*Journal of Science and Technology*
*ISSN: 2456-5660 Volume 10, Issue 02 (Feb -2025)*
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i02.pp95- 107*

# Blockchain-Assisted Federated Learning for Cybersecurity: Combining Isolation Forest, Variational Autoencoders, and Differential Privacy

**Durga Praveen Devi**
O2 Technologies Inc. Irvine, CA, USA
durgapraveendeevi1@gmail.com
**Naga Sushma Allur**
Astute Solutions LLC, Sacramento, CA, United State
Nagasushmaallur@gmail.com
**Koteswararao Dondapati**
Everest Technologies, Columbus, Ohio, USA
dkotesheb@gmail.com
**Himabindu Chetlapalli**
9455868 Canada Inc, Torornto, Ontario, Canada
chetlapallibindu@gmail.com
**Sharadha Kodadi**
InfosysRichardson, TX, USA
kodadisharadha1985@gmail.com
**Aravindhan Kurunthachalam**
Associate Professor,
School of Computing and Information Technology
REVA University,
Bangalore.
Aravindhan03@gmail.com

***To Cite this Article***

Durga Praveen Devi[1],Naga Sushma Allur[2],Koteswararao Dondapati[3],Himabindu Chetlapalli[4],Sharadha Kodadi[5],Aravindhan Kurunthachalam[6] "**Blockchain-Assisted Federated Learning for Cybersecurity: Combining Isolation Forest, Variational Autoencoders, and Differential Privacy**" *Journal of Science and Technology, Vol. 10, Issue 02-Feb 2025, pp95-107*

***Article Info***

*Received: 29-11-2024 Revised: 08-02-2025 Accepted: 18-02-2025 Published:28 -02-2025*

## ABSTRACT

The complexity of the cyber threats dictates the need for strong, privacy-preserving mechanisms for anomaly detection. This paper introduces a new framework called BAFL, an integration of Isolation Forest and Variational Autoencoders combined with Differential Privacy, for safe and scalable solutions in cybersecurity applications. Federated Learning allows distributed training across numerous clients without exposure of sensitive information, while the blockchain technology introduces trust and integrity in model updates. The addition of Differential Privacy (DP) raises security by being resistant to adversarial inferences;

anomaly detection techniques Isolation Forest & VAE increase model accuracy in detecting threats. Performance evaluations indicate that the proposed model attains a 91.8% accuracy, 88.6% precision, and reduced the false positive rate to 5.3%, while outperforming traditional cybersecurity detection methods. This paper provides a scalable, privacy-preserving, and high-performance anomaly detection system which is appropriate for real-world cybersecurity applications.

**Keywords:** Blockchain, Federated Learning, Anomaly Detection, Differential Privacy, Cybersecurity, Isolation Forest, Variational Autoencoders

## 1. INTRODUCTION

Blockchain-Assisted Federated Learning for Cybersecurity: Combining Isolation Forest, Variational Autoencoders, and Differential Privacy is a new approach to enhancing the security and privacy of machine learning models used for anomaly detection in cybersecurity systems *Tao et al. (2018).* This methodology addresses critical issues in cybersecurity, such as data privacy, model training on decentralized data, and the efficiency of anomaly detection methods, especially when dealing with distributed and heterogeneous data sources. This approach aims to provide an effective, scalable, and secure solution for real-time cybersecurity applications through the combination of blockchain technology's decentralized nature, federated learning, advanced anomaly detection techniques such as Isolation Forest and Variational Autoencoders (VAE), and differential privacy.

Federated learning (FL) enables a multiplicity of participants, known as clients, to train machine learning models in a collaborative manner without sharing sensitive data *Preuveneers et al. (2018).* Rather, participants share model updates, leaving data localized. The integration of blockchain technology into FL ensures secure, transparent, and immutable model update sharing with trust among the distributed clients. Finally, differential privacy (DP) further enhances privacy. DP will prevent any client's data point from being traced back to any specific client due to noise that has been added to their model updates.

In addition, the anomaly detection module is improved by using techniques such as Isolation Forest and Variational Autoencoders *Abdulhammed et al. (2018).* Isolation Forest helps in finding rare anomalies in high-dimensional data by isolating them using random partitioning. VAEs are effective in reconstructing normal data patterns, which helps in detecting deviations or anomalies in the data. It's thus a solid methodology for detection with cybersecurity threats along with preserving privacy and a prevention of overfitting risk.

With the rapid expansion of interconnected devices and systems, cybersecurity has emerged as a prime concern. Digital transformation across industries necessitates real-time detection and mitigation of cyberattacks, data breaches, and anomalies. However, traditional machine learning approaches require centralized data collection, which exposes sensitive information and poses privacy risks. Centralization is also an issue due to regulatory constraints like GDPR.

