International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-15 Issue-4, April 2026

Integrated Collaborative Intrusion Detection System Using Ensemble Learning Algorithms

Pramod A. Jadhav, Nitin Sale, Vinod H. Patil, A. Y. Prabhakar, Chetan More

Abstract: ***As the internet-connected systems have expanded, albeit briefly, intrusion detection systems (IDS) have become an important element in cybersecurity. Conventional host-based and network-based IDS systems are unable to detect advanced and distributed attacks promptly. Collaborative Intrusion Detection Systems (CIDS) enhance precision by enabling nodes to share intelligence. Nevertheless, CIDS usually have issues associated with secure data sharing and trust. To overcome these constraints, this paper presents a smart, collaborative intrusion detection system based on the Ethereum blockchain. Decentralised trust, data immutability, and the absence of a central authority are guaranteed through blockchain integration. Both the signature-matching and fuzzy genetic algorithms are machine learning algorithms used in anomaly- and signature-based intrusion detection. Datasets such as NSL-KDD, CIC IDS 2017, and CIC IDS 2018 are used to assess the system's performance. Findings show better accuracy, fewer false positives and greater resilience in the multi-node environments. The suggested architecture will include IDS tools such as Snort, Zeek, and Suricata, and will be combined with smart contracts to enable secure cooperation. The given work contributes to the development of the field by combining AI, blockchain, and CIDs to provide a new solution to the current threats posed by cybersecurity violations in distributed networks.***

Keywords: Intrusion Detection System, Collaborative IDS, Blockchain, Ethereum, Machine Learning, Signature Matching, Fuzzy Genetic Algorithm, Network Security, Smart Contracts.

Nomenclature:
IDS: Intrusion Detection Systems
CIDS: Collaborative Intrusion Detection Systems
IDSs: Intrusion Detection Systems
RF: Random Forest
SVMs: Support Vector Machines
KNN: K-Nearest Neighbours

Manuscript received on 25 March 2026 | First Revised Manuscript received on 02 April 2026 | Second Revised Manuscript received on 07 April 2026 | Manuscript Accepted on 15 April 2026 | Manuscript published on 30 April 2026.

*Correspondence Author(s)
Dr. Pramod Jadhav, Associate Professor, Department of Computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: pajadhav@bvucoep.edu.in
Nitin Sale, Research Scholar, Department of Computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: nitinsale139@gmail.com
Dr. Vinod H. Patil*, Researcher, Department of Electronics and Telecommunication Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: vhpatil@bvucoep.edu.in, ORCID ID: 0000-0002-3328-9248
Dr. A Y Prabhakar, Professor, Department of Electronics and Telecommunication Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: ayprabhakar@bvucoep.edu.in
Dr. Chetan More, Assistant Professor, Department of Electronics and Telecommunication Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: csmore@bvucoep.edu.in

I. INTRODUCTION

The rate of growth in internet usage has been exponentially high; the susceptibility of systems and networks to hacking has been on the rise. Intrusion Detection Systems (IDS) are an essential component of computer network security today, as they detect unauthorised access and malicious activity. The broad categories of deployment and detection approaches are used to classify IDS. Host-based IDS (HIDS) are used to check for suspicious activity on individual systems. In contrast, network-based IDS (NIDS) are used to monitor network traffic to identify any indication of intrusion activity. Also, there can be signature-based and anomaly-based IDS. IDS signature-based IDS identifies intrusions by matching observed activities to a database of known threat patterns. Conversely, anomaly-based IDS detect abnormal behaviour by creating a baseline of normal behaviour and identifying deviations from it.

Nonetheless, single IDS models, however sophisticated they may be, are no longer sufficient to address distributed and evolving cyber threats. Lack of integration between Detection systems may fail to prevent advanced attacks, thereby compromising the integrity of organizations networks. To overcome this weakness, a Collaborative Intrusion Detection System (CIDS) has emerged in which the different IDS nodes interact to enhance detection capabilities. CIDS allows nodes to share mistreatment information with alerts, logs, and threat intelligence, providing a broader view of threats that may occur in a network. CIDS, however, introduces new challenges and trade-offs, primarily in data sharing and trust management. Due to privacy concerns, nodes may not voluntarily provide sensitive information, leading to insider attacks on the system. Such problems require a decentralized and secure and tamper resistant data exchange mechanism. Another solution is provided by blockchain technology, which was initially developed to facilitate the transfer of cryptocurrencies [1]. It offers an unalterable, open, decentralised registry. Trust is achieved through the implementation of blockchain in CIDS, which does not require a central authority. Every transaction, including intrusion alerts, is checked and stored on the blockchain, ensuring data integrity and resistance to manipulation. Ethernet, which supports smart contracts, also helps improve this system by automating data validation and data-sharing protocols.

