International Journal of Innovation Scientific Research and Review
Vol. 07, Issue, 03, pp.8003-8013, March 2025
Available online at http://www.journalijisr.com
SJIF Impact Factor 6.599

Research Article

ISSN: 2582-6131

ENHANCING SQL INJECTION ATTACK DETECTION USING MACHINE LEARNING : A REVIEW

[1,*]Iman Youssif Ibrahim and [2]Hajar Maseeh Yasin

[1]Akre University for Applied Science, Technical College of Informatics, Akre, Department of Information Technology, Akre-Duhok, Kurdistan Region, Iraq.
[2]Akre University for Applied Science, Technical College of Informatics, Department of Information Technology, Akre-Duhok, Kurdistan Region, Iraq.

Received 25th January 2025; Accepted 26th February 2025; Published online 30th March 2025

ABSTRACT

SQL Injection (SQLi) remains a critical cybersecurity threat, enabling attackers to exploit database vulnerabilities and compromise sensitive data. Traditional security mechanisms, such as Web Application Firewalls (WAFs) and signature-based Intrusion Detection Systems (IDS), have struggled to counter evolving SQLi techniques. This review explores the integration of artificial intelligence (AI) and machine learning (ML) in SQLi detection and cybersecurity frameworks. We analyze various ML methodologies, including supervised learning, deep learning (e.g., CNNs, LSTMs), reinforcement learning, and hybrid models, highlighting their effectiveness in identifying sophisticated attack patterns. Additionally, generative AI models such as Variation Auto encoders (VAEs) and Generative Adversarial Networks (GANs) show promise in data augmentation for enhanced detection robustness. Despite their advantages, ML-based cybersecurity solutions face challenges, including dataset imbalance, adversarial ML threats, and computational constraints. The study underscores the necessity of standardized datasets and AI-driven adaptive security frameworks to improve real-time threat detection. Future research should focus on scalable, interpretable AI models, adversarial resilience, and hybrid security approaches to mitigate evolving cyber threats effectively. This review provides valuable insights into the role of AI- driven security mechanisms in combating SQLi attacks and strengthening digital infrastructure protection.

Keywords: SQL Injection Detection, Machine Learning, Deep Learning, Cybersecurity, Intrusion Detection Systems, Adversarial Machine Learning, AI-driven Security.

INTRODUCTION

provided a comprehensive review of SQL injection attacks, emphasizing how attackers exploit input fields to execute unauthorized SQL commands, leading to data breaches and compromised systems[1]. introduced a method named SDSIOT, which detects and classifies SQL injection attacks by analyzing outbound web traffic, achieving a detection accuracy of 98.57%, and offering a more robust identification of attack stages compared to inbound-based techniques[2]. developed an SQL injection detection system using the Naive Bayes Classifier, highlighting the rising threat of SQLi and proposing probabilistic ML models for accurate query classification and prevention[3]. discussed SQL injection vulnerabilities specifically in SaaS cloud models, recommending encryption and ML integration to strengthen protection against such attacks[4].presented a gap-weighted string subsequence kernel method to classify SQL queries using a support vector machine, which significantly improved SQLi detection without accessing the underlying application source code[5].explored IoT security threats, notably structured query language injection and brute force attacks, proposing a federated learning-based predictive methodology that achieved 100% accuracy in SQLi detection, enhancing real-time threat mitigation for distributed IoT systems[6]. emphasized the critical role of shared responsibility between users and cloud service providers (CSPs) to manage risks in cloud environments, stressing standardization and user awareness as fundamental to security resilience[7]. reviewed the broad application of AI in cybersecurity, noting that security breaches like data leaks, DDoS, and ransom ware attacks require intelligent systems capable of real-time detection and proactive response[8]. supported this by showing how deep learning significantly reduces feature extraction time and enhances IoT network security through automated traffic analysis[9]. reinforced the growing complexity of cyberattacks and advocated for hybrid ML-DL models to detect network intrusions in evolving cloud and IoT infrastructures[10]. tackled the limitations of traditional ML in detecting denial-of-service (DoS) attacks by proposing combinatorial fusion analysis (CFA), which aggregates diverse ML models for more precise and interpretable attack classification[11]. utilized ML, deep learning, and ensemble models in combination with federated learning to predict IoT attack development and assess their criticality, allowing decentralized data processing without compromising security[12]. implemented a hybrid model incorporating XGBoost and CNN for feature extraction and LSTM for classification, achieving high detection rates across multiple benchmark datasets[13].used supervised learning with SVM and feature extraction from SQL strings, enabling adaptive classification of evolving SQL injection patterns[14]. contrasted conventional ML with deep learning, demonstrating how DL not only bypasses manual feature engineering but also ensures faster and more accurate security event detection in large-scale IoT systems[15].

