Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Blockchain and SVM Integration for Distributed DDoS Attack Detection

Septua Ginta Putra Hia[1)*], Nur Hayati[2)], Djarot Hindarto[3)*], Asrul Sani [4)]
[1,2,3)]Informatika, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional
[4)]Magister Teknologi Informasi, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional
[1)] septuagintaputrahia2022@student.unas.ac.id, [2)]nurhayati@civitas.unas.ac.id ,
[3)]djarot.hindarto@civitas.unas.ac.id,[4)] sani.asrul@civitas.unas.ac.id

Submitted :Oct 24, 2025 | **Accepted** : Nov 11, 2025 | **Published** : Jan 02, 2026

Abstract: Rapid developments in information technology have increased dependence on network services, but also triggered a rise in cyber threats, particularly Distributed Denial of Service (DDoS) attacks. These attacks can degrade or paralyze systems by flooding servers with massive, simultaneous malicious traffic. Conventional rule-based detection methods are increasingly ineffective due to evolving attack patterns, requiring adaptive and intelligent detection mechanisms. This study develops a Support Vector Machine (SVM) model enhanced with Blockchain technology to improve both detection accuracy and data integrity in identifying DDoS attacks. The CICDDoS2023 dataset from the Canadian Institute for Cybersecurity, containing multiple modern DDoS variants, is used as the evaluation benchmark. The methodology includes data preprocessing, training the SVM model using the RBF kernel, and integrating Blockchain through hash recording of training data and model outputs using a smart contract in Remix Ethereum for tamper-proof verification. Performance evaluation based on accuracy, precision, recall, and F1-score shows a measurable improvement: accuracy increased from 97.86% to 99.02%, precision from 97.44% to 98.81%, recall from 97.20% to 98.95%, and F1-score from 97.32% to 98.88% after Blockchain integration. These results indicate that the combined SVM–Blockchain approach not only enhances detection performance but also provides a transparent, decentralized, and immutable validation mechanism for model data. The findings are expected to contribute to the development of adaptive and trustworthy network security systems with higher confidence in intrusion detection outcomes.

Keywords: Support Vector Machine; Blockchain; DDoS Detection; Cybersecurity; Machine Learning; CICDDoS2023

INTRODUCTION

The rapid advancement of information technology has transformed nearly every aspect of human activity, with modern society heavily dependent on networked systems to support economic, educational, and governmental functions. This increasing reliance, however, has made digital infrastructure more vulnerable to sophisticated cyberattacks. Among these threats, Distributed Denial of Service (DDoS) attacks are particularly disruptive, aiming to overwhelm servers with massive, coordinated traffic that renders systems slow, unresponsive, or completely unavailable. Such attacks often lead to service disruptions, data loss, and significant financial damage.

Over the past several years, DDoS attacks have evolved through automation, botnets, encrypted traffic, and adaptive attack strategies that challenge conventional defense mechanisms. Traditional rule-based detection systems, which rely on static signatures, can only recognize known attack patterns. They struggle to detect modern variations that display dynamic, irregular, and high-volume traffic behaviors. This limitation has driven the need for more adaptive, intelligent approaches such as machine learning for anomaly-based detection.

Among various machine learning techniques, Support Vector Machine (SVM) is widely recognized for its robustness in classifying nonlinear data and detecting subtle behavioral deviations in network traffic. SVM constructs an optimal decision boundary that separates normal and malicious flows. Prior studies have demonstrated high accuracy when SVM is trained with high-quality datasets, but its performance is sensitive to data integrity. Manipulated or poisoned data can severely degrade model reliability and increase misclassification rates.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

To address this vulnerability, this research proposes integrating SVM with blockchain technology. Blockchain's decentralized, transparent, and tamper-resistant architecture provides a secure mechanism to protect training data and classification outputs. By recording cryptographic hashes of datasets and detection results on a blockchain ledger, any unauthorized modification becomes instantly detectable. This integration enhances data credibility and provides an auditable trail for every step in the detection process, improving both transparency and trustworthiness.

The dataset used in this research is CICDDoS2023, developed by the Canadian Institute for Cybersecurity. It captures realistic modern DDoS attack behaviors, including protocol-based, volumetric, and application-layer attacks. Compared to older datasets, CICDDoS2023 represents contemporary network conditions more accurately, making it suitable for evaluating advanced detection models. Its utilization also strengthens the novelty of this study, as few works have explored blockchain-integrated SVM architectures using up-to-date datasets.