Machine learning is an essential component of the proposed system. Signature matching and fuzzy genetic algorithms are among the algorithms used to detect both known and unknown threats. The algorithms analyse

traffic data to identify patterns that may indicate malicious activity. The system will be able to react more efficiently to new threats than the rule-based methods because it constantly learns and evolves.

The proposed intelligent collaborative intrusion detection system is tested using benchmark datasets such as NSL-KDD, CIC IDS 2017, and CIC IDS 2018. The outcomes show a decrease in false positives, more accurate detection, and increased collaborative efficiency, yielding better results than conventional IDS approaches [10]. Traffic analysis is performed using tools such as Snort, Suricata, and Zeek; secure exchange of alerts and logs is enabled via Ethereum-based smart contracts. The purpose of this paper is to contribute to the cybersecurity field and propose an integrated approach to the integration of machine learning and blockchain technology for use in a joint detection system. The resulting product is a safe, precise, and scalable system that can meet current cybersecurity challenges in a decentralised environment [8] [9].

II. PROBLEM STATEMENT

Even though Intrusion Detection Systems (IDSs) have improved, the existing architectures, whether standalone or collaborative, have major limitations. Traditional IDS have difficulty identifying complex and distributed attacks because they are isolated. In contrast, Collaborative Intrusion Detection Systems (CIDS), though effective, face challenges in data privacy, trust management, and resistance to tampering. The nodes in CIDS may be reluctant to provide confidential information due to concerns about privacy invasion or ill intent. Additionally, in the absence of a trusted, decentralised trust system, insider threats and data alteration are also high risks. A secure, intelligent, and decentralised CIDS is demanded that guarantees trust, data integrity, and cooperative efficiency, while also achieving a high intrusion-detection rate and a low false-positive rate. There is a potential solution in combining blockchain technology and machine learning to eliminate these shortcomings.

III. LITERATURE REVIEW

The combination of blockchain and collaborative IDS is currently under active study in recent research. S. R. A hybrid IDS model, named BC-HyIDS, was proposed by Khonde and V. Ulagamuthalvi (2022) to have a blockchain-enhanced signature exchange and has shown a high accuracy and low false alarms [2]. According to Meng (2018), collaborative IDS faces major challenges related to trust management and secure data sharing and proposes blockchain as a means of safe alert exchange [3]. Salam Al-E'mari (2022) reviewed blockchain-based IDS frameworks, identifying scalability and cost as areas for improvement [4]. According to H. Guo and X. Yu (2022), they examined how consensus algorithms can be used to guarantee data integrity in blockchain-enhanced IDS [5].

R. Xing and colleagues (2024) and Govindaram et al. (2024) have also made significant contributions to the field; specifically, the former developed a blockchain-based collaborative Internet of Vehicles intrusion detection system (IDS), and the latter proposed a federated learning methodology leveraging blockchain for IoT-centric IDS [6][7]. These investigations highlight the increasing significance of decentralized and intelligent IDS designs. Notwithstanding these developments, the practical implementation of blockchain-CIDS systems in real-time scenarios, as well as the optimisation of energy consumption, remain areas of limited exploration [16], revealing a research void that this study aims to fill.

IV. PROPOSED METHODOLOGY

The proposed methodology combines collaborative IDS, blockchain, and machine learning solutions to establish a secure, scalable, and intelligent intrusion detection system [11]. The major elements of the methodology are:

Data Collection: Snort, Suricata, and Zeek are popular IDS tools for collecting network traffic data. The tools produce alerts and logs in response to identified anomalies and recognised signature threats.

The NSL-KDD, CIC IDS 2017, and CIC IDS 2018 datasets undergo preprocessing to remove noise and normalise features. Feature selection is performed to retain only the relevant features.

Machine Learning Algorithms: There are three algorithms:

A. Collaborative IDS (CIDS): A decentralized detection system in which nodes broadcast alerts to other nodes to enhance detection [12].

B. Random Forest (RF): This technique is an ensemble learning method that builds several decision trees and votes by a majority.

C. Support Vector Machines (SVMs) and K-Nearest Neighbours (KNNs) are compared.

D. Blockchain Integration: There is an Ethereum blockchain that holds intrusion alerts and logs safely. The IDS nodes post the alerts they detect, in the form of transactions, to the blockchain. Smart contracts automatically validate and disseminate alerts between nodes.