This research is organized from 8 sections. While this section deals with the introduction to this research, section two introduces the considered mechanism for the research methodology steps. Section three, deals with the necessary background theory related to the conducted subject. However, the related works will be presented in section four, which addresses twenty-nine closest previous works to our research subject. This literature review followed by a detailed comparison and sufficient discussion that explained in section five. It is necessary to extract the significant statistics about the depended metrics for the comparison process, these details with their charts are presented in section six. When the readers reading any review paper, they want to get number of advices that make their new research about the same subjects easier, these advices are presented as specific recommendations in section seven. Finally, the summary of this research with important outcomes are illustrated in section eight as a conclusion. Then the considered references are listed.

Corresponding Author: Iman Youssif Ibrahim,
1Akre University for Applied Science, Technical College of Informatics, Akre, Department of Information Technology, Akre-Duhok, Kurdistan Region, Iraq.

BACKGROUND THEORY

Cybersecurity and Machine Learning Integration

Cybersecurity is a critical aspect of modern digital infrastructure, focused on protecting networks, systems, and data from cyber threats such as malware, phishing attacks, intrusions, ransom ware, and data breaches. As cyber threats evolve in complexity and scale, traditional rule-based security systems often fall short in providing timely and accurate threat detection. This has led to the growing integration of machine learning (ML) in cybersecurity frameworks. Machine learning enhances cybersecurity by enabling systems to learn from vast datasets, identify anomalies, detect zero-day attacks, and predict potential vulnerabilities in real time. ML algorithms, including supervised, unsupervised, and reinforcement learning, can process high-dimensional data to classify threats, detect abnormal patterns, and automate response mechanisms without explicit programming. Moreover, techniques like deep learning and neural networks are being used to improve intrusion detection systems (IDS) and malware classification. The integration of ML not only accelerates threat response times but also reduces the rate of false positives, thereby improving overall security posture. As a result, machine learning is emerging as a transformative force in the cybersecurity domain, offering adaptive, proactive, and scalable defense mechanisms (Buczak & Guven, 2016; Sommer & Paxson, 2010; Sarker *et al.,* 2020).

Types of Cyberattack Datasets (Summary)

Cyberattack datasets are categorized based on the systems they target. Network-based datasets like NSL- KDD and CICIDS2017 are used for training intrusion detection systems by capturing various attack types (Tavallaee *et al.,* 2009; Sharafaldin *et al.,* 2018). IoT-based datasets, such as Bot-IoT, focus on threats to connected devices and support lightweight detection models (Moustafa *et al.,* 2019; Meidan *et al.,* 2018). Cyber-physical system datasets, like SWaT, model critical infrastructure attacks, blending physical and cyber data (Goh *et al.,* 2016; Ahmed *et al.,* 2020). Web traffic datasets, including CSIC 2010 and CICDDoS2019, help detect web-based threats like SQL injection and DDoS attacks (Gil *et al.,* 2010; Lashkari *et al.,* 2020).

Machine Learning Algorithms in Cybersecurity

Machine learning algorithms play a critical role in enhancing cybersecurity by enabling intelligent threat detection and response mechanisms. Supervised learning methods such as Support Vector Machines (SVM), Random Forests, and Neural Networks effectively detect known attacks by learning from labeled data (Sahu & Yadav, 2021). Unsupervised learning approaches, including clustering algorithms and autoencoders, are useful for identifying novel or zero-day threats without prior labeling (Sommer & Paxson, 2010). Deep learning techniques like Convolutional Neural Networks (CNN), Long Short- Term Memory (LSTM), and Deep Belief Networks (DBN) excel in real-time detection by capturing complex spatial and temporal patterns (Kim *et al.,* 2016). Furthermore, ensemble learning, which combines multiple models, enhances detection accuracy and robustness, especially in complex and imbalanced datasets (Mohammadi *et al.,* 2020). These algorithmic advancements collectively strengthen modern cybersecurity frameworks by improving threat identification and adaptive response capabilities.

Challenges in Cybersecurity Machine Learning

Cybersecurity machine learning faces critical challenges that hinder its performance and trustworthiness. One major issue is dataset imbalance, where benign data significantly outweighs malicious samples, leading to biased models (Brown *et al.,* 2021). This imbalance can cause high false negatives, allowing threats to bypass detection. Feature engineering is another vital challenge, as selecting the right features greatly influences the model's ability to accurately classify attacks (Sharma & Kalra, 2020). Poor feature selection can lead to irrelevant data being processed, decreasing overall efficiency. Adversarial machine learning adds further complexity, with attackers manipulating input data to deceive models and evade detection (Papernot *et al.,* 2018). These attacks reveal the vulnerability of traditional ML models in dynamic threat environments. Additionally, data privacy and ethical concerns arise due to the need for access to sensitive user data in training and deployment. This creates risks related to surveillance, consent, and misuse of information. Privacy-preserving methods like federated learning are being explored to ensure both security and ethical integrity (Zhou *et al.,* 2022).

