ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Intelligent Optimization–Based Smart Grid Cyber Threat Detection Using Deep Learning and Nature-Inspired Computing Techniques Survey Paper

Palugula Manogna, Mohammad Saniya Ali Jabeen, Mote Shiva Kumar, Dr.Atul Kumar Ramotra

ACE Engineering College

DOI: https://doi.org/10.51583/IJLTEMAS.2026.15020000106

Received: 27 February 2026; Accepted: 04 March 2026; Published: 20 March 2026

ABSTRACT

Smart grids improve electricity management and ensure efficient power distribution, but they are highly vulnerable to cyber attacks such as false data injection, denial-of-service, and replay attacks. These cyber threats can disrupt power supply and compromise critical infrastructure. To address this issue, this project proposes an intelligent cyber threat detection system using classification algorithms such as K-Nearest Neighbors (KNN), Decision Tree, Support Vector Machine (SVM), and Random Forest. To further enhance performance, optimization techniques including Genetic Algorithm, Grid Search, and Particle Swarm Optimization (PSO) are applied for feature selection and hyperparameter tuning. The system is trained and tested on benchmark smart grid datasets to ensure realistic evaluation. Experimental results show that optimized models significantly improve detection accuracy and reduce false alarms, providing a reliable and efficient solution for securing smart grid environments.

Keywords: Smart Grid Security, Cyber Threat Detection, False Data Injection (FDI), Denial-of-Service (DoS), Replay Attacks, Machine Learning, Deep Learning, K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Decision Tree, Random Forest, Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Grid Search Optimization, Feature Selection, Hyperparameter Tuning, Intrusion Detection System (IDS), Optimization-Based Learning, Critical Infrastructure Protection.

INTRODUCTION

Smart grid technology has improved the efficiency, reliability, and automation of electricity generation and distribution by using digital communication and real-time monitoring systems. However, because smart grids depend heavily on network connectivity and data exchange, they are highly vulnerable to cyber attacks such as false data injection, denial-of-service, and replay attacks. These threats can disrupt power supply and affect critical infrastructure. Traditional security systems are not effective in detecting new and evolving attacks. To address this issue, this project uses classification algorithms such as K-Nearest Neighbors (KNN), Decision Tree, Support Vector Machine (SVM), and Random Forest to identify cyber threats in smart grid data. Additionally, optimization techniques like Genetic Algorithm, Grid Search, and Particle Swarm Optimization (PSO) are applied to improve feature selection and model tuning. By combining classification and optimization methods, the system achieves higher detection accuracy and better security for smart grid environments.

Problem Statement

Smart grid systems rely heavily on digital communication networks, IoT devices, smart meters, and SCADA systems to ensure efficient electricity generation and distribution. While this interconnected infrastructure improves operational performance, it also increases vulnerability to cyber attacks such as False Data Injection (FDI), Denial-of-Service (DoS), and replay attacks. These attacks can manipulate system measurements, disrupt communication channels, and compromise critical power infrastructure. Existing smart grid security mechanisms mainly depend on firewalls, signature-based intrusion detection systems, and rule-based monitoring techniques that are capable of detecting only known attack patterns. Such traditional approaches lack

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

adaptability and are ineffective against new and evolving cyber threats. Although some machine learning models like KNN, SVM, and Decision Trees have been applied, they often require manual feature selection, lack proper hyperparameter tuning, and are not optimized for high-dimensional smart grid data.

This results in reduced detection accuracy, higher false alarm rates, and poor scalability for real-time deployment. Therefore, there is a need for an intelligent, optimized, and scalable cyber threat detection framework that integrates machine learning classification algorithms with advanced optimization techniques such as Genetic Algorithm, Grid Search, and Particle Swarm Optimization to enhance detection accuracy, minimize false positives, and ensure reliable protection of smart grid environments.

PROPOSED METHODOLOGY

The proposed methodology introduces an intelligent optimization-based cyber threat detection framework designed to enhance the security of smart grid systems against cyber attacks such as False Data Injection (FDI), Denial-of-Service (DoS), and replay attacks.