E. Smart Contracts: Smart contracts ensure that only authorised nodes can participate in and contribute to alerts. They maintain node reputations and implement collaboration policies.

F. Evaluation Metrics: Accuracy, False Positive Rate (FPR), precision, recall, and F1-score are calculated to measure the performance of the systems on the datasets.

G. Proposed Architecture: The proposed system will have the following four major layers:

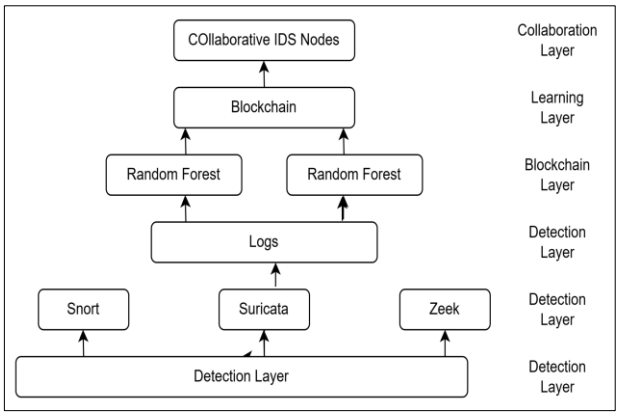
H. Detection Layer: IDS nodes monitor network traffic, and tools such as Snort, Suricata, and Zeek are used. Real-time local logs and alerts are created.

I. Learning Layer: ML algorithms analyse logs to identify normal and malicious events. It is compared to Random Forest, SVM and KNN.

J. Blockchain Layer: The Ethereum blockchain guarantees immutability and distributed consensus. Lists of alerts and logs are digitized. Smart contracts authenticate the information and then store it.

K. Collaboration Layer: Communication between nodes occurs via smart contracts. The mutual

intelligence enhances international detection. The reputation management is done off-chain. This hierarchical design has enabled strong threat detection, decentralised data exchange, and trustless cooperation among IDS nodes. The modular architecture is scalable, resistant to insider threats, and adaptable to any network environment.



[Fig.1: Proposed System]

The proposed intelligent CIDS system integrates Random Forest, SVM, and KNN algorithms with an Ethereum-based blockchain to enhance network security. Fig. 1 Random Forest can make well-founded decisions and is therefore able to detect them with high accuracy under diverse attacks. KNN is a good choice for modest-sized datasets, whereas SVM generalises well to linearly separable data. Alerts and logs shared on the blockchain are secured by immutability and decentralisation. The study integrates collaborative detection into its framework, using a blockchain trust model to reduce false positives and improve resilience to tampering and internal attacks.

In this article, we present a novel system, an intelligent CIDS, that integrates Random Forest, SVM, and KNN algorithms on an Ethereum-based blockchain to improve network security. Thanks to the ensemble-based strategy that aids pattern detection, Random Forest has proved capable of delivering stable classification accuracy across various attack forms. Given the nature of SVMs' linearity and robustness in generalising to linearly separable data, the scope of both algorithms can be very wide. KNN, on its own, is an effective algorithm to implement for those unique and simple datasets where you are working with small problems, particularly if your inputs have huge

variations. Absence of fuzzy alerts/loss of information: SCFC's inherently decentralised operation makes it a prime candidate for sharing alerts and logs across multiple server clusters, with a design that ensures both immutability and decentralised control. Through the use of collaborative detection and a A decentralized trust model based on blockchain, the system limits false positives while increasing resistance to tampering and insider threats.

4.1 Algorithm:

1. Framework of collaborative IDS.

Step 1: Implementation of IDS nodes in the network.

Step 2: Traffic is monitored, and anomalies are identified in each node.

Step 3: Hashes of the detected intrusions are sent to the blockchain.

Step 4: Maintenance involves validating and recording alerts using smart contracts.

Step 5: Nodes can use stored alerts to enhance local detection models.

2. Random Forest Algorithm

Step 1: Choose several random subsets of the dataset.

Step 2: Independent training of decision trees.

Step 3: Allow new information to be classified by each tree.

Step 4: A majority vote makes the final decision.

3. Support Vector Machine (SVM)

Step 1: Project information onto high-dimensional space.

Step 2: Establish the best separating plane.