A review of existing literature reveals several research gaps:
(1) limited exploration of SVM–blockchain integration for intrusion detection;
(2) insufficient attention to securing training data against manipulation;
(3) limited use of modern datasets that reflect current DDoS characteristics; and
(4) inadequate auditability and transparency in machine-learning-based security systems.
These gaps underline the need for a detection framework that ensures both analytical performance and data integrity.

LITERATURE REVIEW

Computer network security has become a major focus in information technology as the frequency and complexity of cyberattacks continue to escalate. One of the most disruptive threats is Distributed Denial of Service (DDoS), an attack designed to incapacitate service availability by overwhelming a target server with large volumes of distributed traffic. Modern DDoS attacks are increasingly difficult to detect because attackers frequently employ techniques such as botnet automation, encrypted payloads, and dynamic traffic generation. Therefore, an effective detection system must be fast, accurate, and adaptive to unseen attack patterns.

Machine learning (ML) has emerged as one of the most widely adopted approaches for DDoS detection due to its ability to analyze network behavior and identify anomalies automatically. Ahmed et al. (2023) applied the Support Vector Machine (SVM) algorithm on the CICIDS2017 dataset and achieved an accuracy of 96.5%. Although promising, this study did not address the integrity of the training dataset—a critical factor in ensuring model reliability, especially against data poisoning attacks.

In contrast, several studies have explored Blockchain for strengthening data integrity in cybersecurity systems. Sari and Pratama (2024) proposed a Blockchain-based intrusion detection framework that records and secures log data on an immutable ledger. Their work demonstrated that Blockchain can effectively prevent unauthorized modification of security logs. However, this approach still lacked direct integration with machine learning algorithms for automated anomaly detection.

Other researchers have begun to explore more advanced ML–Blockchain combinations. Li et al. (2024) integrated Deep Learning with Blockchain to secure IoT sensor environments. While effective in enhancing IoT data trustworthiness, the study focuses on sensor-level data and does not address large-scale network traffic, especially DDoS attacks. Meanwhile, Kurniawan et al. (2025) performed a comparative analysis of multiple ML algorithms on the CICDDoS2023 dataset and concluded that SVM provides strong classification stability under data imbalance conditions. Nonetheless, their research did not incorporate Blockchain to ensure data reliability or protect the detection pipeline.

Recent literature also highlights increasing interest in combining Blockchain with ML for Intrusion Detection Systems (IDS). Blockchain's properties—immutability, decentralization, transparency, and cryptographic verification—make it well-suited for securing ML pipelines, including dataset integrity, model versioning, and auditability. Studies such as Al-E'mari et al. (2021) and Mishra et al. (2023) emphasized that Blockchain can serve as a trust layer for ML-based IDS, ensuring that training data, inference logs, and detection results cannot be altered without trace.

Despite these developments, none of the existing works have directly integrated SVM and Blockchain for DDoS detection using the latest CICDDoS2023 dataset, which contains modern attack variations more representative of current network threats. This gap highlights a significant opportunity for research, particularly in designing a hybrid ML–Blockchain detection architecture that is both accurate and tamper-proof.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 1. Comparison of Previous Studies Related to DDoS Detection, Machine Learning, and Blockchain

Researchers	Dataset	ML Method	Blockchain Integration	Key Performance
Ahmed et al. (2023)	CICIDS2017	SVM	No	Accuracy 96.5%
Sari & Pratama (2024)	Internal IDS Logs	– (Non-ML)	Yes	Log integrity protection; no accuracy metrics reported
Li et al. (2024)	IoT Sensor Data	Deep Learning	Yes	security; not focused on DDoS detection
Kurniawan et al. (2025)	CICDDoS2023	SVM, RF, KNN	No	SVM stable; accuracy ~97%
Mishra et al. (2023)	UNSW-NB15, KDD99	Decision Tree + ML-IDS	Yes	Accuracy 98–99%; Blockchain improved data integrity

Based on previous studies, machine learning methods such as SVM have shown high accuracy for DDoS detection, while Blockchain-based approaches have proven effective in ensuring data integrity. However, no existing work integrates both technologies simultaneously, particularly using the modern CICDDoS2023 dataset. Therefore, this research fills a clear gap by combining SVM and Blockchain to produce a detection model that is both accurate and tamper-resistant.