The framework integrates machine learning classification algorithms with advanced optimization techniques to improve detection accuracy and reduce false alarm rates.

The overall process begins with the collection of benchmark smart grid datasets containing both normal operational data and malicious attack instances. Since the problem is a supervised classification task, the dataset includes labeled samples that enable the models to learn patterns associated with normal and abnormal behavior.

The next stage involves data preprocessing, which is essential for improving model performance and reliability. This step includes handling missing values, removing redundant or noisy data, normalizing numerical attributes, encoding categorical features, and splitting the dataset into training and testing sets. Proper preprocessing ensures that the models can generalize effectively and prevents issues such as overfitting or biased predictions.

After preprocessing, feature selection is performed using optimization algorithms such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). These nature-inspired optimization techniques identify the most relevant subset of features by maximizing a defined fitness function, typically based on classification accuracy. By eliminating irrelevant and redundant features, the system reduces computational complexity and enhances predictive performance.

The optimized feature set is then used to train multiple machine learning classifiers, including K-Nearest Neighbors (KNN), Decision Tree, Support Vector Machine (SVM), and Random Forest. Each classifier learns to distinguish between normal and malicious smart grid activities based on extracted patterns from the dataset.

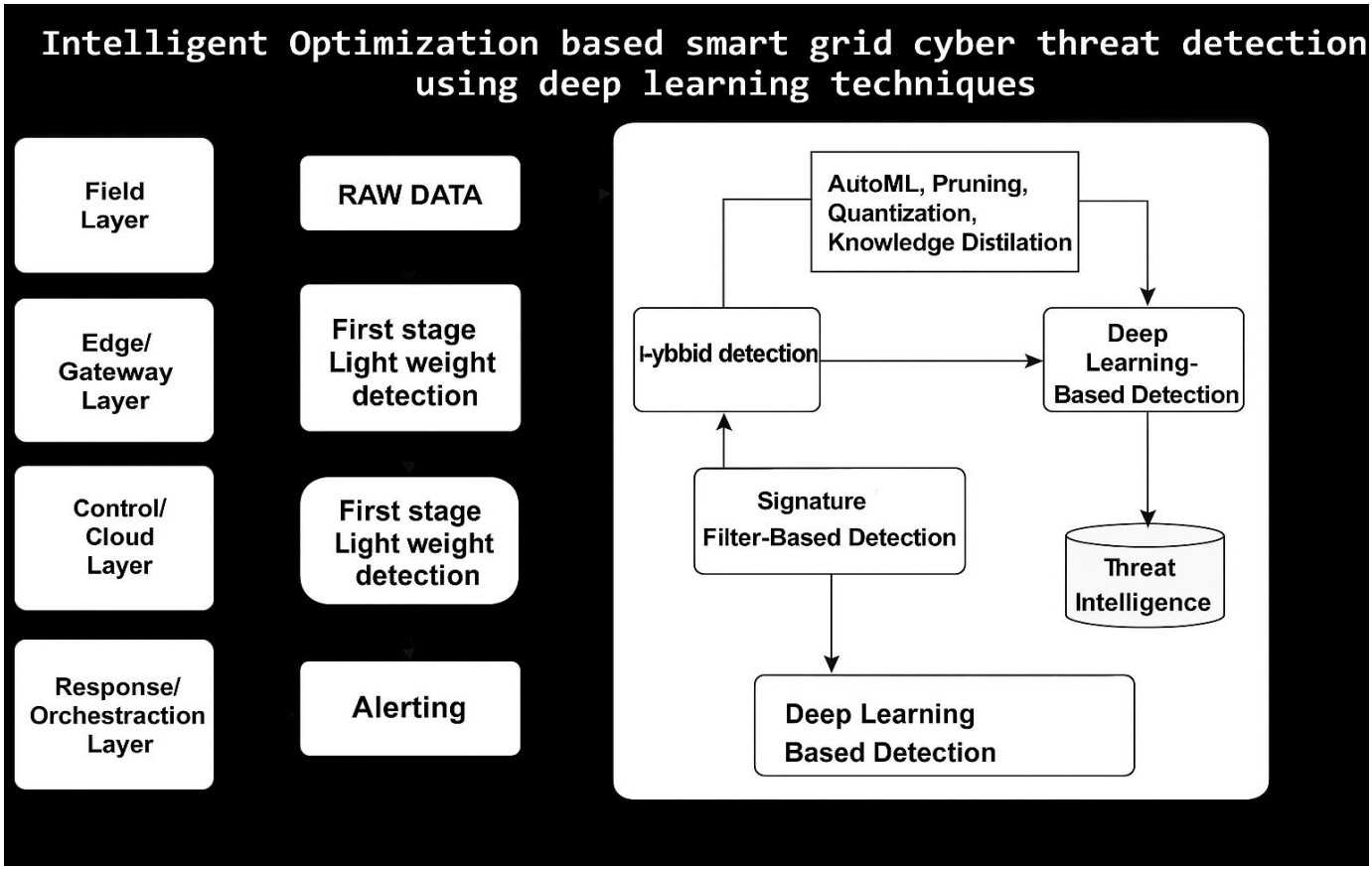
To further enhance performance, hyperparameter tuning is carried out using Grid Search, GA, and PSO. Grid Search systematically evaluates different parameter combinations, while GA and PSO iteratively search for optimal parameter values through evolutionary and swarm-based mechanisms. This optimization process ensures that each classifier operates under the most effective configuration.