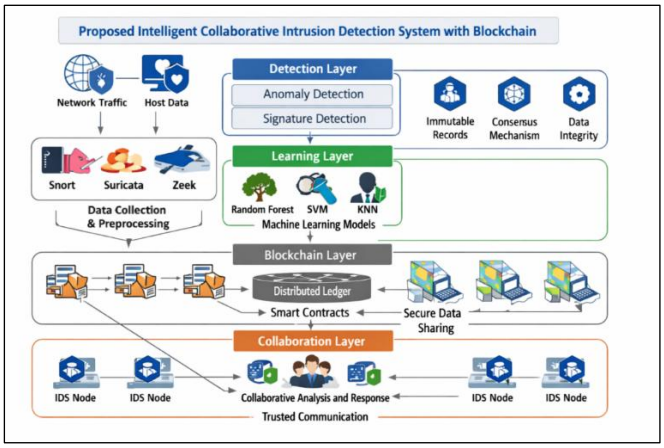
Step 3: Classify the new data according to the margin boundary.

4. K-Nearest Neighbours (KNN)

Step 1: Choose the value of K.

Step 2: Distance between test instances and training points.

Step 3: Take the K nearest points and vote on them by majority vote.



[Fig.2: Proposed Intelligent Intrusion Detection System Diagram]

The proposed system (Fig. 2) employs a layered architecture that integrates Intrusion Detection Systems (IDS), machine learning methods, and blockchain technology to enhance network security and collaborative threat detection. This architecture has four main layers: the Detection Layer, the Learning Layer, the Blockchain Layer, and the Collaboration Layer.

The detection layer gathers network traffic and host data using intrusion detection system (IDS) tools, including Snort, Suricata, and Zeek. This layer employs both anomaly-detection and signature-based detection methods to pinpoint potentially malicious behaviour. Subsequently, the acquired data is preprocessed before being transmitted to the learning layer.

Using machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbours (KNN), the learning layer classifies network traffic into malicious and benign categories. These models improve detection accuracy and reduce false positives. The blockchain layer ensures the secure, decentralised sharing of intrusion alerts via distributed ledgers and smart contracts. This layer maintains data integrity, immutability, and dependable communication between IDS nodes. Finally, the Collaboration Layer enables multiple IDS nodes to share alerts and perform joint analysis and response. This enhances

detection performance and fortifies system resilience against dispersed cyber threats. All things considered, the proposed architecture provides a cooperative intrusion detection system that is suitable for modern distributed network environments and is safe, scalable, and intelligent.

V. MATHEMATICAL MODEL

Let the set of network observations be defined as:

- $D = \{d_1, d_2, ..., d_n\}$, where each d_i is a network record with selected features.
- Let $f: D \rightarrow \{0, 1\}$ be the binary classification function where 0 = Normal, 1 = Intrusion.

For Random Forest (RF):

- Each decision tree T_k votes on the classification of d_i.
- The final output: $f(d_i) = \text{mode}(T_1(d_i), T_2(d_i), ..., T_k(d_i))$.

FOR Support VECTOR MACHINE (SVM):

- A hyperplane is defined as $w^T x + b = 0$.
- Classification rule: $f(d_i) = 1$ if $w^T x_i + b \geq 0$, otherwise $f(d_i) = 0$.

For K-Nearest Neighbours (KNN):

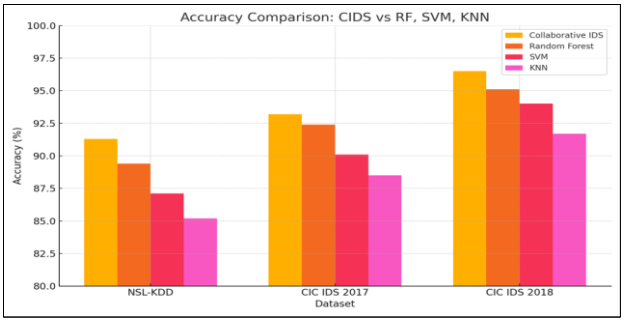
- Let $N_k(d_i)$ be the k-nearest neighbours of d_i.
- $f(d_i) = \text{mode}(\{f(d_j) \mid d_j \in N_k(d_i)\})$.

For Blockchain Integration:

- Each intrusion alert A_i is hashed as $H(A_i) = SHA256(A_i)$.
- The blockchain ledger B stores tuples: $B = \{(A_i, H(A_i), t_i)\}$, where t_i is the timestamp.
- Smart contracts enforce a trust threshold τ, such that only if $T\_node(A_i) \geq \tau$, then A_i is accepted and broadcast to peers.

This mathematical model describes the classification process used in the IDS framework. It helps define how network activities are analysed and categorised, while also supporting data integrity and trust through BLOCKCHAIN technology.