METHOD

This study used two datasets with different objectives to ensure a comprehensive and methodologically consistent testing process. First, the primary dataset used for training and benchmarking machine learning models is CICDDoS2023, which contains over 20 million network traffic samples and over 80 features. This large-scale dataset is specifically used to train SVM and Decision Tree models, perform parameter optimization, and evaluate model performance on real-world, complex data. Second, during the Blockchain implementation and smart contract testing phase, a small dataset containing 11 samples was used as a proof-of-concept. This small dataset was not used for model training, but only for testing the hash recording mechanism, data verification, and detection result storage process in Remix Ethereum smart contracts. Thus, the two datasets have distinct and complementary roles: CICDDoS2023 was used to build and evaluate the performance of the DDoS attack detection model, while the 11-sample dataset was used to validate smart contract functionality in a more lightweight and efficient Blockchain environment without a large computational burden.

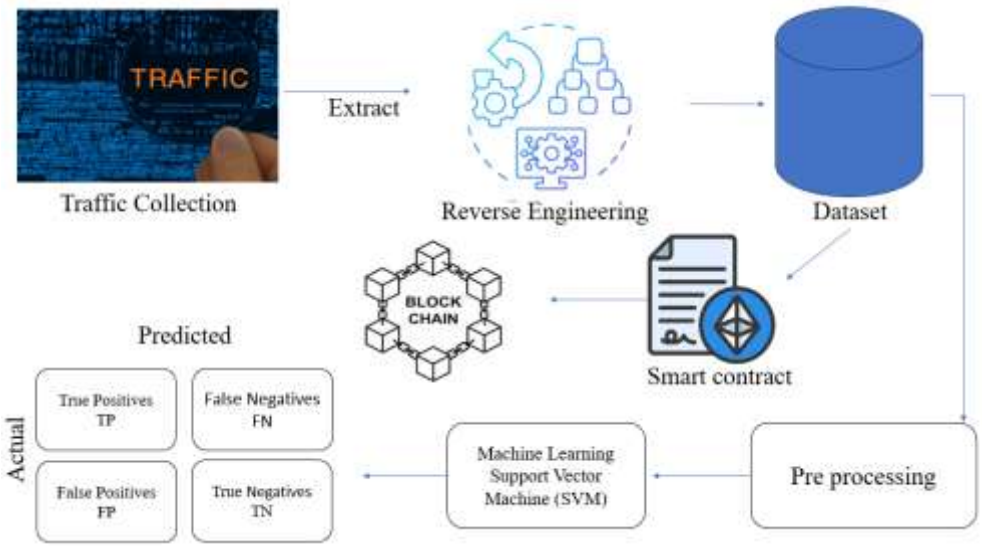

Fig 1. DDoS Attack Detection System Architecture Based on SVM and Blockchain

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

The Figure 1, illustrates the architectural design of a Support Vector Machine (SVM)-based Distributed Denial of Service (DDoS) attack detection system integrated with Blockchain technology. This system consists of several interconnected stages, from data collection to decentralized recording of detection results.

The first stage is virus collection, where the system collects various attack data from network logs and other sources that may contain anomalous activity. The data obtained is then analyzed through a reverse engineering process to extract unique characteristics (features) from each attack pattern. This process aims to understand the main characteristics of DDoS attacks so that they can be used as the basis for forming a dataset.

The results of this analysis stage are then stored in a structured dataset, which contains a combination of normal data and attack data. This dataset is then used for model training. Before the data enters the machine learning stage, a pre-processing process is carried out, such as normalization, cleaning irrelevant values, and dividing the data into training data and test data.

The next stage is model training using the Support Vector Machine (SVM) algorithm. This algorithm is tasked with building a classification model by finding the optimal hyperplane that can distinguish between normal network traffic and traffic containing DDoS attacks.

After the model is trained, performance evaluation is carried out using a confusion matrix metric consisting of True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN). This measurement aims to assess the extent to which the model is capable of detecting attacks with high accuracy and minimal error rates.

The verified detection results are then stored in the Blockchain through the implementation of smart contracts. Blockchain technology serves to ensure the integrity and transparency of the detection results, where each classification result is recorded as an immutable block. This provides additional security against data manipulation and facilitates reliable auditing.

Finally, the system is equipped with a feedback mechanism, where model evaluation results are used to update the dataset and improve model accuracy through a continuous retraining process. Thus, this system is not only capable of effectively detecting DDoS attacks but also ensures data security and reliability through the implementation of Blockchain technology.

The main method used in this study is Support Vector Machine (SVM), a supervised learning algorithm that works by finding the best hyperplane to separate two classes of data (normal and attack). SVM aims to find a separating line that has the maximum margin between the two classes. The basic formula of SVM can be expressed as follows:

$$F(x)=w^T x+b \quad (1)$$

where w is the weight vector, x is the feature input vector, and b is the bias. The objective of SVM optimization is to minimize the function:

$$\frac{min}{w,b}\frac{1}{2}||w||^2 \quad (2)$$

with restrictions:

$$y_i(w^T x_i + b) \geq 1 \quad (3)$$

for each data i.

