INTERNATIONAL JOURNAL OF SCIENTIFIC INFORMATION

Research | ISSN: 2583-8512

Development of Intelligent Frameworks for Brute Force Intrusion Detection using Large Language Models

Komal and Dr. Shailesh Kumar *

Department of Computer Science and Engineering (CSE)
School of Engineering & Technology (SET), Om Sterling Global University, Hisar, Haryana, India
Komalsingh05panwar@gmail.com

Abstract

As people utilize more digital devices and networks, cyber dangers like brute force attacks that take advantage of poor authentication techniques are becoming more common. Signature-based or classical machine learning algorithms are often not very good at uncovering new and unexpected attack patterns with low false positives. This paper suggests creating a smart hybrid system that uses ML and LLMs to find brute-force attacks. The method starts with speedy initial detection through data preprocessing, feature engineering, and categorization based on machine learning. Then it moves on to semantic analysis led by LLMs, which makes it even easier to understand the context and make decisions. Experimental results reveal that the suggested hybrid model works better than solo models since it lowers false alarms and raises accuracy, precision, recall, and F1-score. Adding LLMs can help you comprehend and evaluate complicated attack behaviors more easily.

Keywords: *Brute Force Attack, IDS, LLMs, Cybersecurity, Deep Learning, Network Security, Anomaly Detection*

Address for Correspondence
Dr. Shailesh Kumar
(Professor &Dean)
Department of Computer Science and Engineering (CSE)
School of Engineering & Technology (SET)
Om Sterling Global University, Hisar, Haryana, India

Article Received on: 11.06.26
Revised on: 20.06.26
Approved for publication: 11.07.26

How to Cite this Article: **Komal and Kumar S.** ***Development of Intelligent Frameworks for Brute Force Intrusion Detection using Large Language Models*** Int., J. Sci. Info. 2026; 4 (4): 50-59

1. Introduction

Cyber-attacks are more easier to pull off now that digital technologies, cloud computing, and interconnected networks are common. Brute force attacks are one of the most common and long-lasting ways that hackers gain into systems without permission. These attacks usually hit web apps, business systems, and IoT devices. They want to break authentication methods by attempting different password combinations over and over. Finding new or changing attack patterns is getting difficult and harder for traditional intrusion detection systems (IDS) that use signature-based or rule-based techniques. Intrusion detection systems have come a long way, from basic rule-based systems to more complex machine learning (ML) and deep learning (DL) technologies. Machine learning-based intrusion detection systems have gotten better at spotting weird activity and putting risky activities into groups by looking at patterns in network traffic data. But these models have a lot of problems. For example, they have trouble with shifting attack patterns, extra input data, not comprehending the context, and feature spaces with a lot of dimensions. Also, it's hard to make clear conclusions in cybersecurity applications because many deep learning models function like black boxes. In the last few years, LLMs have proved quite useful since they can interpret sequential data, links between different contexts, and complicated patterns. LLMs were originally made to help computers understand natural language, but they have showed a lot of potential in three areas of cybersecurity: log analysis, anomaly detection, and intrusion detection.