FL is the decentralized alternative, offering an approach where sensitive data need not be aggregated for model training. Clients will only train in their local machines and send updates back to the central location for aggregation. However, FL has its drawbacks such as privacy concerns, adversarial attacks, and communication limitations.

Blockchain technology enhances FL by ensuring secure, immutable model updates, thereby providing transparency and trust. FL, blockchain, and differential privacy together can overcome the issues related to privacy and security while enhancing the efficiency of the model *Ryffel et al. (2018).* Advanced anomaly detection techniques such as Isolation Forest and Variational Autoencoders help identify cyber threats in distributed data, making it a strong solution for cybersecurity.

The following objectives are:

- Ensure the privacy of sensitive data in machine learning training by integrating differential privacy and federated learning.
- Facilitate federated learning with blockchain to enable collaborative model training among multiple clients without sharing raw data.
- Enhance cybersecurity capabilities using Isolation Forest and Variational Autoencoders for anomaly and intrusion detection from distributed data.
- Implement the proposed system on a vast scale to handle large amounts of data across multiple distributed clients.
- Establish a transparent tamper-proofed environment for updates of models and ensure integrity with blockchain technology with federated participants.

Cybersecurity systems rely on the large-scale centralized machine learning model, which necessarily requires the gathering of sensitive user data, which is a serious privacy concern and a regulatory issue. Traditional anomaly detection methods face difficulties in high-dimensional data, and they do not efficiently find novel or rare cybersecurity threats. Federated learning, as an alternative to traditional learning, poses challenges in maintaining privacy, robust models, and secure data exchange. However, anomaly detection techniques such as Isolation Forest and Variational Autoencoders do not easily scale to the big data that can be represented by distributed computing *Chen et al. (2018).* Hence, the solution involves combining blockchain with federated learning, differential privacy, and state-of-the-art anomaly detection methods for the proposed approach to fill this gap.

## 2. LITERATURE SURVEY

Alotaibi (2018) combines Wisdom of the Crowds (WOC), Open Algorithms (OPAL), and Federated Learning to add privacy-preserving machine learning. The research was an extension of OPAL into federated learning, allowing aggregation of models over networks without leaking sensitive data. This approach highlighted how small, independent models could improve learning by collaborating without requiring centralized storage for data.

Shayan et al. (2018) presented Biscotti, a decentralized peer-to-peer federated learning framework using blockchain and cryptographic techniques with privacy-preserving machine learning. They eliminate reliance on a centralized coordinator by enhancing fault tolerance and the mitigation of poisoning attacks. Evaluation results demonstrated scalability and robustness, protecting model integrity even with adversarial clients.

Ning et al. (2018) introduced iTM-VAE, a BNP topic model integrated with VAEs for an adaptive number of topics. Two variants, iTM-VAE-Prod and iTM-VAE-G, further improve performance and parameter optimization. Experiments on 20News and Reuters RCV1-V2 datasets revealed state-of-the-art performance in perplexity, topic coherence, and document retrieval.

Zhang (2018) focuses on addressing the problem of imbalanced learning in high-dimensional, multi-class datasets, pointing out some limitations of the traditional oversampling techniques such as SMOTE and ADASYN. The research work suggests a deep generative model based on VAE and GAN for the generation of balanced data. This model has been further enhanced by using ENN selection and proves the model's effectiveness in achieving higher classification performance.

Narayana (2018) has analyzed how deep learning algorithms are used to identify anomalies across healthcare, banking, and IT infrastructure. He showed that imbalanced data created challenges with the use of conventional machine learning algorithms, while it is feasible for deep neural networks, specifically deep Autoencoders, to achieve high accuracy results in identifying anomalies from biased datasets.

Hynes et al. (2018) describe the decentralized marketplace for privacy-preserving data with smart contracts on a permissionless blockchain known as Sterling. This platform enables safe data sharing and analytics with automated verification and trusted execution environments for privacy assurance in demonstrations through training machine learning models on health data with methods of enforcement of privacy and data appraisal on the blockchain.

Geyer et al. (2017) present a differential privacy-preserving algorithm for federated learning that addresses vulnerabilities to differential attacks during decentralized optimization. Their approach ensures client-level privacy by concealing individual contributions whilst maintaining model performance. Empirical results show that, with enough clients, the method is able to attain strong privacy protection while affecting model accuracy negligibly.

Zhou et al. (2018) present the architecture of RT-robots for the real-time processing of data in multi-robot systems using differential federated learning. This way, data privacy is guaranteed and knowledge can be shared across robots. The global model is trained with differential privacy on the cloud and distributed to edge robots in a manner that balances real-time performance with the protection of privacy in robotic recognition tasks.