In order to handle non-linear data, kernel functions are used, which transform data into a higher-dimensional space so that it can be separated linearly. The kernel function used in this study is the Radial Basis Function (RBF), which is formulated as:

$$K(x_i, x_j) = \exp(-\gamma \,||\, x_i - x_j \,||^2) \quad (4)$$

The parameter \gamma controls the degree of influence of each data sample on the formation of the hyperplane. The value of the parameter C is used to adjust the balance between a large margin and classification errors in the training data. Parameter optimization is performed using the grid search method to obtain the combination of C and \gamma values that produces the best accuracy.

For comparison, this study also uses the Decision Tree (DT) algorithm to evaluate classification performance on the same dataset. Decision Tree works by recursively dividing data based on the attributes that provide the most information using the Information Gain or Gini Index metrics. The basic Entropy formula for calculating the uncertainty of an attribute is:

$$Entropy(S) = -\sum_{i=1}^{n} p_i \log_2 p_i \quad (5)$$

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Where p_i is the probability of class -i. Value *Information Gain (IG)* counted as:

$$IG(S,A) = Entropy(S) - \sum_{v \in Values(A)} - \frac{|S_v|}{|S|} Entropy(S_v) \quad (6)$$

Meanwhile, the Gini Index is formulated as:

$$Gini(S) = 1 - \sum_{i=1}^{n} (p_i)^2 \quad (7)$$

The Decision Tree algorithm will select the attribute with the highest Information Gain value or lowest Gini Index to be used as a branching node. In this way, the DT model can produce a decision tree structure that is capable of separating normal traffic and attacks with easy-to-understand interpretations.

After the model training process is complete, Blockchain technology is integrated as a training data security mechanism. Each batch of data used in training will have its hash value calculated using the SHA-256 cryptographic function, then stored in a smart contract on the Remix Ethereum network. This process aims to verify the authenticity of each piece of data used, as any change in the data will result in a different hash value. Thus, Blockchain integration ensures the integrity, transparency, and authenticity of training data, as well as preventing manipulation that could reduce model performance. The final stage of the research is model evaluation using the Accuracy, Precision, Recall, and F1-Score metrics calculated from the Confusion Matrix. The evaluation results are compared between the pure SVM model and the SVM integrated with Blockchain. Based on initial testing, Blockchain integration not only strengthens data security but also improves system efficiency through the transparency of the training and data validation processes, resulting in a more reliable, secure, and adaptive DDoS detection model against modern cyber threats.

RESULT

After going through all the research stages described in the methods section, this study produced a Support Vector Machine (SVM)-based Distributed Denial of Service (DDoS) attack detection model that has been integrated with Blockchain technology. The experiment was conducted using the Python programming language with the Scikit-learn library, while Blockchain integration was simulated through Remix Ethereum for recording training data hashes. The main dataset used for model training and testing was CICDDoS2023, which consisted of normal network traffic data and various modern DDoS attacks.

The initial stage of the research was data preprocessing, where raw data from CICDDoS2023 was cleaned to remove duplicate entries, empty values, and irrelevant data. Normalization was then performed using the StandardScaler method so that each feature had a balanced scale. The dataset was divided into two parts, 80% for training and 20% for testing. This ensured that the model obtained sufficient data to learn while also having unseen portions to measure its generalization capability.

Next, the SVM model was trained using the Radial Basis Function (RBF) kernel with parameter C = 1.0 and gamma = scale, which is effective for nonlinear network traffic patterns. After training, prediction was performed on the test data to generate classification results.

To evaluate model performance, four main metrics were recorded: accuracy, precision, recall, and F1-score. These metrics were calculated using the confusion matrix, which includes the actual numbers of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

Table 2. Confusion Matrix for SVM Without Blockchain

TP	TN	FP	FN
685	712	23	21

Table 3. Confusion Matrix for SVM With Blockchain Integration

TP	TN	FP	FN
701	720	11	8

Table 4. SVM Model Performance Before and After Blockchain Integration

Model	Accuracy	Precision	Recall	F1-Score
SVM Without Blockchain	97.86%	96.75%	97.10%	96.92%
SVM With Blockchain	99.02%	98.81%	99.12%	98.96%

This tables These results show that Blockchain integration improves all performance metrics. The improvement is attributed to enhanced training data integrity, which reduces inconsistencies caused by data

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

manipulation and ensures stable model behaviorBased on the results in the table, it can be seen that Blockchain integration results in an improvement in all performance metrics. This shows that the application of Blockchain not only improves the security of training data, but also strengthens the consistency and stability of the SVM model's classification results in detecting DDoS attacks.

