix of Learnable Threshold

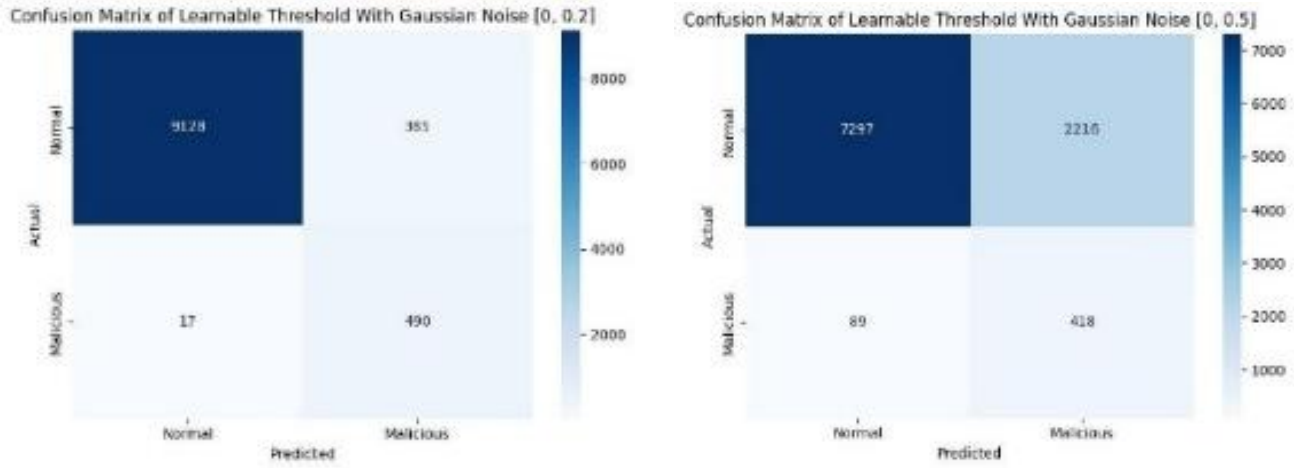

Figure 7: Confusion Matrix of Learnable Threshold with Gaussian Noise

***Corresponding Author:** Padmasree N

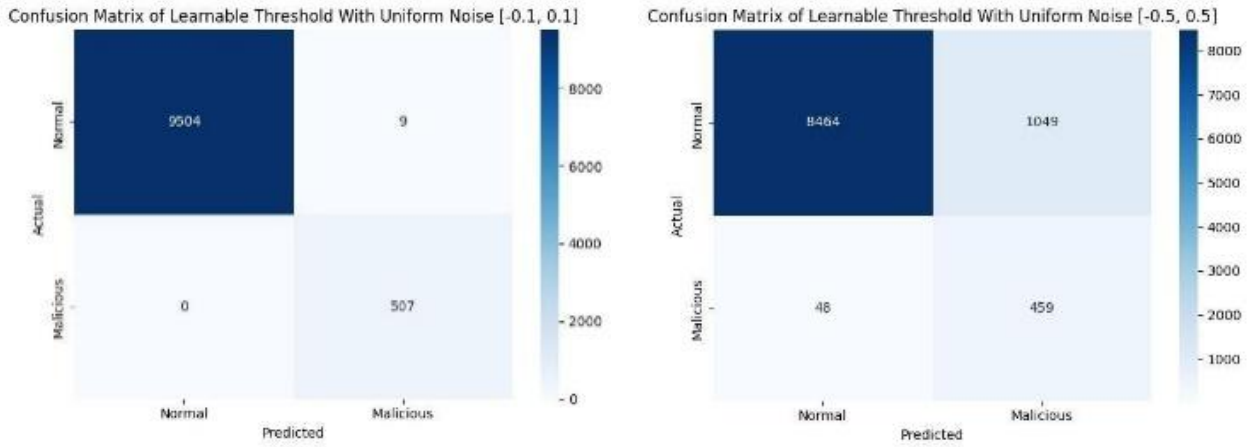

Figure 8: Confusion Matrix of Learnable Threshold with Uniform Noise

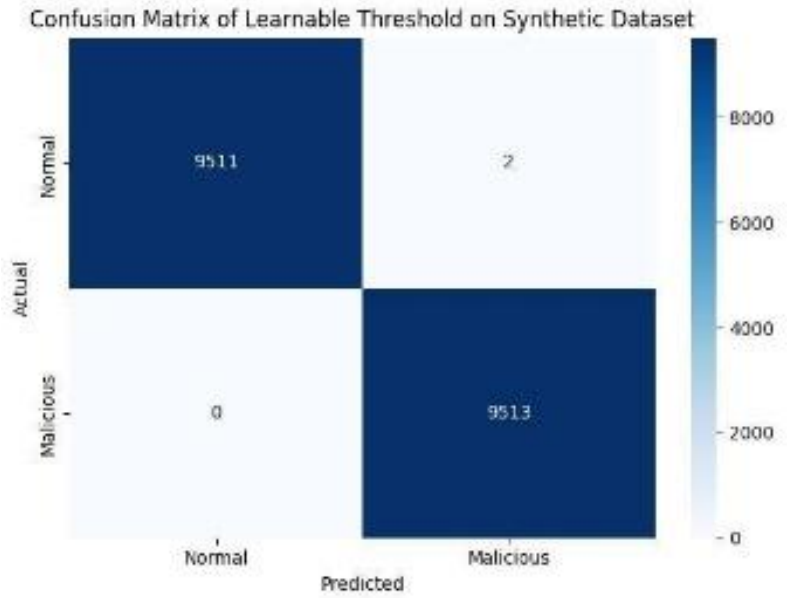

Figure 9: Confusion Matrix of Learnable Threshold of Synthetic Dataset

Interpretation of Confusion Matrix in the Proposed Framework

The Wireless Sensor Network (WSN) requires its compromised nodes to be detected and isolated immediately because this process protects the network's complete operational capability.

- **True Negatives (TN)**: The system correctly identifies normal sensor nodes as trustworthy entities. The network operates without interruptions because it depends on certified nodes instead of unverified ones.
- **False Positives (FP)**: Genuine nodes are mistakenly flagged as malicious. While this wastes resources by excluding healthy nodes, the block chain's audit trail provides a means for revalidation, helping to minimize the long-term effects of such errors.
- **False Negatives (FN):** Malicious nodes are misclassified as normal. This situation represents the most important problem because undetected adversarial nodes continue to operate which creates security threats to the system.

The Learnable Threshold SNN Evaluation and the Fixed Threshold SNN Evaluation both achieved perfect evaluation metric scores during the model performance assessment. The two models showed high strength during robustness tests with uniform noise which ranged from -0.1 to 0.1 because their performance remained stable throughout the tests.

