JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Federated Learning-Based Privacy-Enhancing Framework for Detecting False Data Injection Attacks in Websites

Dasara Ravikishore, Manas Kumar Yogi

MTECH-Student, Assistant professor
Computer Science and Engineering,
Pragathi Engineering College, Surampalem, INDIA

Abstract : False Data Injection (FDI) attacks pose a significant threat to website security, undermining the reliability of web-based services and data integrity. These attacks exploit vulnerabilities in distributed systems to inject malicious or deceptive data, resulting in misinformation and operational disruptions. Traditional centralized detection approaches often rely on aggregating data from multiple sources, which raises privacy concerns and introduces scalability challenges. To address these issues, this paper proposes a Federated Learning (FL)-based privacy-enhancing framework for detecting FDI attacks in websites. The proposed framework leverages FL to enable collaborative model training across distributed websites without transferring raw data, thus preserving user privacy. By incorporating privacy-preserving mechanisms such as differential privacy and secure aggregation, the framework ensures data confidentiality while maintaining high detection accuracy. A tailored anomaly detection model is integrated to identify FDI attack patterns effectively. Experimental results demonstrate the framework's robustness, achieving superior detection performance compared to centralized methods while ensuring privacy preservation. Furthermore, scalability tests reveal its adaptability to varying website sizes and traffic loads. This study highlights the potential of federated approaches in enhancing cybersecurity, offering a novel pathway to safeguard websites against FDI attacks while upholding user privacy. The framework sets the stage for future advancements in secure, decentralized cybersecurity solution.

1. Introduction

I. Background and Motivation

False Data Injection (FDI) attacks have emerged as a growing threat to the cybersecurity landscape, particularly in websites and web-based applications. These attacks involve the deliberate injection of malicious or misleading data into systems, often to corrupt decision-making processes, compromise data integrity, or disrupt website functionality. In modern digital ecosystems, where websites act as central nodes for communication, commerce, and information exchange, FDI attacks undermine trust, lead to financial losses, and tarnish reputations.

The proliferation of dynamic, interactive websites that rely on user-generated data has further increased the attack surface for FDI. With applications ranging from e-commerce platforms to social networking sites, the consequences of successful FDI attacks include manipulated analytics, degraded service quality, and even propagation of misinformation. Additionally, the covert nature of FDI attacks often makes their detection challenging, as they blend seamlessly with legitimate traffic, thereby evading traditional signature-based detection mechanisms.

Traditional methods for detecting FDI attacks frequently rely on centralized approaches, where data is aggregated from multiple sources to train machine learning models. While effective in creating robust detection systems, these centralized methods come with significant drawbacks. First, they expose sensitive user data to potential breaches during data collection and processing. Second, the centralized architecture poses scalability challenges, as the volume and diversity of data from modern websites continue to grow exponentially. The inherent latency and bandwidth limitations of such systems further hinder their real-time detection capabilities.

II. In light of these challenges, there is an urgent need for innovative approaches that can detect FDI attacks while preserving user privacy and addressing scalability concerns. Federated Learning (FL) offers a promising solution by decentralizing the model training process and eliminating the need to share raw data. This paradigm shift not only enhances data privacy but also facilitates collaboration across distributed websites without centralized bottlenecks.

1.2 Federated Learning in Security Applications

Federated Learning (FL) is an emerging machine learning paradigm that enables collaborative model training without transferring raw data from individual devices or nodes. Instead, FL allows each participating entity (e.g., a website or server) to train a local model using its own data. The locally trained models' parameters are then aggregated at a central server to produce a global model, ensuring that sensitive data remains localized.

In the context of cybersecurity, FL has shown significant promise for privacy-preserving anomaly detection, fraud detection, and intrusion detection. By decentralizing data processing, FL mitigates the privacy risks associated with centralized data collection while also addressing the challenge of diverse data distributions across multiple entities. FL can effectively capture contextual variations in data, making it particularly suitable for identifying complex attack patterns like FDI.

Moreover, FL's adaptability to resource-constrained environments and its compatibility with advanced privacy-preserving techniques such as differential privacy and homomorphic encryption further enhance its suitability for cybersecurity applications. This research leverages FL's unique advantages to develop a novel framework tailored to detecting FDI attacks on websites, providing a robust balance between privacy, scalability, and accuracy.