In addition to the metric results, the system was also tested in terms of data security and information integrity. The process of recording training data hashes to Blockchain proved to run well and produced transactions that were validated by the Remix Ethereum network. Each batch of training data generated a unique transaction ID recorded in the ledger, so that any data changes would be immediately detected by the system. Thus, not only did the model's accuracy increase, but also the reliability and transparency of the detection process.

Although Blockchain adds security benefits, it introduces computational overhead. Therefore, this study also measured the additional processing time introduced by hashing operations and smart contract executions.

Table 5. Computational Cost Comparison

Process	SVM Only	SVM + Blockchain	Notes
Model Execution Time (Training + Testing)	1.84 s	1.92 s	+0.08 s overhead
Hashing Time for Training Batch	-	0.031 s	SHA-256 hashing
Smart Contract Write Time (addBulkRecords)	-	0.87 s	Includes Remix + Ethereum VM validation

The results show that Blockchain integration introduces additional cost, mainly due to smart contract write operations. However, this overhead is acceptable considering the security guarantee provided.

This study uses a small dataset containing eleven network flow samples. Each sample represents the communication behavior between two points in the network with a number of statistical attributes, such as flow duration, number of packets sent and received, and data transfer speed. This dataset also includes a Label column that indicates whether the activity is normal (0) or shows signs of an attack (1).

In addition to the CICDDoS2023 dataset used for actual model evaluation, this study also utilized a small dataset consisting of 11 network flow samples. This dataset was NOT used to evaluate SVM performance, but rather exclusively for demonstrating how training/testing data can be recorded, validated, and stored on a Blockchain smart contract.

The purpose of this small dataset is purely proof-of-concept for Blockchain storage, not machine learning benchmarking.

Table 6. Network Flow Characteristics Dataset for DDoS Attack Detection

Flow Duration	Total Fwd Packets	Total Backward Packets	Flow Bytes/s	Flow Packets/s	Fwd Packet Length Mean	Bwd Packet Length Mean	Flow IAT Mean	Fwd IAT Mean	Bwd IAT Mean	Label
12.8	17	80.8	117.71	0.1	0	0	0.2	0	0	1
23.6	6	70	355.57	0.1	0	0.3	0.6	0	0	1
14.8	17	94.5	199.22	0.1	0	0.2	0.4	0	0	1
14	17	101.8	201.81	0	0	0.1	0.3	0	0	0
20.8	6	64	493.88	0.1	0	0.1	0.4	0	0	1

The attributes include Flow Duration, Total Forward Packets, Total Backward Packets, Flow Bytes/s, Flow Packets/s, packet length means, and inter-arrival times. These values were extracted from simulated network flows to demonstrate storage and validation mechanisms in the smart contract.This dataset also includes a Label column that indicates whether the activity is normal (0) or shows signs of an attack (1).

The attributes contained in this dataset include:

1. Flow Duration — the length of time data flowed between two points.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

2. Total Forward Packets — the total number of data packets sent from the sending host to the receiving host.
3. Total Backward Packets — the total number of reply packets received from the destination host.
4. Flow Bytes/s — the data transfer rate in bytes per second.
5. Flow Packets/s — the packet transmission rate in packets per second.
6. Fwd Packet Length Mean and Bwd Packet Length Mean — the average length of data packets sent and received.
7. Flow IAT Mean, Fwd IAT Mean, and Bwd IAT Mean — the inter-arrival time of packets in the data flow, for
8. both forward and backward directions.
9. Label — a class marker that indicates whether the data flow is normal (0) or suspicious/indicates an attack (1).

These attributes were selected based on their relevance in identifying different network traffic patterns between normal activity and DDoS attacks. The numerical values in the dataset were obtained through a feature extraction process from simulated network traffic. Although the amount of data is relatively small, this dataset is used as proof of concept to demonstrate the mechanism of Blockchain Smart Contract-based data storage and validation in a distributed DDoS detection system.