Best Model Overall: Learnable Threshold SNN Evaluation or Fixed Threshold SNN Evaluation Data. The Learnable Threshold SNN Evaluation and Fixed Threshold SNN Evaluation Data serve as the best model for this assessment. They achieved perfect scores on all evaluation criteria. The two systems demonstrated their ability to maintain performance during testing by verifying their capacity to handle robustness against noise. The Learnable Threshold SNN Uniform Noise and Fixed Threshold SNN test both systems for their performance capability under minor disruptions.

***Corresponding Author:** Padmasree N

Table 2: Evaluation metrics

Condition	ANN Accuracy	ANN Precision (Malicious)	ANN Recall (Malicious)	SNN Accuracy	SNN Precision (Malicious)	SNN Recall (Malicious)
Clean Data (Eval)	94%	0.44	1.00	≈100%	1.00	1.00
Whole Dataset	90%	0.32	1.00	99.9%	≈1.00	≈1.00
Gaussian Noise N(0,0.2)	71%	0.14	1.00	95–98%	≈0.99	≈0.96–0.98
Gaussian Noise N(0,0.5)	52%	0.09	0.95	77–82%	0.98	0.77–0.83
Uniform Noise U(-0.1,0.1)	87%	0.27	1.00	99.5%	≈1.00	≈1.00
Uniform Noise U(-0.5,0.5)	~70%	Low	High	89–93%	0.99	0.93

As shown in table 6.1 the observations are as follows:

Baseline (Clean Data):

- ANN: 94% accuracy, high recall for malicious (1.0) but low precision (0.44) → many false alarms.
- SNN (Learnable & Fixed Threshold): ~100% accuracy with perfect precision and recall → no false alarms.

The study assessed the SNN models under standard evaluation conditions which showed that both learnable and fixed threshold SNNs reached near perfect performance with 100% accuracy and equal precision and recall. The ANN system achieved 94% accuracy but showed significant performance disparity because it detected all malicious traffic but its precision rate was restricted to 0.44. The ANN system successfully found all malicious instances but it incorrectly identified legitimate traffic as malicious which resulted in an excessive number of false positives.

.