1.3 Research Objectives

The primary objective of this research is to design and implement a Federated Learning-based framework that enhances privacy while effectively detecting False Data Injection (FDI) attacks on websites. This objective is grounded in addressing the following key goals:

1. To Develop a Privacy-Enhancing Detection System

Build a framework that leverages FL to detect FDI attacks without requiring raw data sharing among websites. The framework will incorporate privacy-preserving techniques to ensure user confidentiality and data security.

2. To Achieve High Detection Accuracy

- Develop machine learning models capable of identifying nuanced FDI attack patterns while minimizing false positives and negatives. The framework will optimize the trade-off between accuracy and computational efficiency.

3. To Ensure Scalability and Adaptability

- Design the framework to accommodate a diverse range of websites with varying traffic volumes, data distributions, and computational resources. Scalability will be tested to ensure robustness in large-scale deployments.

4. To Explore Privacy-Enhancing Techniques

- Integrate advanced techniques such as differential privacy and secure aggregation within the FL architecture to strengthen privacy guarantees while preserving detection performance.

5. To Provide Actionable Insights for Website Administrators

- Develop mechanisms to generate interpretable insights and alerts that can guide administrators in mitigating FDI attacks effectively and promptly

This paper aims to contribute to the growing body of research in privacy-preserving cybersecurity by proposing a novel solution tailored to the unique challenges of FDI attack detection.

2. Literature Review

2.1. Overview of False Data Injection Attacks

- Explain FDI attack vectors, mechanisms, and impact on website ecosystems.
- Review existing approaches for FDI detection.

2.2. Federated Learning for Cybersecurity

- Highlight applications of FL in anomaly detection, intrusion detection, and privacy-sensitive scenarios.
- Discuss gaps in current FL implementations for website security.

2.3. Privacy-Enhancing Techniques

- Survey techniques such as differential privacy, homomorphic encryption, and secure multi-party computation in FL.

3. Problem Statement and Challenges

3.1. Nature of False Data Injection Attacks

- Characteristics of FDI attacks in websites (e.g., subtlety, scalability, distributed nature).

3.2. Challenges in Detection

- Privacy concerns in centralized data collection.
- Scalability and adaptability to diverse website infrastructures.

3.3. Key Requirements

- Outline critical requirements for the proposed framework, including privacy preservation, real-time detection, and robustness.

4. Proposed Framework

4.1. Framework Overview

- High-level architecture of the FL-based privacy-enhancing framework.

4.2. Data Collection and Preprocessing

- Methods for local data collection on websites without breaching privacy.
- Preprocessing techniques for handling diverse website traffic patterns.

4.3. Federated Model Training

- Federated learning architecture, including local model updates and global aggregation.
- Privacy-preserving enhancements (e.g., encryption during communication).

4.4. FDI Attack Detection Module

- Design of a machine learning model tailored for identifying FDI attack patterns.
- Integration of anomaly detection methods.