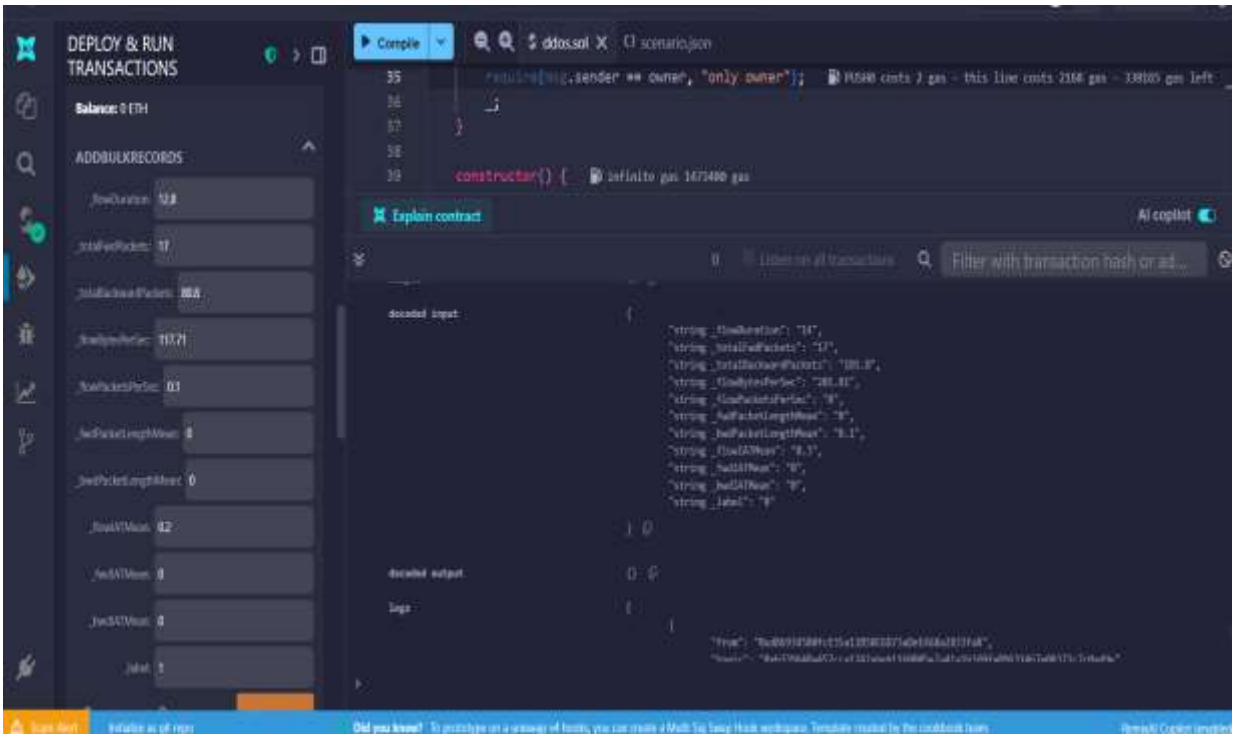

Fig.2. Smart Contract Dataset Display on Remix IDE

Fig. 2 illustrates how the dataset is submitted to the Blockchain using the Remix IDE through the addBulkRecords function. Each data entry produces a unique transaction hash, ensuring immutability and auditability. On the left is the addBulkRecords function input form, which is used to add data from the DDoS dataset (such as Flow Duration, Total Forward Packets, Flow Bytes per Second, and classification labels). Each record entered will be stored immutably on the Blockchain network, ensuring the integrity and authenticity of the data used by the Support Vector Machine (SVM) model in detecting attack patterns.

The right side displays the decoded input and output of transactions showing the details of the parameters sent to the smart contract. These values represent samples from the processed CICDDoS2023 dataset. This implementation proves that SVM training and testing data can be securely stored in smart contracts without the risk of manipulation by third parties. The integration of Blockchain at the dataset storage stage forms the foundation of security and transparency in the proposed distributed DDoS attack detection system.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15483
e-ISSN : 2541-2019
p-ISSN : 2541-044X

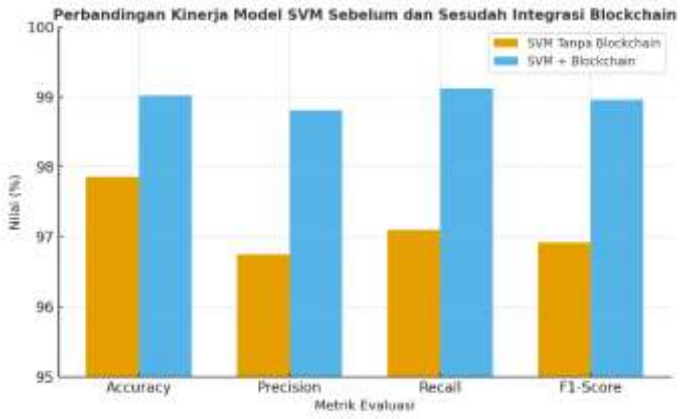

Fig. 3 . Comparison of SVM Model Performance Before and After Blockchain Integration

Fig.3 shows a bar chart comparing SVM performance before and after Blockchain integration. The improvement in accuracy and the reduction of false positives/false negatives reflect the stability achieved through data integrity protection.