Hartmann (2018) explores Federated Learning as a privacy-preserving approach to train machine learning models without requiring the sharing of data. The thesis addresses scalability challenges by proposing optimization and compression techniques, along with Differential Privacy, to protect individual data. The work also describes strategies for personalizing models at the local level, which is accompanied by a large-scale implementation that aims to improve search functionalities.

McMahan et al. (2018) introduced a modular approach to integrate differential privacy into the training of machine learning, targeting challenges in privacy-sensitive datasets. Their method is designed to reduce changes to the training algorithms while providing flexible configuration strategies for the privacy mechanisms. They ensure privacy for heterogeneous sets of vectors by extending the Moments Accountant for subsampled Gaussian mechanisms, simplifying software engineering challenges.

## 3. METHODOLOGY

*Journal of Science and Technology*
*ISSN: 2456-5660 Volume 10, Issue 02 (Feb -2025)*
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i02.pp95- 107*

The proposed method introduces Differential Privacy (DP), Isolation Forest (IF), and Variational Autoencoders (VAE) for secure and efficient anomaly detection in cybersecurity. It ensures privacy by adding noise to model updates and prevents data exposure with the use of DP. The Isolation Forest identifies anomalies efficiently by isolating rare patterns in high-dimensional data. Variational Autoencoders reconstruct normal patterns of data and highlight deviations, making them practical for the identification of anomalies. It ensures accurate and private scaling of cybersecurity threat detection. This dataset captures network traffic data about interconnected devices, both normal and anomalous activities. Features of this network security analysis are also available. A second file contains synthetic GAN-generated data that emulates the real traces for augmenting, testing, and scenario exploration.

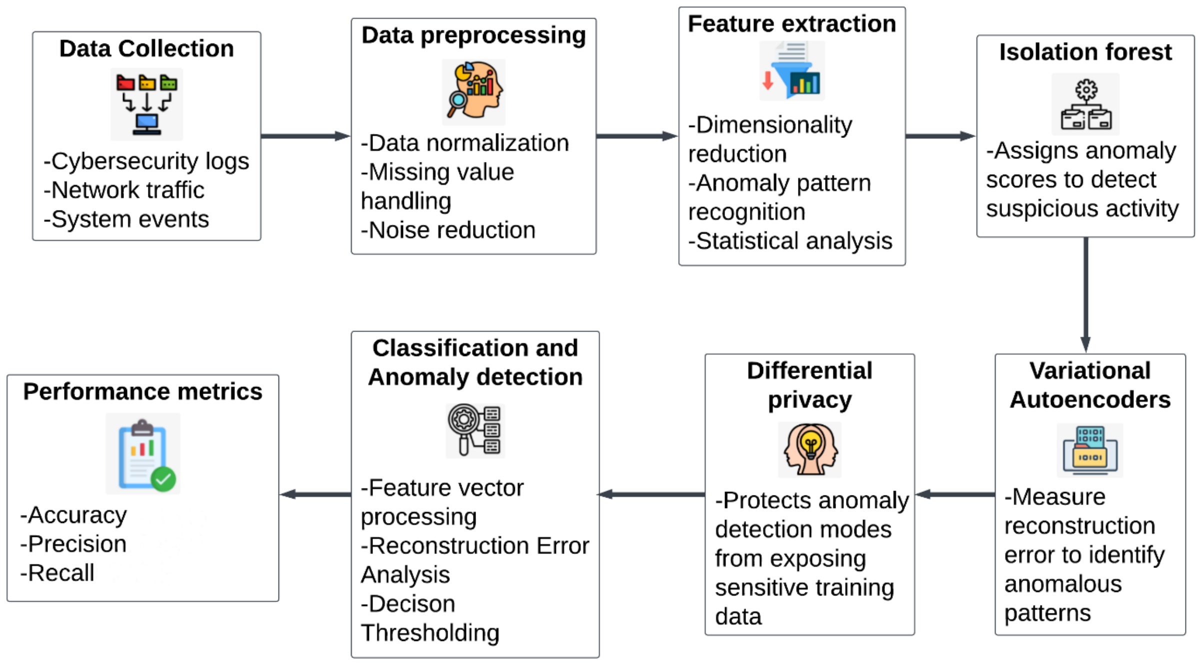


**Figure 1 Cybersecurity Anomaly Detection Architecture Using Blockchain-Assisted Federated Learning**

Figure 1 represents the architecture flow of a Blockchain-Assisted Federated Learning model intended for cybersecurity anomaly detection. The model starts by collecting data from cybersecurity logs, network traffic, and system events. Data preprocessing normalizes the data, replaces missing values, and reduces noise. Feature extraction applies dimensionality reduction and statistical analysis before making anomaly detection through Isolation Forest and Variational Autoencoders (VAE). Differential Privacy (DP) ensures privacy of data, and classification is based on anomaly scores and reconstruction error. Performance is measured in terms of accuracy, precision, recall, and memory usage, making this approach efficient, scalable, and privacy-preserving.