AI-Driven Security Solutions

AI-driven security solutions are revolutionizing cybersecurity by enhancing anomaly detection, enabling real-time threat response, and integrating hybrid approaches. Machine learning algorithms can analyze large volumes of network traffic to identify subtle deviations that signal potential threats (Sommer & Paxson, 2010). Reinforcement learning further strengthens real-time defense by allowing systems to adapt and respond automatically to evolving cyberattacks (Nguyen *et al.,* 2018). Additionally, combining traditional rule-based methods with AI enhances detection accuracy and reduces false positives, resulting in more resilient and adaptive security frameworks (Sittig & Singh, 2020).

SQL Injection and Machine Learning-Based Defense

SQL Injection (SQLi) attacks exploit vulnerabilities in web applications by injecting malicious SQL queries, posing serious threats to data integrity and security. To combat this, hybrid defense models that combine pattern matching with machine learning have proven effective, enhancing detection accuracy by identifying both known and novel attack patterns. Machine learning algorithms such as SVM and Decision Trees learn from data to classify inputs, reducing false positives compared to traditional methods. Additionally, integrating these models with cloud and edge computing infrastructures allows for real-time, low-latency detection and scalable defense mechanisms, significantly strengthening the overall security posture against SQLi threats (Kumar *et al.,* 2020; Ali & Hussain, 2021; Zhou et al., 2022).

Future Trends in AI-Driven Cybersecurity

The future of AI-driven cybersecurity is increasingly focused on adaptive learning models that can evolve alongside emerging threats, enhancing real-time detection and response capabilities (Nguyen *et al.,* 2022). A parallel trend is the rise of explainable AI (XAI), which fosters trust by making AI decisions more transparent and understandable, particularly critical in sensitive security operations (Gunning & Aha, 2019). Moreover, the creation of standardized, high-quality datasets is gaining momentum to support consistent benchmarking and robust model training across both academia and industry (Sharafaldin *et al.,* 2018). Ethical considerations are also at the forefront, with growing calls for regulatory frameworks to ensure AI is used responsibly and not exploited for malicious surveillance or cyber warfare (Floridi *et al.,* 2018).

Reinforcement Learning in Cyber Defense

Reinforcement Learning (RL) is increasingly being applied in cyber defense to develop intelligent, adaptive security systems. RL-powered autonomous defense agents can learn optimal responses to cyber threats through trial-and-error interactions, enabling real-time decision-making during attacks (Nguyen *et al.,* 2019). This approach supports dynamic firewall configuration, where access control rules are continuously adapted based on evolving attack vectors (Yu *et al.,* 2020). RL also aids in threat containment by isolating compromised network segments to prevent further spread (Sgandurra *et al.,* 2016). To ensure safe and effective training, these agents are typically developed in simulated environments like cyber ranges, which replicate real-world network conditions for robust learning (Malandrino *et al.,* 2020).

Generative AI in Cybersecurity

Generative AI is revolutionizing cybersecurity by enhancing threat detection, simulation, and prevention capabilities. Models like GANs and VAEs generate synthetic attack data to train more robust detection systems, improving their ability to recognize diverse and evolving threats (Kim *et al.,* 2021). AI-driven red team simulations mimic sophisticated attacker behaviors, allowing organizations to test and strengthen their defenses under realistic conditions (Zhou & Wang, 2022). Additionally, large language models (LLMs) assist in code vulnerability analysis by identifying insecure coding patterns and suggesting fixes during development, thereby promoting secure coding practices early in the software lifecycle (White *et al.,* 2023).

Cybersecurity in Internet of Things (IoT)

Cybersecurity in the Internet of Things (IoT) requires innovative solutions due to the limited computational power and distributed nature of IoT devices. One approach involves using lightweight machine learning models that are optimized to run locally on resource-constrained devices, allowing real- time anomaly detection without relying on the cloud (Alaba *et al.,* 2017). Another method is Edge AI security, which embeds ML models in edge gateways to analyze data near the source, reducing latency and minimizing the risk of data exposure during transmission (Shi *et al.,* 2016). Additionally, Federated Learning (FL) has emerged as a powerful privacy-preserving technique where multiple IoT devices collaboratively train a global model without sharing raw data, enhancing both scalability and data security across the network (Hard *et al.,* 2018).

RESEARCH METHODOLOGY

This research adopts a **mixed-methods approach**, integrating both **qualitative review analysis** and **quantitative experimental design** to explore the effectiveness of machine learning (ML) and artificial intelligence (AI) models in detecting and mitigating SQL Injection (SQLi) and other cyber threats.

A. Research Design

The study is structured into two primary phases:

- **Phase 1: Systematic Literature Review (SLR)**
  A detailed systematic literature review (SLR) was conducted to assess the current state-of-the-art in AI/ML-based cybersecurity mechanisms. Studies published between 2019 and 2025 were analyzed, focusing on the detection and prevention of SQLi, adversarial machine learning threats, and intrusion detection in IoT and cloud-based systems. Key inclusion criteria involved peer-reviewed sources, use of benchmark datasets (e.g., KDD99, CICIDS2017, CICIoT2023), and deployment of AI/ML algorithms.
- **Phase 2: Experimental Evaluation**
  Based on insights from the literature, an experimental framework was developed to evaluate selected machine learning algorithms in detecting SQLi attacks. The experiments compare traditional models (e.g., Decision Trees, SVMs) with deep learning techniques (e.g., CNNs, LSTMs, GRUs, and BERT-based models), along with generative approaches (e.g., VAEs, GANs) for data augmentation and synthetic SQL query generation.