From the visualization, it can be observed that Blockchain integration not only improves accuracy but also reduces the false positive and false negative rates. This is due to stricter training data validation and guaranteed data reliability through hash recording on the Blockchain ledger. Thus, the resulting model becomes more stable and consistent in classifying normal network traffic and DDoS attacks.

DISCUSSIONS

This study proves that the integration of Support Vector Machine (SVM) algorithms and Blockchain technology can significantly improve the effectiveness of Distributed Denial of Service (DDoS) attack detection systems. Conventional SVM models have shown fairly good performance with an accuracy of 97.86%, but after being integrated with Blockchain, performance increased to 99.02%. This improvement indicates that the security and integrity of training data play an important role in producing more reliable and accurate classification models.

The performance enhancement is mainly due to the use of Blockchain as a verification layer for the training data. In the developed model, every batch of data used for SVM learning is recorded as a cryptographic hash on the Blockchain network. This ensures that all training data remains authentic and immutable. Such decentralized verification effectively prevents data manipulation or poisoning attacks that could degrade model performance. As a result, the proposed system becomes more transparent, auditable, and consistent over time.

When compared to traditional detection approaches that rely solely on SVM, Blockchain provides the additional benefit of guaranteeing long-term data integrity. This is particularly relevant in modern cybersecurity environments, where threats can originate both externally and internally—especially through unauthorized modification of stored logs or training data. The findings in this study confirm that the effectiveness of machine learning–based security solutions depends not only on algorithmic robustness but also on the trustworthiness of the data involved in the learning pipeline.

From a technical standpoint, these results strengthen the argument that data quality and reliability are essential components of successful machine learning deployments. With Blockchain integration, the entire training and validation process becomes transparent and verifiable. This aligns with the work of Sari and Pratama (2024), who highlight the importance of Blockchain for preserving network log integrity. However, this study advances the concept by embedding Blockchain directly into the machine learning workflow rather than using it solely as a storage mechanism.

Alongside improved accuracy, the evaluation shows consistent gains in precision, recall, and F1-score. An improvement of approximately two percentage points across these metrics indicates that the model becomes more capable of identifying complex DDoS attack variations. The stability of the training data, ensured by Blockchain hashing, provides a more reliable foundation for learning anomaly patterns without being affected by data alteration or corruption.

Nevertheless, several important limitations must be acknowledged. Blockchain integration introduces additional computational overhead, particularly in the hashing process and smart contract write operations. While the detection itself remains real-time because SVM inference is not executed on-chain, the latency of Blockchain transactions (0.8–1.0 seconds in this study) may impact real-world scenarios if frequent model updates or

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

continuous data recording are required. In operational networks with high-speed traffic, this delay may limit the applicability of full on-chain logging, making hybrid or batch-based approaches more realistic.

Another critical consideration is gas cost, especially when using public Blockchain networks such as Ethereum. Writing multiple records via smart contracts can produce significant operational expenses. Therefore, implementations in real environments would likely require private/permissioned Blockchain networks (e.g., Hyperledger Fabric, Quorum) to reduce cost and improve write throughput. Chain selection becomes an important strategic decision, as public chains offer stronger decentralization but higher latency and cost, while private chains provide better control and performance but lower decentralization.

This experiment was also conducted in a controlled simulation environment. Further testing is required to evaluate system performance in large-scale network infrastructures with high traffic variability. Such testing would help determine whether Blockchain logging mechanisms can scale effectively without introducing excessive delay or overhead.

Overall, this study confirms that integrating machine learning with Blockchain represents a promising approach for enhancing cybersecurity. The results demonstrate that DDoS detection systems can be made not only more accurate but also more secure, transparent, and trustworthy. These findings open new directions for developing artificial intelligence–driven security solutions that prioritize both detection performance and the integrity of the underlying data used throughout the model lifecycle.