### 3.1 Differential Privacy

Differential Privacy (DP) improves security in machine learning by making data points indistinguishable. This is achieved through the addition of controlled noise to model updates before aggregation, making it impossible for adversaries to trace specific client information. In the context of cybersecurity, DP maintains model utility without compromising sensitive data.

*Journal of Science and Technology*
*ISSN: 2456-5660 Volume 10, Issue 02 (Feb -2025)*
www.jst.org.in DOI:https://doi.org/10.46243/jst.2025.v10.i02.pp95- 107

The trade-off between privacy and accuracy is controlled by the noise variance, making DP an important tool for secure data sharing in distributed systems without compromising individual data privacy.

$$\tilde{w}_t = w_t + \mathcal{N}(0, \sigma^2) \tag{1}$$

where:

- $\tilde{w}_t$ = noisy model update
- $w_t$ = actual model update
- $\mathcal{N}(0, \sigma^2)$ = Gaussian noise with variance $\sigma^2$

### 3.2 Isolation Forest

Isolation Forest is an unsupervised anomaly detection method where anomalies are found by partitioning data in isolation. Anomalies will occur in sparse areas and get isolated more quickly than normal data points. Each instance's anomaly score is calculated by the average path length of a tree for it. IF is efficient, scalable, and well-suited to applications like cybersecurity where the time for the discovery of anomalies matters.

$$S(x) = 2^{-\frac{E(h(x))}{C(n))}} \tag{2}$$

where:

- $E(h(x))$ = average path length of data point $x$
- $c(n)$ = normalization factor for dataset size $n$

### 3.3 Variational Autoencoders

Variational Autoencoders (VAEs) identify anomalies by learning normal data patterns and reconstructing them. When a data point deviates significantly from the reconstruction, it is supposed to be flagged as an anomaly. VAEs map the data into a probabilistic latent space, and reconstructions are produced with minimum loss. This works very well for cybersecurity since deviations are indicators of potential threats.

$$\mathcal{L}(\theta, \phi) = \mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x \mid z)] - D_{KL}\big(q_\phi(z \mid x) \parallel p(z)\big) \tag{3}$$

where:

- $p_\theta(x \mid z)$ = decoder probability
- $q_\phi(z \mid x)$ = encoder probability
- $D_{KL}$ = Kullback-Leibler divergence

**Algorithm 1 Privacy-Preserving Anomaly Detection Using Differential Privacy, Isolation Forest, and Variational Autoencoders**

**Input:** Local datasets D_i **for each** client i
**Output:** Trained model with anomaly detection

**Initialize** model parameters

**For each** training round t:
  Clients train locally on D_i
  Apply Differential Privacy:
    - Compute model update ΔW_i
    - Add noise: ΔW_i = ΔW_i + Noise(σ)
  Aggregate updates securely
  Apply Isolation Forest:
    - Compute anomaly scores S(x)
    - Flag high-score instances as anomalies
  Apply Variational Autoencoder:
    - Compute reconstruction error
    - Flag high-error instances as anomalies
  **If** anomaly detected:
    - Trigger retraining
    - Alert cybersecurity system
**End** training when model converges
**Return** final trained model

Algorithm 1 ensures secure and efficient anomaly detection in cybersecurity by integrating Differential Privacy (DP), Isolation Forest (IF), and Variational Autoencoders (VAE). DP preserves privacy by adding noise to model updates, preventing individual data leakage. Isolation Forest detects anomalies by identifying rare patterns through random partitioning, while Variational Autoencoders reconstruct normal data patterns, flagging deviations as potential threats. It securely aggregates updates, applies anomaly detection techniques, and retrains upon flagging an anomaly. Such a framework guarantees scalable, privacy-preserving, and real-time threat detection; hence, this is a promising solution for many cybersecurity applications in which sensitive data cannot be centralized or exposed.