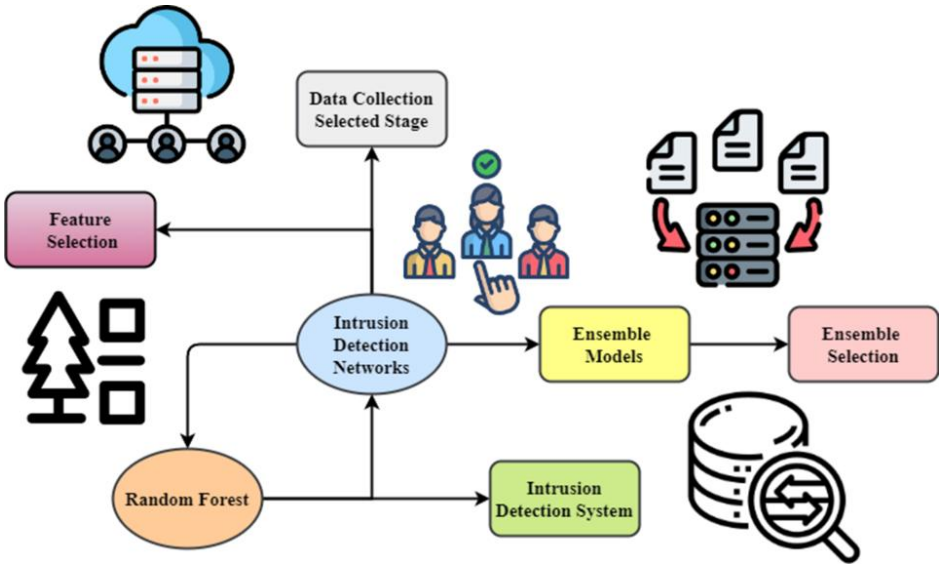

Figure 1: Machine learning based multi-stage intrusion detection system

Based on this, the major purpose of this project is to come up with a sensible way to use LLMs to find

brute-force intrusions. The suggested method uses feature engineering, machine learning-based classification, and LLM-powered semantic analysis to improve detection accuracy, cut down on false positives, and make the results easier to understand. This framework's structured network traffic operations on datasets like CICIDS and UNSW-NB15 could be used in real life in organizational networks, cloud services, and IoT systems.

2. Literature Review

Several recent studies have investigated the utilization of advanced AI approaches in intrusion detection systems. Daniel N. et al. [1] compared MITRE ATT&CK methods against LLMs for labeling NIDS rules and found that LLMs improved semantic mapping. S. G. AboulEla and R. F. Kashef [2] put forward a hybrid framework that combines LLMs, graph neural networks, and explainable AI for intrusion detection systems of the next generation. Simultaneously, A. Ali and M. C. Ghanem [3] underscored the revolutionary influence of LLMs in enhancing cybersecurity beyond conventional detection techniques. H. Ma et al. [4] put forth an architecture for an Internet of Things (IoT) intrusion detection system (IDS) that uses feature selection and LLM fine-tuning to improve detection accuracy. M. T. Bui et al. [5] evaluated the efficacy of LLMs in intrusion detection, demonstrating their functionality across several datasets. P. R. Houssel et al. [6] focused on explainable intrusion detection systems (IDS) that use large language models (LLMs) to make them easier to understand. E. Nwafor et al. have demonstrated that LLMs could be more effective in confined environments for Internet of Things intrusion detection [7]. M. Fu et al. put forward IoV-BERT-IDS, a mixed LLM-based system for vehicular networks [8]. M. H. Gewida examined the concept of integrating ML and LLMs to prevent password breaches in IoT [9]. H. Lai illustrated the use of LLMs for intrusion detection [10]; N. Alotibi and M. Alshammari created an IDS employing deep learning to identify brute-force attacks on FTP and SSH protocols [11]; and S. Sakaoglu introduced an innovative approach for detecting vulnerabilities via fine-tuned LLMs [12]. R. V. Mendonca et al. created a lightweight deep learning intrusion detection system (IDS) for the industrial Internet of Things (IoT) [14]. F. Zhou et al. put forward an intelligent IDS model for certain healthcare environments [15]. M. M. I. Jabed et al. enhanced IDS by merging business intelligence (BI) with AI-driven machine learning (ML) [13]. J. B. Awotunde and S. Misra talked about ways to apply AI to make IoT systems safer by extracting features [17]. F. Setianto et al. discussed GPT-2C, which employs pre-trained language models to analyze honeypot logs [18]. M. S. A. Muthanna et al. discussed an SDN-enabled IDS for IoT networks [16]. W. Liang et al. [19] also talked about how few-shot learning can be used to discover intrusions in IoT systems that are spread out. M. Abdel-Basset et al. [20] also discussed a semi-supervised

spatiotemporal deep learning model aimed at the same objective.