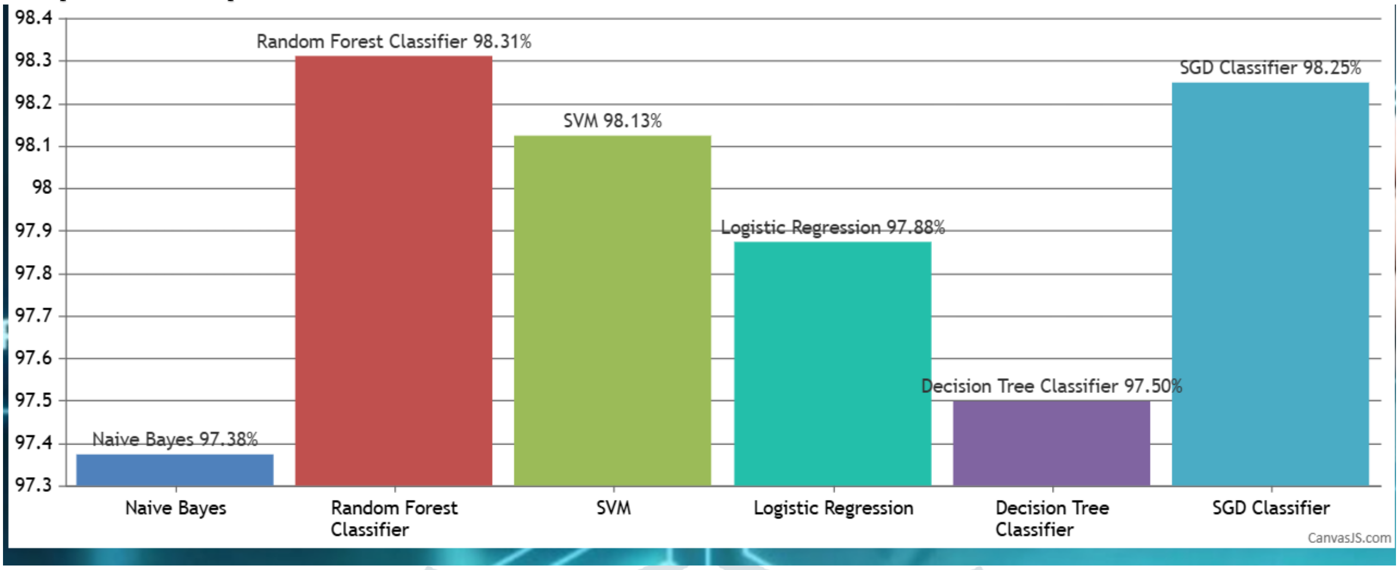
4.5. Communication Protocols

- Secure communication mechanisms between websites and the central FL server.

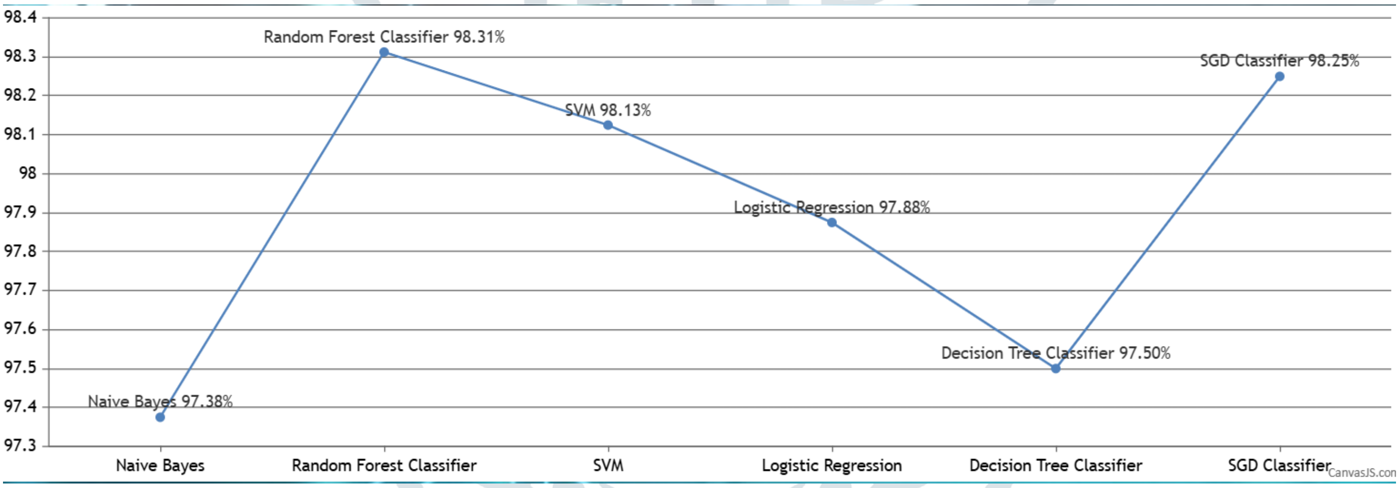
4.6. Evaluation Metrics

- Metrics for assessing detection accuracy, privacy preservation, and computational efficiency.

5. Experimental Setup and Results



[Figure01]