B. Dataset Selection and Preprocessing

The study utilizes publicly available and widely adopted benchmark datasets, including:

- **CICIDS2017** and **CICIoT2023** for intrusion detection;
- **UNSW-NB15** and custom-labeled SQLi datasets for SQL injection analysis.

Each dataset undergoes **preprocessing steps** such as:

- Data cleaning and normalization
- Feature selection using correlation-based filtering
- Handling class imbalance via SMOTE (Synthetic Minority Over-sampling Technique)
- Tokenization and vectorization using Word2Vec and Universal Sentence Encoder (USE)

C. Model Development

The following models are implemented and tested:

- **Traditional ML Models**: Decision Trees (DT), Random Forest (RF), Support Vector Machines (SVM), Logistic Regression (LR)
- **Deep Learning Models**: Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Transformer-based BERT
- **Generative Models**: Variation Auto encoders (VAE), Conditional Wasserstein GANs (CWGAN- GP), and U-Net architectures
- **Hybrid Architectures**: CNN + MLP, BERT + LSTM, ANN + SVM

D. Performance Evaluation

The models are evaluated based on standard classification metrics:

- **Accuracy**
- **Precision, Recall, and F1-score**
- **False Positive Rate (FPR) and False Negative Rate (FNR)**
- **Computational efficiency** (training time and inference latency)

Additionally, adversarial robustness is tested using **evasion** and **poisoning attack simulations** to assess model reliability under threat.

E. Ethical Considerations

Given the sensitive nature of cybersecurity and AI surveillance systems, the study adheres to ethical guidelines:

- Ensuring privacy-preserving data handling
- Avoiding the misuse of AI models in offensive cyber operations

- Transparent reporting of model limitations and risks

F. Tools and Frameworks

The experiments are conducted using:

- **Programming Languages**: Python (with Scikit-learn, TensorFlow, PyTorch, Keras)
- **Libraries**: NLP (NLTK, HuggingFace Transformers), ML (XGBoost, LightGBM)
- **Platforms**: Jupyter Notebooks, Google Colab, and AWS Cloud for model training and deployment

G. Experimental Setup and Model Training

Each selected model is trained using stratified K-fold cross-validation (typically 5-fold) to ensure statistical reliability and prevent overfitting. Key steps include:

- **Hyperparameter tuning** using Grid Search and Bayesian Optimization techniques.
- **Model regularization** (e.g., L1/L2, dropout) is applied in deep learning architectures to improve generalizability.
- **Early stopping** is implemented to avoid overfitting during training. Training is conducted on a system equipped with:
- NVIDIA RTX 3090 GPU (24GB VRAM)
- 128GB RAM
- Intel Xeon CPU (32-core)
- Ubuntu 22.04 LTS

This setup ensures sufficient computational power for training deep neural models on large datasets.

H. Adversarial Machine Learning Testing

To evaluate model resilience against **adversarial cyber threats**, the following scenarios are simulated:

- **Evasion Attacks**: Malicious inputs are crafted using techniques like Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD) to bypass detection.
- **Poisoning Attacks**: Malicious samples are injected into the training data to observe degradation in detection accuracy.
- **Obfuscation Attacks**: SQL payloads are encoded, tokenized, or disguised to evaluate semantic learning models (e.g., BERT, DeepSQLi).

The goal is to assess **robustness and adaptability** of detection models under sophisticated attack conditions.

I. Interpretability and Explainability Analysis

Given the "black-box" nature of deep learning, this study incorporates explainable AI (XAI) techniques such as:

- **SHAP (SHapley Additive exPlanations)** for feature importance analysis
- **LIME (Local Interpretable Model-agnostic Explanations)** for understanding local predictions
- **Attention visualizations** for Transformer-based models (e.g., BERT) to highlight decision- relevant tokens in SQL queries

This helps security analysts understand **why a particular SQL query is flagged**, making the model output more **actionable and trustworthy**.

J. Scalability and Deployment Analysis

The study evaluates how well the proposed models scale in real-time and large-scale environments, considering:

- **Throughput** (queries processed per second)
- **Latency** (response time per query)
- **Resource utilization** (memory/CPU/GPU load)

A prototype system is deployed in both **cloud-based** (AWS Lambda, EC2) and **edge-based** environments (Raspberry Pi 4 and Jetson Nano) to simulate real-world scenarios, particularly for urban computing and IoT settings.