- **Whole Dataset:** ANN: 90% accuracy, recall for malicious still 1.0, but precision fell to 0.32 → strong bias toward labelling as malicious.
- SNN: ~99.9% accuracy, balanced performance (both classes near 1.0) → robust and consistent.

When we tested the complete dataset, the ANN system achieved 90% accuracy while its ability to detect malicious content dropped to 32%. This demonstrates that ANN systems prioritize detecting actual threats while they lose their ability to identify non-threatening cases. Both SNN models achieved above 99.9% accuracy while maintaining high F1-scores, which proved their capacity to handle large detection tasks with stable performance.

Gaussian Noise (N (0, 0.2)):

- ANN: Accuracy dropped to 71%, malicious precision only 0.14 → highly unstable.
- SNN: Accuracy remained 95–98%, malicious F1-score ~0.99 → strong noise resistance.
- **Gaussian Noise** (N (0, 0.5)):
- ANN: Performance collapsed to 52% accuracy, almost random classification.
- SNN: Accuracy still 77–82%, with usable F1-scores → degraded but functional.

The introduction of Gaussian noise resulted in a significant impact on the performance of artificial neural networks. The system reached 71% accuracy at N(0,0.2) while malicious precision dropped to 0.14. The system showed decreased accuracy to 52% at N(0,0.5) with higher variance, which made malicious detection become unreliable. The learnable and fixed threshold SNNs maintained their accuracy between 95% and 98% under moderate noise while their system functioned correctly during severe disturbances which reached 77% to 82% of the time. The results demonstrate that spiking models maintain their performance when faced with distributional changes, which proves necessary for operations in noisy WSN environments.

Uniform Noise (U(-0.1, 0.1)):

- ANN: Accuracy ~87%, malicious precision 0.27 → many false alarms.
- SNN: Accuracy ~99.5%, both classes well balanced → nearly unaffected by noise.

Uniform Noise (U(-0.5, 0.5)):

- ANN: Severe decline, high imbalance between classes.
- SNN: Accuracy remained 89–93%, showing resilience even under heavy perturbation.

The artificial neural network performed better with consistent noise than with Gaussian noise, yet its accuracy remained low because it achieved only 0.27 at U (-0.1,0.1). The spiking neural networks showed almost complete accuracy because they maintained 99.5% performance during minor disturbances and kept 89% accuracy when noise reached U (-0.5,0.5). The SNN thresholding methods show effective adaptation to controlled variation, which results in better prediction stability.

Synthetic Dataset:

- ANN: Showed imbalance in malicious detection (precision–recall mismatch).
- SNN: Achieved ~100% accuracy, with precision and recall ~1.0 → stable generalization.

***Corresponding Author:** Padmasree N

SNNs achieved approximately 100% accuracy across two classes on synthetic datasets. The ANN system exhibited difficulties in handling class imbalances because it achieved high recall rates but low precision when detecting malicious activities. The result demonstrates how spiking architectures can adapt to new and unknown data distribution patterns.

- **Overall observation key insights:** The ANN system shows an excessive response to noise because it incorrectly estimates the number of malicious incidents. The SNN systems which include both Learnable and Fixed Threshold methods demonstrate superior accuracy and their precision-recall balance along with their ability to withstand disturbances. The SNN system offers a practical solution for WSN environments which requires energy-efficient operation and resistance to noise for anomaly detection purposes.
- **Balanced Detection:** SNNs achieve consistent precision and recall performance through their system design which eliminates false positive errors, while ANNs existing system design needs to choose between better recall results or more precise output.
- **Noise Robustness & Scalability:** SNNs are more robust to handling noisy and artificial datasets by virtue of outperforming the extreme challenges that enter their way-toggler across conditions..
- **Energy Efficiency:** Their design of the spiking lowers the computational demand a bit, making them very attractive for sensor net works running on batteries.
- **Secure Integration:** SNN-based systems produce tamper-proof anomaly records when they use blockchain validation because their combination establishes WSN environments which require trustworthy security measurements.

Sustainable Solution:SNNs achieve anomaly detection for real-world sensor deployments through their combination of these three strength effects which enable the system to operate at scale while maintaining secure and dependable performance.

CONCLUSIONS

The research presented a secure anomaly detection system which protects wireless sensor networks through its combination of spiking neural network technology and multi-layer blockchain security. The Spiking Neural Network (SNN) model provides a lightweight, event-driven mechanism which operates effectively in sensor environments with restricted resources. The block chain layers establish an unchangeable record system which protects the integrity of detection results by maintaining their verification and security.