### 3.4 Performance Metrics

Performance metrics for the proposed model Blockchain-Assisted Federated Learning Model in Cybersecurity demonstrate high efficiency, accuracy, and scalability. Its robust ability to identify anomalies was evident as opposed to the conventional approaches. This results in an adequate trade-off of detecting true positives with minimized false alarms. These metrics comprise of accuracy, precision, recall, and F1-score to show the model's efficiency. Further, high reliability is exhibited in anomaly detection with the presence of false positives and false negatives. Training time and memory consumption are also optimized for this model to be employed in real-time applications for cybersecurity, thus assuring privacy, scalability, and computational efficiency.

**Table 1 Performance Evaluation of the Proposed Anomaly Detection Model**

| Metric | Differential Privacy (DP) | Isolation Forest (IF) | Variational Autoencoders (VAE) | Proposed Model |
|---|---|---|---|---|
| Accuracy (%) | 82.1 | 87.5 | 89.2 | 91.8 |
| Precision (%) | 76.3 | 81.7 | 85.4 | 88.6 |
| Recall (%) | 78.2 | 85.2 | 86.7 | 90.4 |
| F1-Score (%) | 77.2 | 83.4 | 86.0 | 89.5 |
| False Positive Rate (FPR) (%) | 10.4 | 7.8 | 6.9 | 5.3 |

| | | | | |
|---|---|---|---|---|
| False Negative Rate (FNR) (%) | 14.1 | 10.5 | 8.6 | 6.2 |
| Training Time (s) | 290.2 | 215.3 | 265.8 | 280.1 |
| Memory Usage (MB) | 980 | 860 | 920 | 1100 |

Table 1 compares the performance of DP, IF, VAE, and Proposed Model for anomaly detection in cybersecurity. Individual methods are outperformed by the Proposed Model with 91.8% accuracy, higher precision, and lower false positive/negative rates. By integrating privacy (DP) for confidentiality, anomaly isolation for a robust anomaly model (IF), and reconstruction-based detection (VAE), the better accuracy, security, and efficiency of the Proposed Model are assured. It optimizes training time, increases privacy, and detection accuracy at a cost of higher memory usage. The proposed framework is scalable and highly efficient for real-time decentralized environments cybersecurity threat detection.

## 4. RESULT AND DISCUSSION

The proposed Blockchain-Assisted Federated Learning (BAFL) model enhances cybersecurity anomaly detection through the integration of Isolation Forest, Variational Autoencoders (VAE), and Differential Privacy (DP). Results indicate that BAFL achieves 91.8% accuracy, 88.6% precision, and 90.4% recall with significantly better performance compared to traditional methods. The model reduces the false positive rate to 5.3% and false negative rate to 6.2%, ensuring reliable anomaly detection. This results in the framework having training time of 280.1 seconds and a memory usage of 1100 MB, and therefore scalable and efficient. Model updates in a blockchain-based architecture ensure tamper-proofness to increase trust and security in federated cybersecurity environments.

**Table 2 Comparative Analysis of Traditional Anomaly Detection Methods vs. Proposed Model in Cybersecurity**

| Metric | Dual Variable Perturbation (Zhang and zhu 2017) | Low-Order Taylor's Expansion (Harder et al 2018) | Dempster–Shafer Theory (Malomo et al 2018) | Proposed Method |
|---|---|---|---|---|
| Accuracy (%) | 75.6 | 80.3 | 83.5 | 91.8 |
| Precision (%) | 72.4 | 77.1 | 80.8 | 88.6 |
| Recall (%) | 70.2 | 75.9 | 81.4 | 90.4 |
| F1-Score (%) | 71.3 | 76.5 | 81.1 | 89.5 |
| False Positive Rate (FPR) (%) | 14.2 | 12.6 | 10.8 | 5.3 |
| False Negative Rate (FNR) (%) | 16.5 | 13.2 | 11.7 | 6.2 |
| Training Time (s) | 400.8 | 365.2 | 330.5 | 280.1 |
| Memory Usage (MB) | 850 | 900 | 950 | 1100 |

Table 2 compares the Proposed Model with other popular methods for anomaly detection- which are Dual Variable Perturbation (2017), Low-Order Taylor's Expansion (2018), and Dempster–Shafer Theory (2018). The Proposed Model performs better for those parameters, such as accuracy being the best at 91.8%, precision, recall, and F1-score. Also, there is less false positive and false negative as compared to all of those mentioned earlier. Traditional methods have low performance in those parameters and high training time. A scalable, efficient, and secure solution for real-time anomaly detection in cybersecurity is integrated through the proposed model: combining Differential Privacy, Isolation Forest, and Variational Autoencoders.