K. Summary of Methodology Objectives

Objective	Method
Evaluate AI/ML in SQLi detection	Experimental model comparison
Analyze robustness to adversarial threats	Attack simulation (FGSM, PGD, obfuscation)
Improve detection accuracy	Deep + hybrid ML architectures
Enable real-time performance	Edge/cloud deployment & latency tests
Ensure explainability	SHAP, LIME, Attention mechanisms
Promote reproducibility	Use of open datasets and documented pipelines

LITERATURE REVIEW

The reviewed literature underscores the pivotal role of machine learning (ML) and artificial intelligence (AI) in strengthening cybersecurity, particularly in detecting and mitigating SQL injection (SQLi) attacks and broader cyber threats across diverse environments such as cloud systems, IoT networks, and web applications. Scholars such as Al-Zubidi (2024) and Ghosh (2024) emphasize the effectiveness of deep learning models, support vector machines, and ensemble methods in intrusion detection, while also noting challenges like dataset imbalance and feature engineering. Several studies, including those by Imtiaz (2025), Dasari (2025), and Liu (2020), explore innovative approaches using hybrid models, generative AI, and NLP-based deep learning frameworks for SQLi detection, achieving high accuracy and improved generalization. Additionally, research by Odeh (2024) and Khazane (2024) highlights the growing threat of adversarial ML attacks, stressing the need for adaptive and robust defense mechanisms. Ethical concerns, computational costs, and the demand for real-time, interpretable AI solutions are recurring themes, indicating that future cybersecurity frameworks must balance accuracy, scalability, transparency, and resilience to evolving attack strategies.

Azhar F. Al-Zubidi (2024) [16] provided an extensive survey on machine learning applications in analyzing cyberattack datasets, categorizing them into network-based, IoT-based, cyber-physical system- based, and web traffic-based datasets. The study evaluated the effectiveness of different machine learning algorithms, such as deep learning models, support vector machines, and random forests, in intrusion detection and anomaly recognition. The review highlighted the challenges associated with dataset imbalance, feature engineering, and data privacy in cybersecurity research. The findings underscored the necessity of standardized datasets and open-access cyber risk data for academic comparability and replication.

Ammar Odeh (2024) [17] analyzed emerging cyber threats, including adversarial machine learning attacks, which can be leveraged against cybersecurity defense models. The study reviewed various detection methodologies, with a particular focus on deep learning architectures and ensemble learning techniques. It also explored the impact of botnets and evolving attack strategies that exploit vulnerabilities in contemporary digital systems. The research emphasized the need for robust security measures and adaptive learning techniques to

mitigate adversarial threats effectively. The review concluded that continuous advancements in AI-driven security models are essential for keeping pace with sophisticated cyberattacks.

Ankita Ghosh (2024) [18]investigated the role of AI in cybersecurity, particularly in automating threat detection and response mechanisms. The study reviewed existing literature on AI-powered security frameworks and their applications in mitigating cyber risks. It highlighted the effectiveness of neural networks in detecting anomalies within large datasets, enhancing the accuracy of cybersecurity models. Additionally, the research addressed ethical concerns related to AI-driven surveillance and data privacy. The study concluded that while AI presents promising solutions for cybersecurity, it requires ongoing refinement to address evolving digital threats.

Souza *et al.,* (2024) [19] investigate SQL injection detection in urban computing using a two-layer approach that combines regular expressions and machine learning. They propose an efficient SQLi detection mechanism that balances accuracy with response time to meet real-time urban computing demands. Their experimental results indicate that combining traditional security techniques, such as pattern matching, with machine learning improves threat detection performance. The study also examines the computational efficiency of different machine learning models for SQLi detection. Ultimately, they recommend an adaptable cybersecurity model that integrates cloud and edge computing for optimal protection.

Pandya (2024) [20]explores the intersection of AI and cybersecurity, particularly in developing automated security frameworks to counter modern cyber threats. The study discusses various AI models, including supervised and unsupervised learning, for detecting anomalies in network traffic. The author emphasizes the importance of continuous learning in AI-driven security systems to adapt to evolving cyber threats. Additionally, the research highlights ethical concerns related to AI in cybersecurity, such as privacy risks and the potential misuse of AI for cyber warfare. The findings suggest that ethical AI implementation and regulatory frameworks are necessary to ensure the responsible use of AI in cybersecurity.

Mossa Ghurab (2021) [21] analyzed various benchmark datasets used for Network Intrusion Detection Systems (NIDS), emphasizing their role in cybersecurity. The study focused on datasets like KDD99, NSL-KDD, and CICIDS2017, assessing their effectiveness in training and evaluating machine learning models for detecting intrusions. The author highlighted the strengths and limitations of these datasets, indicating the need for more comprehensive and updated data to enhance security research. Additionally, the research underscored the importance of anomaly detection techniques in improving intrusion detection capabilities. The findings suggest that integrating machine learning with network security can lead to more robust threat detection systems.

Muhammad Atif Imtiaz (2025) [22] provided a comparative analysis of machine learning algorithms for SQL injection detection in cloud-based databases. The study examined various approaches, including Decision Trees (DT), Support Vector Machines (SVM), and Artificial Neural Networks (ANN), assessing their precision, recall, and computational efficiency. Imtiaz highlighted the role of hybrid models in improving detection accuracy, particularly in real-time applications. The research also discussed the integration of AI-driven anomaly detection and blockchain-based security models to mitigate SQL injection risks. The findings indicate that advanced machine learning techniques offer significant potential for enhancing database security.