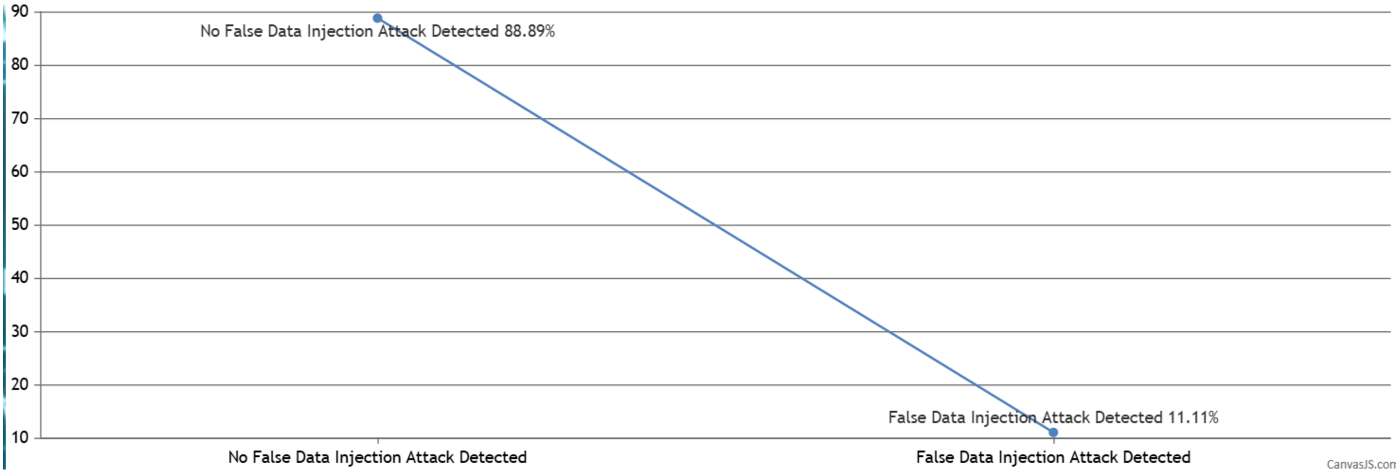


[Figure02]

View False Data Injection Attack Detection Found Ratio Details

Prediction Type	Ratio
No False Data Injection Attack Detected	88.88888888888889
False Data Injection Attack Detected	11.11111111111111

[Figure03]



[Figure04]

6. Future Directions

- Explore avenues for extending the framework, such as incorporating advanced privacy techniques or adapting to other types of attacks.

7. Conclusion

A federated learning-based privacy-enhancing framework for detecting false data injection (FDI) attacks in websites offers a promising solution for enhancing web security while preserving user privacy. By leveraging federated learning, this approach allows websites to collaboratively train machine learning models to identify malicious data injection attempts without the need to share sensitive user data, thereby maintaining privacy. The framework can be particularly beneficial in detecting and mitigating sophisticated FDI attacks, which are often subtle and challenging to detect with traditional methods.The integration of privacy-preserving techniques, such as differential privacy and secure aggregation, further strengthens the security of the system, ensuring that individual user data is not exposed during the model training process. Additionally, by enabling websites to collaborate in a decentralized manner, federated learning enhances the collective ability to detect emerging threats across multiple platforms, offering a broader and more dynamic defense against FDI attacks.While the framework holds significant potential, there are still challenges to address, such as improving model robustness against adversarial attacks, optimizing communication and computational efficiency, and ensuring model explainability and transparency. Future research in these areas will be crucial for refining the system and ensuring its scalability and applicability across diverse web environments. Overall, this federated learning-based approach to detecting FDI attacks represents a significant step forward in building secure, privacy-respecting systems that can adapt to evolving cybersecurity threats. It offers a balanced solution that aligns the goals of enhanced security, privacy preservation, and collaboration among websites to combat malicious activities in the digital space.

References

[1] Tran, Hong-Yen, et al. "An efficient privacy-enhancing cross-silo federated learning and applications for false data injection attack detection in smart grids." IEEE Transactions on Information Forensics and Security 18 (2023): 2538-2552.

[2] Mosaiyebzadeh, Fatemeh, et al. "Privacy-enhancing technologies in federated learning for the internet of healthcare things: a survey." *Electronics* 12.12 (2023): 2703.

[3] Chen, Chunlu, et al. "Trustworthy Federated Learning: Privacy, Security, and Beyond." *arXiv preprint arXiv:2411.01583* (2024).

[4] Sharma, Akash, et al. "A novel deep federated learning-based model to enhance privacy in critical infrastructure systems." *International Journal of Software Science and Computational Intelligence (IJSSCI)* 15.1 (2023): 1-23.

[5] Vyas, Abhishek, et al. "Privacy-Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey." *IEEE Access* (2024).

[6] Manzoor, Habib Ullah, et al. "A survey of security strategies in federated learning: Defending models, data, and privacy." *Future Internet* 16.10 (2024): 374.

[7] Xie, Xianghua, et al. "A survey on vulnerability of federated learning: A learning algorithm perspective." *Neurocomputing* (2024): 127225.

[8] Poorazad, Samira Kamali, Chafika Benzaid, and Tarik Taleb. "A novel buffered federated learning framework for privacy-driven anomaly detection in IIoT." *arXiv preprint arXiv:2408.08722* (2024).