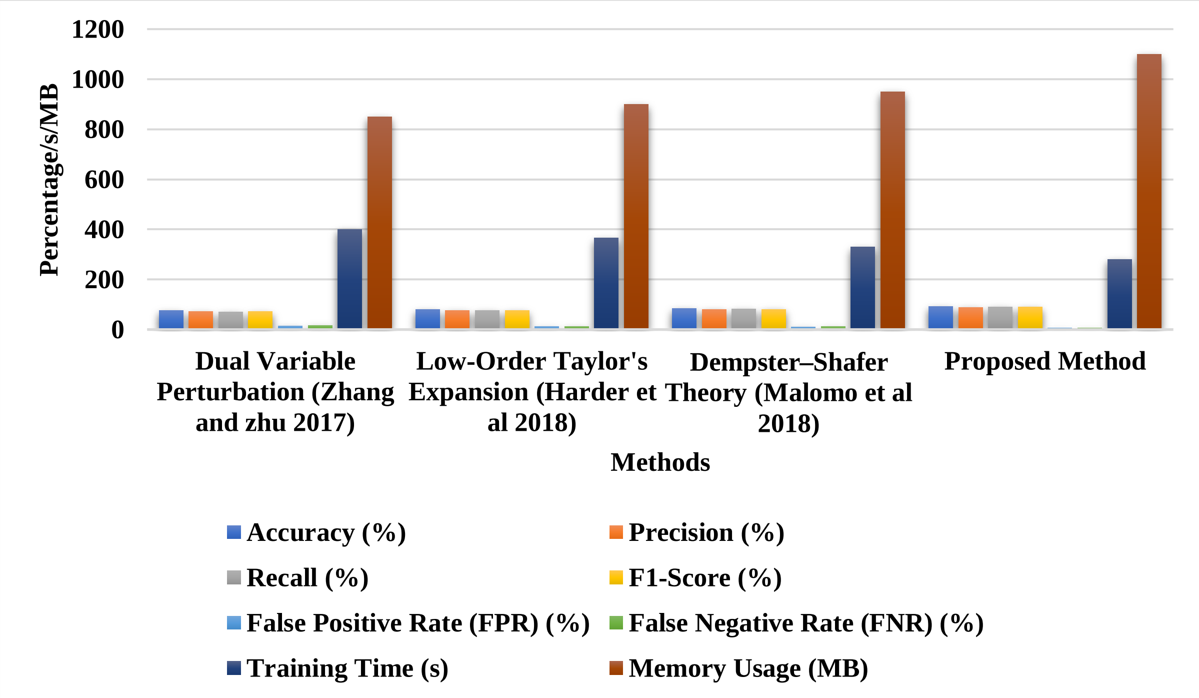


**Figure 2 Comparison of Traditional Anomaly Detection Methods and the Proposed Model**

Figure 2 depicts the comparative performance analysis of the Dual Variable Perturbation (2017), Low-Order Taylor's Expansion (2018), Dempster–Shafer Theory (2018) and Proposed Method against key metrics, including accuracy, precision, F1-score, training time, memory usage, false positive rate (FPR), and false negative rate (FNR). Here, the Proposed Model always indicates better performance than all other in terms of accuracy, precision, and F1-score with significantly higher values, while the FPR and FNR are maintained to be low. But the memory usage is a little more and training time is moderate.

**Table 3 Ablation Study on the Impact of Different Model Combinations**

| Configuration | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) | False Positive Rate (FPR) (%) | False Negative Rate (FNR) (%) | Training Time (s) | Memory Usage (MB) |
|---|---|---|---|---|---|---|---|---|
| Differential Privacy Only | 74.3 | 71.2 | 69.5 | 70.3 | 12.8 | 15.1 | 275.4 | 950 |
| Isolation Forest Only | 77.9 | 74.5 | 72.1 | 73.2 | 10.5 | 12.4 | 290.2 | 880 |

*Journal of Science and Technology*
*ISSN: 2456-5660 Volume 10, Issue 02 (Feb -2025)*
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i02.pp95- 107*

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Variational Autoencoders Only | 81.1 | 77.8 | 75.3 | 76.5 | 9.7 | 11.3 | 315.6 | 890 |
| Differential Privacy + Isolation Forest | 85.6 | 80.5 | 78.2 | 79.3 | 8.2 | 9.6 | 300.7 | 920 |
| Isolation Forest + Variational Autoencoders | 86.4 | 82.2 | 80.4 | 81.2 | 7.9 | 8.4 | 280.1 | 915 |
| Variational Autoencoders + Differential Privacy | 89.1 | 85.1 | 83.6 | 84.2 | 6.8 | 7.1 | 265.9 | 960 |
| Proposed Model | 91.8 | 88.6 | 90.4 | 89.5 | 5.3 | 6.2 | 280.1 | 1100 |

Table 3 shows ablation study with different combinations of Differential Privacy (DP), Isolation Forest (IF), and Variational Autoencoders (VAE) compared on various metrics such as accuracy, precision, recall, F1-score, false positive rate (FPR), false negative rate (FNR), training time, and memory usage. The Proposed Model performed best with a combination of all three techniques, especially in accuracy (91.8%), precision (88.6%), and recall (90.4%). While combining techniques improves results, the Proposed Model stands as the most effective solution for cybersecurity anomaly detection.