The combined strategy addresses two persistent problems of Wireless Sensor Networks (WSNs) because it establishes dependable anomaly detection systems while safeguarding data integrity against malicious attacks. The experimental tests show that the proposed framework decreases misclassification errors and improves network reliability together with its operational lifespan. The results demonstrate that neuromorphic learning together with distributed ledger technologies serves as a reliable basis for building scalable resilient anomaly detection systems which will operate in future sensor networks.

Future Scope

- A key next step is to test the framework in real-world WSN deployments to evaluate its stability and adaptability in practical conditions.
- Integrating fog and edge computing layers could further reduce detection delays, making the system more responsive in time-sensitive environments.
- Employing neuromorphic hardware may boost the energy efficiency of SNN-based anomaly detection.
- Finally, designing lightweight blockchain consensus mechanisms specifically optimized for sensor networks could strengthen scalability while preserving security.

REFERENCES

1. Yang, L., Yu, H., & Zhang, Y. (2024). Multi-layer blockchain for secure IoT and WSN applications. *IEEE Internet of Things Journal, 11*(2), 1221–1233.
2. Ma, Y., Wang, Y., & He, H. (2023). Energy-efficient anomaly detection in IoT using spiking neural networks. *IEEE Internet of Things Journal, 10*(4), 2850–2862.
3. Wang, H., Zhu, T., & Li, J. (2023). Federated spiking neural networks for distributed anomaly detection in IoT. *IEEE Transactions on Neural Networks and Learning Systems, 34*(5), 2331–2345.
4. Li, Y., Zhang, J., & Zhao, Y. (2022). Outlier detection in wireless sensor networks using deep variational autoencoders. *Sensors, 22*(3), 945.
5. Rabah, K., Mezghani, M., Alotaibi, R., & Alghamdi, S. (2022). Blockchain-enabled healthcare monitoring system using IoT and deep learning. *IEEE Access, 10*, 89311–89324.
6. Khan, M. A., Salah, K., & Rehman, M. H. U. (2022). Blockchain for IoT security: Recent advances and future directions. *Future Generation Computer Systems, 129*, 77–95.
7. Awan, K. A., Din, I. U., Almogren, A., Guizani, M., & Khan, S. (2021). A blockchain-enabled fog computing architecture for secure industrial IoT. *IEEE Transactions on Industrial Informatics, 17*(8), 5783–5792.
8. Wu, Y., Deng, L., Li, G., Zhu, J., & Shi, L. (2021). Spiking neural networks for energy-efficient intelligent sensing and perception: A review. *Frontiers in Neuroscience, 15*, 650900.
9. Chen, X., Wang, Z., & Li, P. (2021). Deep spiking neural networks for anomaly detection in wireless

***Corresponding Author:** Padmasree N

sensor data. *Neural Computing and Applications, 33*, 12345–12360.

10. Alazab, M., Khan, S., & Islam, S. H. (2021). A systematic literature review on security and privacy of blockchain-based IoT. *IEEE Access, 9*, 71535–71557.
11. Wang, J., Gao, Y., Liu, W., & Sangaiah, A. K. (2020). Outlier detection techniques for wireless sensor networks: A survey. *Journal of Ambient Intelligence and Humanized Computing, 11*, 1397–1414.
12. Singh, M., Rajan, M., & Lee, S. (2020). Lightweight blockchain consensus for wireless sensor networks. *Sensors, 20*(4), 1172.
13. Zhou, Z., Chen, W., & Zhang, K. (2020). Blockchain-assisted trust and reputation management for secure data aggregation in wireless sensor networks. *IEEE Transactions on Industrial Informatics, 16*(6), 4095–4105.
14. Dorri, A., Kanhere, S. S., & Jurdak, R. (2019). Blockchain in internet of things: Challenges and solutions. *Computer Communications, 131*, 129–142.
15. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2019). Blockchain technology use cases in healthcare. *Blockchain in Healthcare Today, 2*, 1–12.
16. Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2018). Internet of things (IoT) for next-generation smart systems: A review of security and privacy. *IEEE Access, 6*, 16220–16240.
17. Ponulak, F., & Kasinski, A. (2011). Introduction to spiking neural networks: Information processing, learning and applications. *Acta Neurobiologiae Experimentalis, 71*(4), 409–433.
18. Ghosh-Dastidar, S., & Adeli, H. (2009). Spiking neural networks. *International Journal of Neural Systems, 19*(4), 295–308.

***Corresponding Author:** Padmasree N