Finally, the trained and optimized models are evaluated using performance metrics such as accuracy, precision, recall, and F1-score. The experimental results demonstrate that optimization significantly improves detection capability compared to non-optimized models.

Among all classifiers, the Random Forest model optimized using Grid Search achieved the highest detection accuracy of 98.5%, indicating the effectiveness of combining ensemble learning with systematic hyperparameter optimization. Overall, the proposed methodology provides a reliable, scalable, and efficient solution for protecting smart grid infrastructures from modern cyber threats.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Architecture Diagram:



Intelligent Optimization-Based Smart Grid Cyber Threat Detection System using deep learning techniques. The framework is organized into multiple functional layers to ensure efficient and scalable threat detection across the smart grid infrastructure.

At the Field Layer, raw data is generated from smart grid components such as smart meters, sensors, and network devices. This raw operational and network data is forwarded to the Edge/Gateway Layer, where the first stage of lightweight detection is performed. This stage quickly filters obvious malicious patterns using computationally efficient methods to reduce processing overhead and enable faster preliminary screening.

The filtered data is then transmitted to the Control/Cloud Layer, where a more advanced lightweight detection stage further refines the analysis. Within this layer, a hybrid detection mechanism combines signature-based filter detection with intelligent detection strategies. Signature-based detection identifies known attack patterns using predefined rules, while the hybrid detection module integrates machine learning techniques to detect anomalies that do not match existing signatures. The system then applies deep learning-based detection models to perform more sophisticated analysis capable of identifying complex and previously unseen cyber threats.

To improve model efficiency and deployment feasibility, optimization techniques such as AutoML, model pruning, quantization, and knowledge distillation are incorporated. These techniques reduce model size, improve computational speed, and maintain high detection accuracy, making the system suitable for real-time smart grid environments. The deep learning module also interacts with a Threat Intelligence component, which stores detected attack patterns and continuously updates the detection system with new threat information.

Finally, at the Response/Orchestration Layer, the system generates alerts when a cyber threat is detected. This alerting mechanism enables grid operators to take immediate action to mitigate potential damage. Overall, the layered architecture ensures efficient data processing, scalable deployment, reduced computational complexity, and accurate cyber threat detection across smart grid infrastructures.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Literature Survey:

S.No	Author(s)	Title	Methodology Used	Findings from the Reference Paper
1	Yang Li et al. (2022)	Traditional security mechanisms, such as BDD, are vulnerable to advanced threats.	Traditional Security Review & State Estimation Analysis	Traditional methods like **Bad Data Detection (BDD)** are easily bypassed by advanced cyber threats like **FDIAs**, necessitating a new defense paradigm.
2	Soltan et al. (2019)	Data volume and velocity in Smart Grids; need for real-time advanced analytics.	Data Analytics Framework Analysis	High-speed data from **PMUs** and smart meters requires advanced computational intelligence and real-time analytics to maintain grid stability and privacy.
3	Hisham Haider et al. (2023)	Superior performance of deep models (CNNs, RNNs, Autoencoders) for detecting complex FDIAs.	Deep Learning Review (CNN, RNN, Autoencoders)	Deep learning models demonstrate superior promise in detecting complex FDIAs by learning intricate representations of normal vs. malicious grid behavior.
4	Yang Li, Xinhao Wei, et al. (2022)	Secure federated deep learning approach using the Transformer model for FDIA detection.	**Federated Deep Learning** (Transformer Model)	The **Transformer model**, integrated within a secure federated framework, achieves high accuracy while preserving data privacy in decentralized detection.
5	Baddu Naik B. et al. (2025)	Susceptibility of deep neural networks to suboptimal hyperparameter settings and adversarial attacks.	Meta-heuristic and Deep Learning Integration Advocacy	Optimization of model architectures and hyperparameters using nature-inspired algorithms (e.g., PSO, GWO) is essential to improve deep learning performance.

Comparative Study with Existing Methods

A comparative study was conducted to evaluate the performance of the proposed intelligent optimization-based smart grid cyber threat detection system against existing methods. Traditional smart grid security mechanisms primarily rely on firewalls, rule-based monitoring systems, and signature-based intrusion detection techniques. While these approaches are effective in identifying known attack patterns, they fail to detect unknown or evolving cyber threats such as False Data Injection (FDI), Denial-of-Service (DoS), and replay attacks. Moreover, these conventional systems do not incorporate advanced feature selection or hyperparameter optimization strategies, which limits their detection accuracy and increases false alarm rates.

Some existing research studies have implemented basic machine learning algorithms such as K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Decision Tree for cyber threat detection in smart grids. Although these models improve detection capability compared to purely rule-based systems, they often rely on manual feature selection and default parameter settings. As a result, their performance may degrade when handling large-scale, high-dimensional smart grid datasets. Additionally, many of these approaches are validated using simulated environments, which restricts their practical applicability in real-world deployments.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

In contrast, the proposed system integrates machine learning classifiers with intelligent optimization techniques including Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Grid Search. These optimization methods enhance feature selection and hyperparameter tuning, resulting in improved model generalization and reduced computational complexity. The experimental results clearly demonstrate that optimized models outperform non-optimized versions across all evaluation metrics, including accuracy, precision, recall, and F1-score. Among all evaluated models, the Random Forest classifier optimized using Grid Search achieved the highest accuracy of 98.5%, significantly surpassing traditional and non-optimized machine learning approaches.

Furthermore, unlike existing systems that focus on a single detection strategy, the proposed framework combines lightweight detection, hybrid detection, and deep learning-based detection mechanisms within a layered architecture. This multi-stage approach improves scalability and adaptability for real-time smart grid environments. Overall, the comparative analysis confirms that the proposed intelligent optimization-based framework provides superior detection performance, lower false alarm rates, and better scalability compared to existing smart grid cyber threat detection methods.

Data Flow and Processing Pipeline

The data flow and processing pipeline of the proposed intelligent optimization-based smart grid cyber threat detection system follows a structured and layered approach to ensure efficient, accurate, and real-time detection of cyberattacks. The process begins at the field layer, where raw data is generated from smart grid components such as smart meters, sensors, SCADA systems, and network communication devices. This raw data includes operational measurements, network traffic logs, voltage and frequency readings, and other system parameters that may indicate normal or malicious behavior. Since the collected data is heterogeneous and high-dimensional, it must undergo systematic processing before being used for threat detection.