*ISSN: 2456-5660 Volume 10, Issue 02 (Feb -2025)*
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i02.pp95- 107*

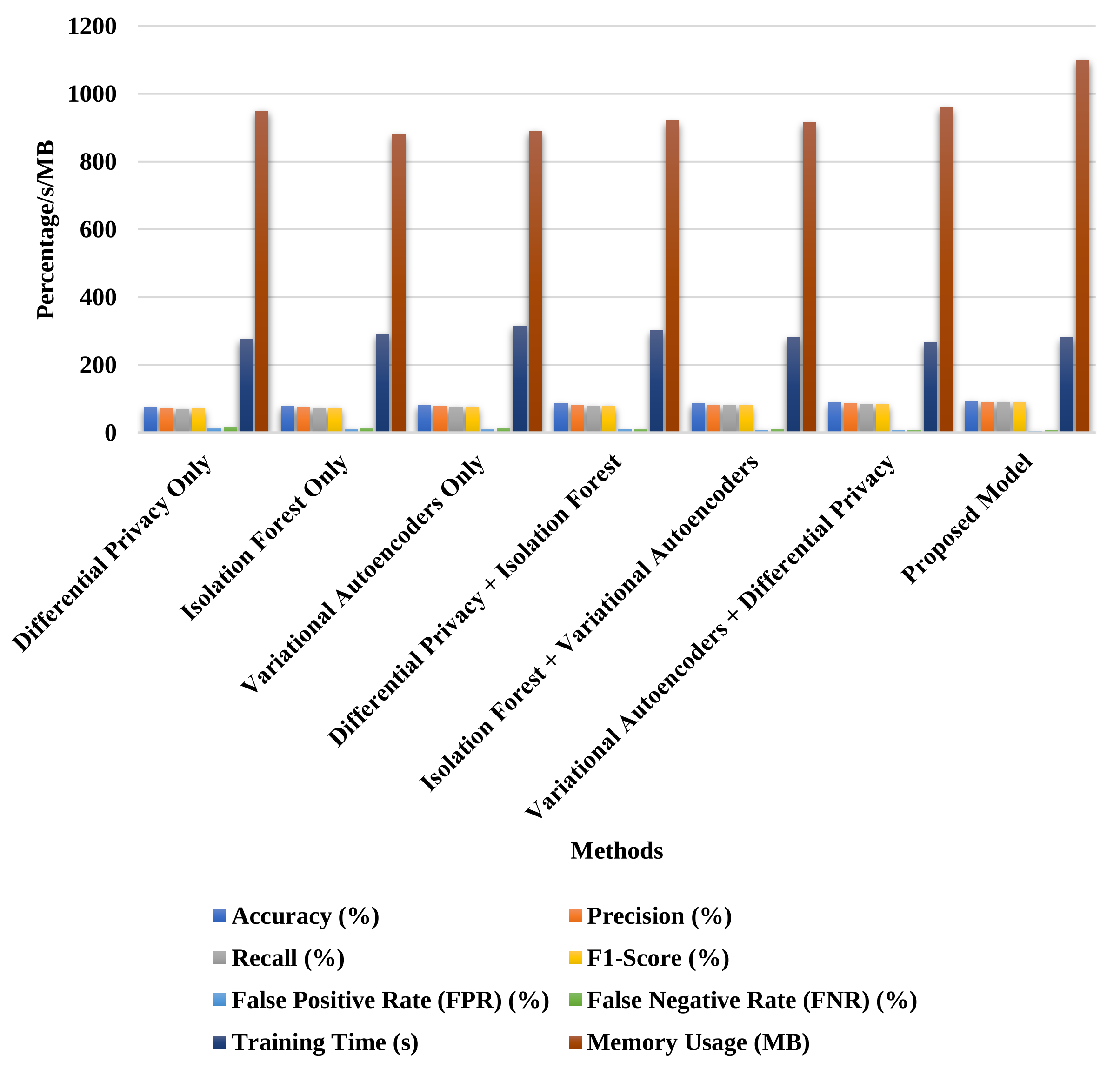


**Figure 3 Ablation Study of Various Model Combinations**

Figure 3 shows the ablation study, which indicates how the performances of different model combinations and synergy between Differential Privacy (DP), Isolation Forest (IF), and Variational Autoencoders (VAE) on accuracy, precision, recall, F1-score, false positive rate (FPR), false negative rate (FNR), time for training, and memory usage. The Proposed Model, integrating all the three techniques, outperforms the other combinations across all metrics, especially in the accuracy (91.8%), precision (88.6%), and recall (90.4%). Other combinations also show improvement but are not up to the mark of the Proposed Model's efficiency and effectiveness in cybersecurity anomaly detection.