3. Problem Statement

Network security has become more critical and harder to understand as digital infrastructures, cloud services, and IoT settings have become increasingly ubiquitous. Brute force attacks are still a huge problem among cyber threats since they are easy to do and can use weak authentication mechanisms. These attacks make it hard to distinguish the difference between real traffic and login attempts, especially on big, fast networks. Traditional IDS, such as signature-based and standard machine learning methods, generally don't work well to discover these kinds of attacks since they rely on set rules and can't rapidly change as attack patterns change. Also, current models have problems with class imbalance, a lot of false positives, and being able to operate with different types of data. Deep learning models are superior, but they have some disadvantages. For example, they are hard to understand and need more computational power. Current intrusion detection systems also don't have the proper contextual understanding of how attacks work to uncover intricate and concealed brute-force attempts.

4. Proposed Framework

The suggested architecture uses both ML and LLM approaches to construct a hybrid intrusion detection system that can find brute force attacks. The system does pre-processing procedures such cleaning up data, normalizing it, and choosing features to get rid of duplicate data and speed up network traffic. The data comes from a variety of different areas, such IoT devices and enterprise networks. The LLM module employs contextual and semantic analysis on the suspicious patterns it detects to cut down on false positives and learn more about how the attack works. Last but not least, an intelligent reaction system helps people make choices and sends forth signals. This hybrid model is better than more traditional ways since it makes it easier to find things, scale up, and understand what you find.

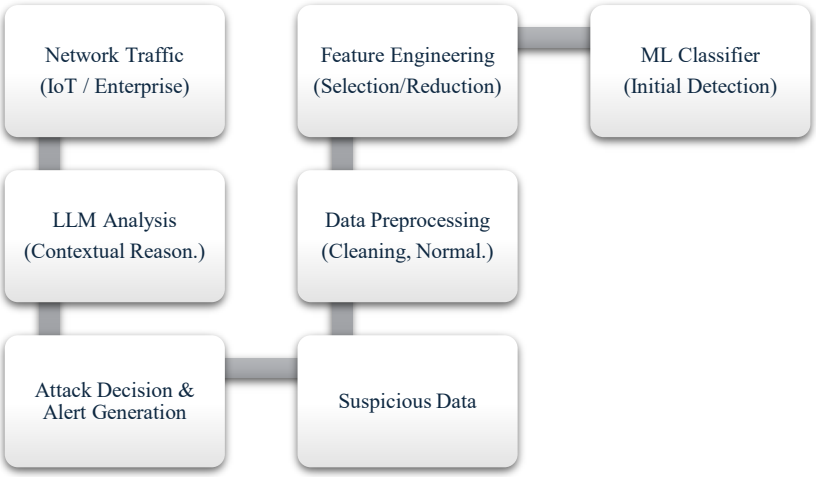

Figure 2: Proposed Framework Architecture

5. Results and Discussion

This part tells you how we tested the suggested hybrid intrusion detection system that uses ML and LLMs to find brute-force attacks. We use a number of performance measurements and graphical comparisons to look at the findings.

5.1 Performance Comparison of Models

Table 1 compares and contrasts different brute-force intrusion detection methods that use machine learning and LLM. Some of the most important measures to measure performance include the F1-score, recall, accuracy, and precision. All of the evaluation parameters show that the suggested hybrid model works better than the individual models, which proves that it works.