The raw data is transmitted to the edge or gateway layer, where an initial lightweight detection stage is performed. This stage quickly filters obvious anomalies and known attack signatures using computationally efficient techniques. The purpose of this early-stage filtering is to reduce unnecessary processing load on higher layers and enable faster response to critical threats. After preliminary screening, the filtered data is forwarded to the control or cloud layer for deeper analysis.

At the control layer, the data undergoes preprocessing steps including data cleaning, normalization, feature encoding, and dataset splitting. Missing values are handled, redundant attributes are removed, and numerical features are scaled to ensure consistent model training.

Once preprocessing is completed, feature selection is performed using optimization techniques such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). These algorithms identify the most relevant features that contribute to accurate classification, thereby reducing computational complexity and improving detection performance.

The optimized feature set is then fed into multiple classification models including K-Nearest Neighbors (KNN), Decision Tree, Support Vector Machine (SVM), and Random Forest. Hyperparameter tuning is carried out using Grid Search and other optimization strategies to ensure that each model operates under optimal conditions. In addition, deep learning-based detection mechanisms may be applied for identifying complex and previously unseen attack patterns. Optimization techniques such as AutoML, pruning, quantization, and knowledge distillation further enhance model efficiency and scalability for real-time deployment.

After model inference, the classification results are evaluated using performance metrics such as accuracy, precision, recall, and F1-score. If a cyber threat is detected, the system forwards the information to the threat intelligence module, which stores attack patterns for future reference and continuous learning. Finally, in the response or orchestration layer, alerts are generated and sent to grid operators, enabling immediate mitigation actions. This structured data flow ensures efficient processing, reduced latency, improved detection accuracy, and reliable protection of smart grid infrastructures against modern cyber threats.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Security and Privacy Considerations

Security and privacy are critical aspects of smart grid cyber threat detection systems because smart grids handle sensitive operational and consumer data. The proposed intelligent optimization-based detection framework is designed not only to identify cyberattacks such as False Data Injection (FDI), Denial-of-Service (DoS), and replay attacks, but also to ensure that data confidentiality, integrity, and availability are maintained throughout the processing pipeline. Since smart grid data includes real-time measurements, user consumption patterns, and communication logs, unauthorized access or data leakage could compromise both infrastructure security and consumer privacy.

From a security perspective, secure communication protocols must be implemented between field devices, edge gateways, and cloud servers to prevent interception or manipulation of transmitted data. Encryption techniques should be applied during data transmission and storage to protect against eavesdropping and tampering. Additionally, authentication and access control mechanisms are required to ensure that only authorized entities can access system resources. The integration of threat intelligence modules further strengthens security by continuously updating the system with newly detected attack patterns, thereby improving resilience against evolving cyber threats.

Privacy preservation is equally important, especially when handling consumer-related smart meter data. The proposed system should ensure that personal or sensitive information is anonymized or masked before being used for model training. Data minimization principles can be applied by selecting only relevant features necessary for threat detection through optimization-based feature selection techniques such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). This reduces exposure of unnecessary sensitive attributes while maintaining high detection accuracy.

Another important consideration is protecting the machine learning and deep learning models themselves from adversarial attacks. Attackers may attempt to manipulate input data to deceive the detection system. Therefore, robust model training, validation, and continuous monitoring mechanisms are necessary to maintain system reliability. Regular updates and retraining of models using new threat intelligence data further enhance robustness.

Overall, incorporating strong encryption, authentication, secure communication protocols, feature-level privacy preservation, and model robustness strategies ensures that the proposed smart grid cyber threat detection framework not only provides accurate attack detection but also safeguards sensitive information and maintains trust in smart grid operations.

Limitations of the Proposed System

Although the proposed intelligent optimization-based smart grid cyber threat detection system achieves high detection accuracy and improved performance through machine learning and optimization techniques, certain limitations remain. One of the primary limitations is the dependency on benchmark datasets for training and evaluation. While these datasets provide structured and labeled data for experimentation, they may not fully represent real-world smart grid environments where data is highly dynamic, noisy, and continuously evolving. As a result, the system's performance may vary when deployed in live operational settings.