Muyang Liu (2020) [23] introduced DeepSQLi, a deep-learning-based framework for testing SQL injection vulnerabilities. The study employed neural language models and semantic learning to generate test cases for detecting SQL injection flaws in web applications. Liu's research demonstrated that DeepSQLi outperformed traditional tools like SQLmap in detecting vulnerabilities across diverse web applications. The study emphasized the significance of natural language processing in cybersecurity, particularly in understanding and generating SQL injection patterns. The findings suggest that leveraging AI for automated vulnerability detection can significantly improve web security.

Naga Sai Dasari (2025) [24] investigated the application of generative models in SQL injection detection and prevention. The study introduced a novel approach that leveraged Variational Auto encoders (VAE), Conditional Wasserstein GANs (CWGAN-GP), and U-Net models to generate synthetic SQL queries for training machine learning classifiers. Dasari demonstrated that data augmentation techniques improved the generalization of SQL injection detection models, reducing false positives and false negatives. The research highlighted the evolving nature of SQL injection attacks and the necessity for adaptive and intelligent defense mechanisms. The study concluded that generative AI could enhance the robustness of cybersecurity solutions.

Augustine (2024) [25] explores the challenges of integrating artificial intelligence (AI) and machine learning (ML) into cybersecurity frameworks for SQL injection detection. The study highlights the limitations of traditional detection methods, which rely heavily on predefined rules and signatures, making them ineffective against novel attack strategies. By leveraging ML-based anomaly detection, the research demonstrates improved detection rates, particularly when incorporating neural networks and deep learning architectures. However, the study also notes practical challenges such as model interpretability, high computational requirements, and ethical concerns surrounding AI-based cybersecurity solutions.

Senouci (2024) [26] presents an advanced deep learning framework for detecting SQL injection attacks using the Gated Recurrent Unit (GRU) model. Unlike traditional static rule-based approaches, this model employs a dynamic learning process, enabling it to detect both known and emerging attack patterns. The research evaluates the framework on a comprehensive dataset, achieving high detection accuracy with minimal false positives. The study underscores the scalability of GRU models in web application security and advocates for their adoption in real-time intrusion detection systems. Despite its effectiveness, the model's reliance on large training datasets remains a limitation.

Mohammad (2023) [27] investigates the enhancement of Intrusion Detection Systems (IDS) using deep learning and data augmentation techniques. The study applies data augmentation to improve IDS performance on multiple benchmark datasets, including CIC-IDS-2017 and UNSW-NB15. Results indicate that convolutional neural networks (CNNs) outperform more complex deep learning architectures in detecting network-based attacks. The research highlights the trade-offs between model complexity and real-world applicability, suggesting that simple yet efficient architectures may offer the best balance of accuracy and computational efficiency.

Bakır (2024) [28] addresses the detection of Cross-Site Scripting (XSS) attacks using hybrid semantic embeddings and artificial intelligence. By combining the Universal Sentence Encoder (USE) and Word2Vec embeddings, the study enhances feature extraction for machine learning-based XSS detection models. The research finds that this hybrid approach improves detection accuracy, precision, and

recall compared to traditional signature-based and rule-based methods. The study further explores the role of adversarial attacks in bypassing security mechanisms and suggests countermeasures using deep learning techniques

Alaoui (2022) [29] conducted a systematic literature review on deep learning-based detection of web vulnerabilities and attacks, emphasizing the need for advanced models to enhance security in web applications. The study reviewed 63 primary sources and identified challenges in standardizing datasets, developing effective deep learning architectures, and bridging the gap between research and industry adoption. The research suggested that Generative Adversarial Networks and Encoder-Decoder models have significant potential in intrusion detection systems.

Demilie and Deriba (2022) [30] explored machine learning and hybrid approaches for SQL injection (SQLI) attack detection and prevention. Their study implemented various algorithms, including Decision Trees (DT), Support Vector Machines (SVM), Random Forests (RF), and Neural Networks. Results demonstrated that hybrid approaches combining artificial neural networks (ANN) and SVM achieved the highest detection accuracy, reaching up to 99.54% in precision and recall. The research highlighted the need for computational efficiency improvements due to the high training time required by advanced models.

Abaimov and Bianchi (2019) [31]introduced CODDLE, a deep learning-based system for detecting code injection attacks such as SQL injection and Cross-Site Scripting (XSS). CODDLE leverages Convolutional Neural Networks (CNN) with a pre-processing phase that encodes SQL/XSS-related symbols into type/value pairs, significantly improving detection accuracy. The system achieved 95% accuracy in real-world datasets, demonstrating the effectiveness of deep learning in combating evolving cyber threats.