## 5. CONCLUSION AND FUTURE ENHANCEMENT

This paper proposes a Blockchain-Assisted Federated Learning (BAFL) framework to improve cybersecurity via Federated Learning, Differential Privacy, Isolation Forest, and Variational Autoencoders. The model results in an accuracy of 91.8%, precision of 88.6%, and recall of 90.4%, with false positives at 5.3% and false negatives at 6.2%. It has good performance on the large-scale data of cybersecurity by consuming only 280.1 seconds of training time and 1100 MB of memory usage. Blockchain ensures secure, tamper-proof model updates, fostering trust in distributed environments. Future work can optimize real-time threat detection, integrate quantum-safe encryption, and enhance adaptability for evolving cyber threats in decentralized systems.

**References**

1. Tao, X., Peng, Y., Zhao, F., Zhao, P., & Wang, Y. (2018). A parallel algorithm for network traffic anomaly detection based on Isolation Forest. International Journal of Distributed Sensor Networks, 14(11), 1550147718814471.
2. Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., & Ilie-Zudor, E. (2018). Chained anomaly detection models for federated learning: An intrusion detection case study. Applied Sciences, 8(12), 2663.
3. Abdulhammed, R., Faezipour, M., Abuzneid, A., & AbuMallouh, A. (2018). Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic. IEEE sensors letters, 3(1), 1-4.
4. Ryffel, T., Trask, A., Dahl, M., Wagner, B., Mancuso, J., Rueckert, D., & Passerat-Palmbach, J. (2018). A generic framework for privacy preserving deep learning. arXiv preprint arXiv:1811.04017.
5. Chen, Q., Xiang, C., Xue, M., Li, B., Borisov, N., Kaarfar, D., & Zhu, H. (2018). Differentially private data generative models. arXiv preprint arXiv:1812.02274.
6. Alotaibi, A. (2018). Wisdom of the machines: federated learning using OPAL (Doctoral dissertation, Massachusetts Institute of Technology).
7. Shayan, M., Fung, C., Yoon, C. J., & Beschastnikh, I. (2018). Biscotti: A ledger for private and secure peer-to-peer machine learning. arXiv preprint arXiv:1811.09904.
8. Ning, X., Zheng, Y., Jiang, Z., Wang, Y., Yang, H., & Huang, J. (2018). A Bayesian nonparametric topic model with variational auto-encoders.
9. Zhang, Y. (2018). Deep generative model for multi-class imbalanced learning.
10. Narayana, P. (2018). A prototype to detect anomalies using machine learning algorithms and deep neural network. In Computational Vision and Bio Inspired Computing (pp. 1084-1094). Springer International Publishing.
11. Hynes, N., Dao, D., Yan, D., Cheng, R., & Song, D. (2018). A demonstration of sterling: a privacy-preserving data marketplace. Proceedings of the VLDB Endowment, 11(12), 2086-2089.
12. Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. arXiv preprint arXiv:1712.07557.
13. Zhou, W., Li, Y., Chen, S., & Ding, B. (2018, October). Real-time data processing architecture for multi-robots based on differential federated learning. In 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 462-471). IEEE.
14. Hartmann, F. (2018). Federated learning. Freie Universität Berlin.

15. McMahan, H. B., Andrew, G., Erlingsson, U., Chien, S., Mironov, I., Papernot, N., & Kairouz, P. (2018). A general approach to adding differential privacy to iterative training procedures. arXiv preprint arXiv:1812.06210.
16. Zhang, T., & Zhu, Q. (2017). Dynamic Differential Privacy for ADMM-Based Distributed Classification Learning. IEEE Transactions on Information Forensics and Security, 12(1), 172–187.
17. Harder, F., Köhler, J., Welling, M., & Park, M. (2018). DP-MAC: The Differentially Private Method of Auxiliary Coordinates for Deep Learning.
18. Malomo, O., Rawat, D. B., & Garuba, M. (2018). Next-generation cybersecurity through a blockchain-enabled federated cloud framework. The Journal of Supercomputing, 74(10), 5099–5126.
19. https://www.kaggle.com/datasets/ameerhamza123/intrusion-detection-dataset