Table 1: Performance Comparison of Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	92.4	91.8	90.6	91.2
Random Forest	95.8	95.1	94.7	94.9
XGBoost	96.9	96.3	95.8	96.0
LLM-Based Model	95.2	94.6	95.0	94.8
Hybrid Model	98.3	97.8	97.5	97.6

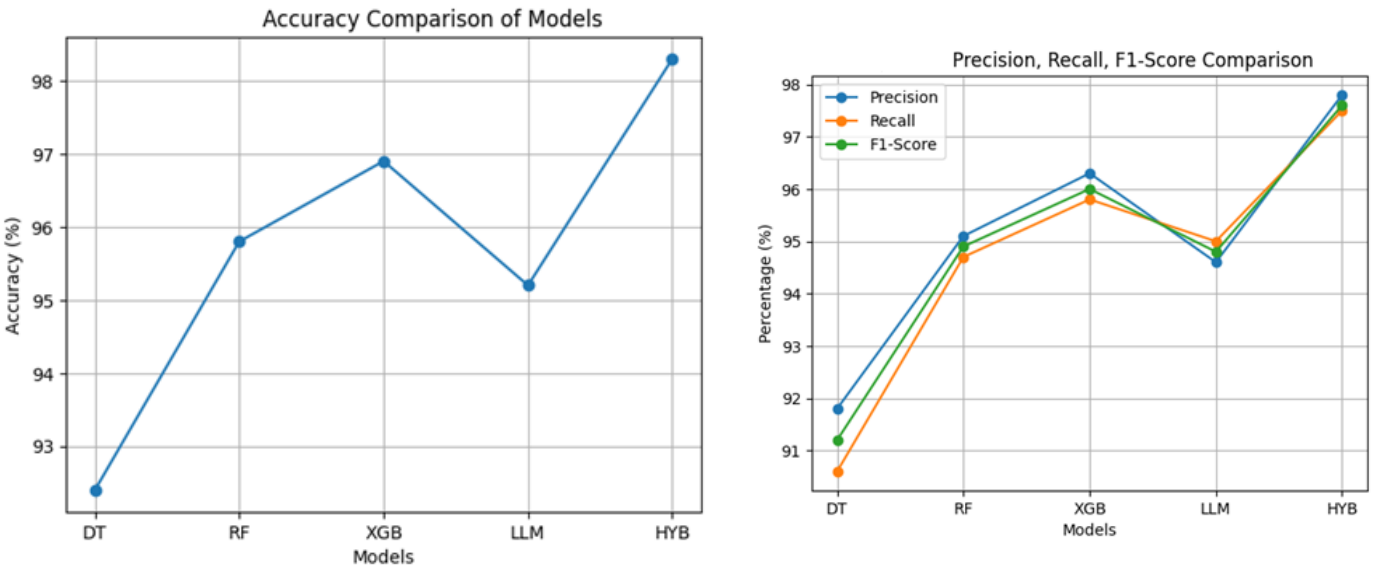

Figure 3: Performance Comparison of Models

Figure 3 demonstrates how well the models did on the tests for F1-score, recall, accuracy, and precision. The graph plainly reveals that the hybrid model is better at finding brute force attacks than the others because it always has the highest values on all measures. The hybrid method works much better than standard models like Decision Tree and Random Forest. The LLM-based model, on the other hand, offers outcomes that are competitive but not quite as good.

5.2 Confusion Matrix Analysis (Hybrid Model)

Table 2 displays the suggested hybrid model's confusion matrix, which shows how well it sorts both normal and attack events. The data reveals that the model correctly finds most examples of both normal and brute force attacks, with only a few errors. This is proof that the model can cut down on false positives and negatives.

Table 2: Confusion Matrix Analysis (Hybrid Model)

	Predicted Normal	**Predicted Attack**
Actual Normal	4820	120
Actual Attack	95	4965

5.3 False Positive and False Negative Rates

Table 3 shows how the rates of false positives and false negatives differ for different intrusion detection systems. The results reveal that the hybrid model is superior at recognizing the difference between good and bad traffic because it has the lowest error rates of all the other models. We need to cease misclassifying things if we want real-time intrusion detection systems to work better.