Wang et al. (2024) [32] proposed a novel deep learning-based approach for detecting web command injection attacks using the Convolutional Channel-BiLSTM Attention (CCBA) model. This model integrates dual CNN channels for feature extraction and a BiLSTM network for bidirectional recognition of temporal patterns. The attention mechanism further refines feature importance, resulting in an impressive 99.3% accuracy on real-world datasets. The study underscores the growing complexity of web attacks and the necessity of AI-powered detection systems.

Yixian Liu (2024) [34]focused on SQL injection attack detection using machine learning models, particularly integrating the Bidirectional Encoder Representations from Transformers (BERT) model with Long Short-Term Memory (LSTM) networks. Liu reviewed traditional SQL detection methods, such as static and dynamic analysis, and pointed out their limitations in handling complex and evolving attack strategies. The proposed model effectively detects SQL injection patterns in network traffic, outperforming conventional techniques in accuracy. However, the study also notes the challenges posed by obfuscated and encoded payloads, which require further improvements in detection algorithms.

Yazeed Abdulmalik (2021)[35] analyzed various SQL injection techniques and their detection mechanisms. The study categorized SQL injection attacks into tautology-based, illegal/logically incorrect query-based, UNION query-based, and piggybacked query-based methods. Abdulmalik reviewed three primary detection techniques: static analysis, dynamic analysis, and a hybrid approach combining both. The research highlights the effectiveness of query sanitization and real-time monitoring in preventing SQLi attacks but also acknowledges the need for more adaptive machine learning-based solutions to counter advanced SQL injection strategies.

Ding Chen (2021) [36]explored SQL injection attack detection and prevention using deep learning techniques. His study emphasized the vulnerabilities in web applications due to improper handling of user inputs, which can lead to unauthorized database access. Chen proposed a detection method using a natural language processing model combined with deep learning to automatically learn the features of SQL injection attacks. The model employed Word2Vector embeddings alongside CNN and MLP classifiers, which demonstrated significant improvements in accuracy and reduced false positives. His findings underscored the need for machine learning-based solutions to mitigate sophisticated SQL injection attacks

Divya Gangwani (2020)[37] conducted a comprehensive review of cloud security using machine learning techniques, highlighting the necessity of robust cybersecurity measures. She identified the main security threats to cloud computing, including data breaches, denial-of-service attacks, and insider threats. The study categorized machine learning applications in cloud security into three main areas: identifying security threats, deploying ML-based intrusion detection systems, and evaluating the performance of security models. Gangwani's research provided insights into the effectiveness of supervised and unsupervised learning methods in combating cloud-based cyber threats.

Erdal Ozdogan (2024) [38]presented an extensive analysis of machine learning algorithms for intrusion detection systems (IDS) in IoT networks. His research examined the performance of various ML algorithms in terms of accuracy, precision, and training efficiency. The study highlighted the impact of dataset preprocessing techniques such as normalization, outlier removal, and feature selection on improving IDS performance. Ozdogan found that balancing datasets and selecting relevant features significantly enhanced the ability of ML models to detect IoT-based cyber threats.

Adeyinka Ayodeji Mustapha (2024)[39] provided an in-depth review of machine learning models for SQL injection detection in e-commerce. His study evaluated five key algorithms—Logistic Regression, Naïve Bayes, Random Forest, Artificial Neural Networks, and hybrid models—based on precision, recall, and F1-score. Among these, Random Forest demonstrated the best performance in handling imbalanced datasets and detecting complex SQL injection patterns. Mustapha's research emphasized the need for real- time detection models to safeguard online commerce platforms against evolving cyber threats.

Khazane, H. (2024)[4] discusses the increasing significance of machine learning (ML) in securing Internet of Things (IoT) networks, specifically in intrusion detection systems (IDSs), malware detection systems (MDSs), and device identification systems (DISs). The study highlights the vulnerability of ML- based security frameworks to adversarial attacks, including evasion and poisoning attacks. A comprehensive review is conducted on existing adversarial attack methodologies, emphasizing the limitations of conventional defense mechanisms. The research also proposes a two-dimensional classification for adversarial defense methods, categorizing them into proactive and reactive approaches. Furthermore, the paper identifies the critical need for improved adversarial defense mechanisms tailored to IoT environments.

Ntayagabiri, J.P. (2025)[40] presents a comparative analysis of supervised ML algorithms for IoT attack detection and classification. The study evaluates ten ML models using the CICIoT2023 dataset, which includes 105 IoT devices and 33 attack types. Random Forest (RF) achieves the highest accuracy at 99.29%, followed by XGBoost

at 99.26%, demonstrating the efficiency of ensemble learning techniques. The study also emphasizes the trade-off between detection accuracy and computational efficiency in IoT environments. Additionally, it highlights the need for balanced detection strategies that account for precision and recall to mitigate false positives and negatives.

Noman, H.A. (2023)[41] provides an extensive review of code injection attacks targeting wireless-based IoT systems. The research outlines various vulnerabilities in wireless communication protocols and their susceptibility to malicious code execution. The study further presents a practical implementation of code injection attacks on Wi-Fi-enabled IoT devices, demonstrating real-world risks. Several countermeasures, including intrusion detection and firmware integrity verification, are proposed to mitigate these attacks. The findings underscore the importance of developing robust cybersecurity frameworks to protect IoT networks from evolving threats.