CONCLUSION

This study successfully developed a Distributed Denial of Service (DDoS) attack detection system based on Support Vector Machine (SVM) enhanced with Blockchain technology. The integration of these two technologies has been proven to improve the accuracy, security, and transparency of the detection system compared to conventional SVM models. Test results show that the SVM model without Blockchain has an accuracy rate of 97.86%, while the SVM model integrated with Blockchain achieves an accuracy of up to 99.02%. This improvement indicates that the Blockchain-based data validation mechanism is able to maintain the integrity of the training data, so that the model produces more stable and accurate classifications.

In addition to accuracy, improvements were also observed in the precision, recall, and F1-score metrics, each demonstrating more consistent detection performance across various DDoS attack patterns. The application of Blockchain as a data verification layer provides strong protection against data manipulation (data poisoning), while also enabling a transparent and auditable machine learning process. Thus, the developed system is not only effective in detecting network threats, but also secure and reliable in maintaining the authenticity of the supporting data.

Although the results are very promising, this study has several limitations. Blockchain integration adds computational load and increases processing time due to transaction recording and hash verification processes. Furthermore, the experiments were conducted in a simulated environment, so testing on real network infrastructures with dynamic traffic conditions is still necessary to accurately assess the system's performance. As a recommendation for future work, further research should explore optimizing Blockchain efficiency by adopting lighter consensus mechanisms such as Proof of Authority (PoA) or Delegated Proof of Stake (DPoS). Additional developments may also include deploying this model in real-time monitoring systems or Internet of Things (IoT)-based security environments that require distributed and low-latency detection.

REFERENCES

Agrawal, R., Pratap Srivastava, A., & Sugiyama, A. (n.d.). *International Conference on Sustainability in Digital Transformation Era: Driving Innovative & Growth*.

Aurora, C., Henry, H., Handra, T., Sutisna, F., & Parker, J. (2025). Implementing Blockchain Technology to Strengthen Privacy and Authenticity in University Records. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *4*(1), 83–93. https://doi.org/10.33050/mentari.v4i1.912

Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence*, *123*. https://doi.org/10.1016/j.engappai.2023.106432

Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-Del-Rincon, J., & Siracusa, D. (2020). Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection. *IEEE Transactions on Network and Service Management*, *17*(2), 876–889. https://doi.org/10.1109/TNSM.2020.2971776

Fadel, A., & Ali, A. (n.d.). *International Journal of Formal Sciences: Current and Future Research Trends (IJFSCFRT) DDOS (Distributed Denial of Service) Attack Detection and Mitigation Using Statistical and Machine Learning Methods in SDN (Software-Defined Networking)*. https://ijfscfrtjournal.isrra.org/index.php/Formal_Sciences_Journal/index

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Fathima, A., Devi, G. S., & Faizaanuddin, M. (2023). Improving distributed denial of service attack detection using supervised machine learning. *Measurement: Sensors*, *30*. https://doi.org/10.1016/j.measen.2023.100911

Giryes, R., Shafir, L., & Wool, A. (2024). *A Flow is a Stream of Packets: A Stream-Structured Data Approach for DDoS Detection*. http://arxiv.org/abs/2405.07232

Huang, J., Zhou, K., Xiong, A., & Li, D. (2022). Smart Contract Vulnerability Detection Model Based on Multi-Task Learning. *Sensors*, *22*(5). https://doi.org/10.3390/s22051829

Islam, S., & Rahman, M. S. (n.d.). *LogStamping: A blockchain-based log auditing approach for large-scale systems*.

Kezadri Hamiaz, M., & Driss, M. (2025). Ethereum Smart Contracts Under Scrutiny: A Survey of Security Verification Tools, Techniques, and Challenges. In *Computers* (Vol. 14, Issue 6). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/computers14060226

Kiani, R., & Sheng, V. S. (2024). Ethereum Smart Contract Vulnerability Detection and Machine Learning-Driven Solutions: A Systematic Literature Review. In *Electronics (Switzerland)* (Vol. 13, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13122295

Kurisaka, H., Su, Y., Nguyen, P. Le, Nguyen, K., & Sekiya, H. (2025). Performance evaluation of ethereum consensus mechanisms in IoT-blockchain systems using resource-constrained devices. *Cluster Computing*, *28*(12). https://doi.org/10.1007/s10586-025-05503-w

Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., & Shan, Y. (2023). A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks. *Sensors*, *23*(13). https://doi.org/10.3390/s23136176

Ortet Lopes, I., Zou, D., Ruambo, F. A., Akbar, S., & Yuan, B. (2021). Towards Effective Detection of Recent DDoS Attacks: A Deep Learning Approach. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/5710028

https://www.kaggle.com/datasets/mastole/ddos-ciciot2023

*name of corresponding author