Table 3: False Positive and False Negative Rates

Model	False Positive Rate (%)	False Negative Rate (%)
Decision Tree	4.2	5.8
Random Forest	2.9	3.6
XGBoost	2.4	3.1
LLM Model	3.1	3.5
Hybrid Model	1.7	2.1

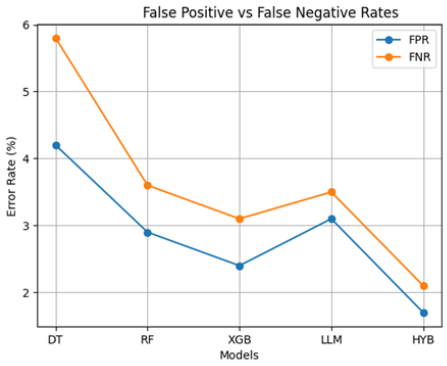

Figure 4: False Positive vs False Negative rates

Figure 4 shows how different intrusion detection methods compare to each other in terms of false positives and false negatives. The hybrid model has the fewest mistakes, which means it can discern the difference between good and negative events, as seen in the picture. On the other hand, traditional models produce more mistakes, which shows how terrible they are at discovering brute force assaults in real-time network situations. The experimental results show that the suggested hybrid framework does better than both traditional machine learning models and independent LLM-based models on all of the tests. The hybrid model is the best at finding brute force attacks because it gets 98.3% of them right. LLMs make it simpler to recall information and cut down on false positives by letting individuals comprehend the context better.

6. Future Work

There are many ways to improve things and make them bigger, even though the suggested hybrid design performs a good job of finding brute force attacks. Future research will focus on lightweight and efficient LLM architectures to enable deployment in resource-constrained situations like the IoT and edge devices by reducing computational complexity. You can improve the system by adding real-

time stream processing algorithms. This will help it handle fast network traffic better and let you detect intrusions in real time. XAI techniques should be used to help security analysts understand LLM-based judgments better and trust them more. This is a major step in the right direction. The system can be made better at finding other kinds of cyber threats, such as insider attacks, phishing, and distributed denial of service (DDoS). This makes it stronger and more adaptable. Future study may explore transfer learning and continuous learning approaches to facilitate model adaptation to changing assault patterns without requiring comprehensive retraining.

7. Conclusion

This article talks about how a hybrid intrusion detection system was made that uses machine learning and logistic regression to find brute force attacks. The research shows that standard Intrusion Detection Systems can't handle sophisticated data, changing attack patterns, and missing context information. The suggested framework makes it easier to discover bad habits and figure out what they mean. It does this by combining the semantic reasoning abilities of LLMs with the ability to quickly sort things using machine learning. This is what lets the system handle these challenges. The experimental results indicate that the hybrid model outperforms conventional machine learning and standalone LLM methods for essential performance metrics like as accuracy, precision, recall, and F1-score.

Conflict of Interest

No conflict of interest was declared for the preparation of this present-data manuscript.

Authors Contribution

Komal contributed to the conceptualization, literature review, analysis, and preparation of the original manuscript. Dr. Kumar contributed to supervision, critical review, interpretation of findings, and refinement of the manuscript. Both authors reviewed and approved the final version of the manuscript

References

1. Daniel, N., Kaiser, F. K., Giladi, S., Sharabi, S., Moyal, R., Shpolyansky, S., ... & Puzis, R. (2025). Labeling network intrusion detection system (NIDS) rules with MITRE ATT&CK techniques: Machine learning vs. large language models. *Big Data and Cognitive Computing*, *9*(2), 23.