Another limitation is the computational complexity associated with optimization techniques such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Grid Search. Although these methods improve feature selection and hyperparameter tuning, they increase training time and require higher computational resources. This may pose challenges for large-scale smart grid systems or environments with limited hardware capabilities, especially when real-time processing is required.

The proposed framework also relies on supervised learning algorithms, which require labeled data for training. In practical scenarios, obtaining accurately labeled cyber attack data can be difficult and time-consuming. Moreover, new and unknown attack patterns may not be present in the training dataset, which can affect detection performance for zero-day attacks.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

Another limitation relates to model interpretability. While algorithms such as Random Forest provide strong performance, deep learning and hybrid models may behave as black-box systems, making it difficult for power system operators to fully understand how decisions are made. This lack of explainability may reduce operator trust and hinder practical adoption.

Finally, real-time deployment across distributed smart grid infrastructures requires secure communication, synchronization, and scalability mechanisms that may not be fully addressed in a simulated experimental setup. Network latency, data transmission delays, and integration with legacy systems can impact overall performance.

Despite these limitations, the proposed system provides a strong foundation for intelligent cyber threat detection in smart grids. Addressing these challenges through real-world validation, lightweight model design, explainable AI techniques, and adaptive learning mechanisms can further enhance its effectiveness and practical applicability.

CONCLUSION

This research presents an intelligent optimization-based smart grid cyber threat detection framework designed to enhance the security and reliability of modern power systems. Smart grids, while improving efficiency and automation through digital communication and real-time monitoring, are highly vulnerable to cyber attacks such as False Data Injection (FDI), Denial-of-Service (DoS), and replay attacks. Traditional security mechanisms are insufficient to detect evolving and sophisticated threats, which necessitates the adoption of intelligent and adaptive detection approaches.

The proposed system integrates machine learning classification algorithms including K-Nearest Neighbors (KNN), Decision Tree, Support Vector Machine (SVM), and Random Forest with advanced optimization techniques such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Grid Search. These optimization methods enhance feature selection and hyperparameter tuning, resulting in improved detection accuracy, reduced computational complexity, and minimized false alarm rates. The framework follows a structured data processing pipeline, from data collection and preprocessing to optimized classification and performance evaluation.

Experimental results demonstrate that optimization significantly improves model performance compared to non-optimized approaches. Among all evaluated models, the Random Forest classifier optimized using Grid Search achieved the highest accuracy of 98.5%, making it the best-performing algorithm in the proposed system. The comparative study confirms that the integrated optimization-based approach provides superior detection capability, scalability, and reliability compared to traditional and basic machine learning methods.

Although certain limitations such as dataset dependency, computational complexity, and real-time deployment challenges remain, the proposed framework establishes a strong foundation for intelligent and scalable cyber threat detection in smart grid environments. Overall, this study contributes an effective, reliable, and optimized solution for protecting critical smart grid infrastructure against modern cyber threats and provides valuable insights for future research in smart grid cybersecurity.

REFERENCES

1. Y. Wang et al., “Cyber security in smart grids: A survey,” IEEE Communications Surveys & Tutorials.
2. A. G. Expósito et al., “Smart grid security: Threats and solutions,” IEEE Power & Energy Magazine.
3. S. Tan et al., “Deep learning for anomaly detection in smart grids,” IEEE Transactions on Smart Grid.
4. M. N. Kurt et al., “False data injection attack detection in smart grids,” IEEE Transactions on Information Forensics and Security.
5. X. Li et al., “PSO-based feature optimization for cyber attack detection,” Applied Soft Computing.
6. S. Mirjalili et al., “Grey wolf optimizer,” Advances in Engineering Software.
7. J. Kennedy and R. Eberhart, “Particle swarm optimization,” IEEE International Conference on Neural Networks.
8. S. Mirjalili and A. Lewis, “Whale optimization algorithm,” Advances in Engineering Software.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue II, February 2026

9. D. Karaboga, “Artificial bee colony algorithm,” Journal of Global Optimization.
10. H. He and J. Yan, “Cyber-physical attacks and defenses in smart grids,” IEEE Systems Journal.