VI. RESULTS AND DISCUSSION



[Fig.3: Comparative Results]

The effectiveness of the proposed Collaborative Intrusion Detection System (CIDS) was evaluated using three well-known datasets: NSL-KDD, CIC IDS 2017, and CIC IDS 2018. (Fig. 3) The performance of the collaborative IDS model was assessed based on accuracy and then compared with commonly used machine learning classifiers such as Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbours (KNN) [13]. The comparative accuracy results obtained from these experiments are summarized in Table I.

Table I: Summarize Data Collection

Dataset	Collaborative IDS	Random Forest	SVM	KNN
NSL-KDD	91.3%	89.4%	87.1%	85.2%
CIC IDS 2017	93.2%	92.4%	90.1%	88.5%
CIC IDS 2018	96.5%	95.1%	94.0%	91.7%

A comparative graph (Fig. 2) presents the accuracy results in a visual form, clearly illustrating the performance improvement of the proposed collaborative IDS approach [14]. The results indicate that collaboration among multiple IDS nodes, enabled by blockchain technology, enhances the system's overall detection capability. This approach improves detection accuracy and helps reduce false alarms.

VII. CONCLUSION

To address several issues with traditional IDS frameworks, this study introduces an intelligent Collaborative Intrusion Detection System that combines blockchain technology with machine learning techniques [15]. Through Ethereum-based smart contracts, the system enables distributed network nodes to securely and unalterably share intrusion-related data. The system can successfully identify both known and unknown cyberthreats by applying machine learning algorithms such as random forest, support vector machine, and k-nearest neighbours. The suggested method outperforms conventional intrusion detection techniques in both accuracy and scalability, according to experimental evaluation on standard benchmark datasets. All things considered, the suggested architecture offers a clever, decentralised solution ideal for contemporary, dynamic network environments. Future research will concentrate on expanding the system's deployment across various computing platforms, enhancing energy efficiency, and implementing the system in real-time scenarios.

DECLARATION STATEMENT

As the article's author, I must verify the accuracy of the following information after aggregating input from all authors.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and without external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Hasan, M. K., Alkhalifah, A., Islam, S., Babiker, N. B. M., Habib, A. K. M. A., Aman, A. H. M., & Hossain, M. A. (2022). Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. Wireless

Communications and Mobile Computing, 2022(1). DOI: https://doi.org/10.1155/2022/9065768
2. Khonde, S. R., & Ulagamuthalvi, V. (2022). A hybrid intrusion detection system using a blockchain framework. EURASIP Journal on Wireless Communications and Networking, 2022(1). DOI: https://doi.org/10.1186/s13638-022-02089-4
3. W. Meng, "When intrusion detection meets Blockchain Technology: A review," IEEE Access, vol. 6, pp. 10179–10188, 2018. https://ieeexplore.ieee.org/stamp/redirect.jsp?arnumber=/6287639/8274985/08274922.pdf
4. Al-E'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S., & Hasbullah, I. (2021). Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges. Computer Systems Science and Engineering, 40(1), 87–112. DOI: https://doi.org/10.32604/csse.2022.017941
5. Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain Research and Applications, 3(2), 100067. DOI: https://doi.org/10.1016/j.bcra.2022.100067
6. Xing, R., Su, Z., & Wang, Y. (2024). Collaborative Intrusion Detection Approach based on blockchain in Internet of Vehicles. IEEE Internet of Things Journal, 12(9), 11965–11976. DOI: https://doi.org/10.1109/jiot.2024.3520615
7. Govindaram, A., & A J. (2024). FLBC-IDS: a federated learning and blockchain-based intrusion detection system for secure IoT environments. Multimedia Tools and Applications, 84(17), 17229–17251. DOI: https://doi.org/10.1007/s11042-024-19777-6
8. Li, W., Stidsen, C., & Adam, T. (2023). A blockchain-assisted security management framework for collaborative intrusion detection in smart cities. Computers & Electrical Engineering, 111, 108884. DOI: https://doi.org/10.1016/j.compeleceng.2023.108884
9. Gupta, R. K., Chawla, V., Pateriya, R. K., Shukla, P. K., Mahfoudh, S., & Shah, S. B. H. (2023). Improving a collaborative intrusion detection system using blockchain and pluggable authentication modules for a sustainable smart City. Sustainability, 15(3), 2133. DOI: https://doi.org/10.3390/su15032133
10. Liang, W., Xiao, L., Zhang, K., Tang, M., He, D., & Li, K. (2021). Data Fusion Approach for Collaborative Anomaly Intrusion Detection in Blockchain-Based Systems. IEEE Internet of Things Journal, 9(16), 14741–14751. DOI: https://doi.org/10.1109/jiot.2021.3053842
11. Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. R. (2020). A deep Blockchain Framework-Enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal, 8(12), 9463–9472. DOI: https://doi.org/10.1109/jiot.2020.2996590
12. Kolokotronis, N., Brotsis, S., Germanos, G., Vassilakis, C., & Shiaeles, S. (2019). On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection, 21–28. DOI: https://doi.org/10.1109/services.2019.00019
13. Hu, B., Zhou, C., Tian, Y., Qin, Y., & Junping, X. (2019). A collaborative intrusion detection approach using blockchain for multimicrogrid systems. IEEE Transactions on Systems Man and Cybernetics Systems, 49(8), 1720–1730. DOI: https://doi.org/10.1109/tsmc.2019.2911548
14. Alexopoulos, N. (n.d.). Towards Blockchain-Based Collaborative Intrusion Detection Systems. Lecture Notes in Computer Science, vol. 10707, Springer, 2018. https://download.hrz.tu-darmstadt.de/pub/FB20/Dekanat/Publikationen/TK/critis17CIDS_camera.pdf
15. Khan, A. A., Khan, M. M., Khan, K. M., Arshad, J., & Ahmad, F. (2021). A blockchain-based decentralised machine learning framework for collaborative intrusion detection within UAVs. Computer Networks, 196, 108217. DOI: https://doi.org/10.1016/j.comnet.2021.108217
16. Abdel-Basset, M., Moustafa, N., Hawash, H., Razzak, I., Sallam, K. M., & Elkomy, O. M. (2021). Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 23(3), 2523–2537. DOI: https://doi.org/10.1109/tits.2021.3119968