2. AboulEla, S. G., & Kashef, R. F. (2025). Leveraging large language models, graph neural networks, and explainable AI for revolutionizing the next-generation network intrusion detection systems. *Journal of Intelligent Information Systems*, *63*(5), 1807-1835.
3. Ali, A., & Ghanem, M. C. (2025). Beyond detection: large language models and next-generation cybersecurity. *SHIFRA*, *2025*, 81-97.
4. Ma, H., Zhang, W., Zhang, D., & Chen, B. (2025). An IoT intrusion detection framework based on feature selection and large language models fine-tuning. *Scientific Reports*, *15*(1), 21158.
5. Bui, M. T., Boffa, M., Valentim, R. V., Navarro, J. M., Chen, F., Bao, X., ... & Rossi, D. (2024). A systematic comparison of large language models performance for intrusion detection. *Proceedings of the ACM on Networking*, *2*(CoNEXT4), 1-23.
6. Houssel, P. R., Singh, P., Layeghy, S., & Portmann, M. (2024, December). Towards explainable network intrusion detection using large language models. In *2024 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)* (pp. 67-72). IEEE.
7. Nwafor, E., Baskota, U., Parwez, M. S., Blackstone, J., & Olufowobi, H. (2024, December). Evaluating large language models for enhanced intrusion detection in internet of things networks. In *GLOBECOM 2024-2024 IEEE Global Communications Conference* (pp. 3358-3363). IEEE.
8. Fu, M., Wang, P., Liu, M., Zhang, Z., & Zhou, X. (2024). IoV-BERT-IDS: Hybrid network intrusion detection system in IoV using large language models. *IEEE Transactions on Vehicular Technology*, *74*(2), 1909-1921.
9. Gewida, M. H. (2024). *Leveraging Machine Learning and Large Language Model to Mitigate Smart Home IoT Password Breaches* (Doctoral dissertation, Colorado Technical University).
10. Lai, H. (2023, October). Intrusion detection technology based on large language models. In *2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT)* (pp. 1-5). IEEE.
11. Alotibi, N., & Alshammari, M. (2023). Deep learning-based intrusion detection: A novel approach for identifying brute-force attacks on FTP and SSH protocol. *International Journal of Advanced Computer Science and Applications*, *14*(6).
12. Sakaoglu, S. (2023). Kartal: Web application vulnerability hunting using large language models: Novel method for detecting logical vulnerabilities in web applications with finetuned large language models.

13. Jabed, M. M. I., Khawer, A. S., Ferdous, S., Niton, D. H., Gupta, A. B., & Hossain, M. S. (2023). Integrating Business Intelligence with AI-Driven Machine Learning for Next-Generation Intrusion Detection Systems. *International Journal of Research and Applied Innovations*, *6*(6), 9834-9849.
14. Mendonca, R. V., Silva, J. C., Rosa, R. L., Saadi, M., Rodriguez, D. Z., & Farouk, A. (2022). A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. *Expert Systems*, *39*(5), e12917.
15. Zhou, F., Du, X., Li, W., Lu, Z., & Wu, J. (2022). NIDD: an intelligent network intrusion detection model for nursing homes. *Journal of Cloud Computing*, *11*(1), 91.
16. Muthanna, M. S. A., Alkanhel, R., Muthanna, A., Rafiq, A., & Abdullah, W. A. M. (2022). Towards SDN-enabled, intelligent intrusion detection system for internet of things (IoT). *IEEe Access*, *10*, 22756-22768.
17. Awotunde, J. B., & Misra, S. (2022). Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks. In *Illumination of artificial intelligence in cybersecurity and forensics* (pp. 21-44). Cham: Springer International Publishing.
18. Setianto, F., Tsani, E., Sadiq, F., Domalis, G., Tsakalidis, D., & Kostakos, P. (2021, November). GPT-2C: A parser for honeypot logs using large pre-trained language models. In *Proceedings of the 2021 IEEE/ACM international conference on advances in social networks analysis and mining* (pp. 649-653).
19. Liang, W., Hu, Y., Zhou, X., Pan, Y., & Wang, K. I. K. (2021). Variational few-shot learning for microservice-oriented intrusion detection in distributed industrial IoT. *IEEE Transactions on Industrial Informatics*, *18*(8), 5087-5095.
20. Abdel-Basset, M., Hawash, H., Chakrabortty, R. K., & Ryan, M. J. (2021). Semi-supervised spatiotemporal deep learning for intrusions detection in IoT networks. *IEEE Internet of Things Journal*, *8*(15), 12251-12265.