AUTHOR'S PROFILE

Dr. Pramod A. Jadhav is an Associate Professor in the Department of Computer Science and Business Systems at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune. He has extensive experience in teaching, research, and academic administration, with expertise in software engineering, IoT, and emerging technologies. Dr. Jadhav has contributed to various research publications in reputed journals and conferences. He is actively involved in curriculum development, student mentoring, and outcome-based education practices. His research interests include machine learning, embedded systems, and data analytics, with a focus on solving real-world engineering problems through innovative and interdisciplinary approaches.

Nitin Sale is a Ph.D. Scholar in the Department of Computer Engineering at Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune, India. He received his M.E. in Computer Engineering from Savitribai Phule Pune University. He has over 12 years of experience as a System Analyst at AISSMS College of Engineering, Pune. His research interests include Intrusion Detection Systems (IDS), Blockchain-based IDS, Machine Learning, Disagreement-based Semi-Supervised Learning, Cybersecurity frameworks, and Network Security. He has published papers in international conferences and journals such as ICCUBEA, IJIRCCE, and ICCIS, and has participated in AICTE-sponsored Faculty Development Programs.

Dr. Vinod H. Patil is a working professional and researcher in the field of Electronics and Telecommunication Engineering, He received a PhD in Electronics Engineering with the topic "Spectrum Management in Cognitive Radios" in the year 2020. He is a reviewer for various reputable international journals and Conferences. Currently working as an Assistant Professor and Research Guide in Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (India). His primary research areas are Cognitive Radio, Wireless Sensor Networks, Smart Agricultural Systems, Smart Grid Systems, Machine Learning, and Artificial Intelligence.

A. Y. Prabhakar, (Deemed to be University) College of Engineering, Pune, widely focused on teaching, learning undergraduate students, studying, developing and evaluating novel approaches to manage the flow of data within resource-constrained WSNs to prevent energy loss, delay in packet arrival and performance degradation caused by traffic bottlenecks. Aimed to enhance network efficiency, reliability, and lifespan by addressing the unique challenges posed by the distributed, often dynamic, and energy-limited nature of WSNs.

Dr. Chetan Sambhajirao More received his PhD in Electronics Engineering from Bharati Vidyapeeth (Deemed to be University) in February 2025. He is an Assistant Professor with the Department of Electronics & Telecommunication Engineering at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune - 411043, Maharashtra, India. He has been in the teaching profession for more than 10 years. He has presented his research papers in several National and international journals and conferences. His current research interests include the design and implementation of programming languages, Wireless communications techniques, Antenna Design, Image processing, intelligent transportation, cybersecurity, Machine Learning, and Artificial Intelligence.