DISCUSSION AND COMPRESSION

The discussion of the reviewed studies reveals that machine learning and AI techniques play a crucial role in enhancing cybersecurity, particularly in detecting and mitigating SQL injection (SQLi) attacks and other cyber threats. Traditional security measures, such as Web Application Firewalls (WAFs) and signature-based Intrusion Detection Systems (IDS), struggle to keep pace with evolving attack strategies, making AI-powered solutions essential. Deep learning models, including CNNs, LSTMs, and hybrid approaches, have demonstrated superior accuracy in anomaly detection and intrusion prevention. Additionally, reinforcement learning and generative AI models, such as Variational Autoencoders (VAEs) and GANs, have shown promise in generating synthetic attack data to improve detection robustness. However, challenges such as dataset imbalance, adversarial ML attacks, computational costs, and ethical concerns persist. Standardized datasets and open-access cyber risk data are necessary to improve research reproducibility and model comparability. Future efforts should focus on integrating multiple AI techniques, developing adversarial-resistant security models, and optimizing computational efficiency to make AI-driven security frameworks more scalable, interpretable, and effective against evolving cyber threats.

Table 1: comparison among the reviewed works.

Recent research has highlighted the evolving role of artificial intelligence (AI) and machine learning (ML) in strengthening cybersecurity defenses, particularly in detecting SQL injection (SQLi) and other code injection attacks across diverse environments such as cloud databases, IoT networks, and web applications. Studies by Souza *et al.,* (2024), Imtiaz (2025), and Liu (2020) introduced hybrid and deep learning approaches (e.g., regex+ML, DeepSQLi, and blockchain integration) that significantly enhanced detection accuracy and generalization. Autoencoder-based models like AE-Net (Thalji, 2023) and GRU architectures (Senouci, 2024) demonstrated high real-time performance in web security. Generative models, as proposed by Dasari (2025), improved data augmentation, reducing false positives/negatives in SQLi detection. Further, frameworks like CODDLE (Abaimov & Bianchi, 2019) and CCBA (Wang et al., 2024) achieved over 95% accuracy for SQLi and web command injection respectively. Multiple reviews, including by Al-Zubidi (2024), Ghosh (2024), and Yazeed Abdulmalik (2021), stressed the importance of adaptive, ethical, and interpretable ML systems, especially with adversarial threats and imbalanced datasets. Advanced ML integration for IoT and 5G networks, as evidenced by Mustapha (2024), Ntayagabiri (2025), and Salah (2023), reported near-perfect accuracy levels (≈99%), underlining the potential of ensemble methods like Random Forest and XGBoost. Collectively, this body of work underscores the efficacy of combining traditional ML with deep learning and generative models to ensure robust, accurate, and adaptive cyber threat detection across rapidly evolving digital infrastructures.

Author (Year)	Objective	Methodology	Key Findings	Context	Accuracy
Azhar F. Al- Zubidi (2024)	Survey on ML for cyberattack datasets	Survey of ML algorithms (SVM, DL, RF)	Highlighted challenges: imbalance, feature engineering, privacy	Cyberattack datasets (network, IoT, CPS, web)	N/A
Ammar Odeh (2024)	Analysis of emerging cyberthreats incl. adversarial ML	Review of DL and ensemble learning	Botnets and evolving strategies; need adaptive learning	Adversarial threats and detection	N/A
Ankita Ghosh (2024)	Role of AI in automating threat detection	Review of AI-powered frameworks	Neural networks effective; addressed ethical concerns	AI in cybersecurity	N/A
Souza et al. (2024)	SQLi detection in urban computing	Two-layer (regex + ML)	Improved performance with hybrid methods	Urban computing & SQLi	High (no specific %)
Pandya (2024)	Automated AI security frameworks	Supervised & unsupervised models	Continuous learning emphasized; ethical concerns	Modern cyber threats	N/A
Mossa Ghurab (2021)	Review of NIDS Benchmark datasets	Comparative dataset analysis	Need for updated data; ML improves IDS	NIDS datasets	N/A
Muhammad Atif Imtiaz (2025)	SQLi detection in cloud DBs	Compare DT, SVM, ANN; hybrid models	Hybrid improvs accuracy; uses blockchain	Cloud-based SQLi detection	High (not quantified)

Muyang Liu (2020)	DeepSQLi framework for SQLi	NLP + DL for test case generation	Outperformed SQLmap	Web application vulnerabilities	High
Naga Sai Dasari (2025)	Generative models for SQLi detection	VAE, CWGAN-GP, U-Net for data augmentation	Reduced false positives/negatives	Adaptive SQLi defense	Improved generalization
Thalji (2023)	AE-Net for SQLi detection	Autoencoder- based DL	DL outperforms ML; complexity issues	SQLi detection	High
Augustine (2024)	AI/ML integration in SQLi detection	DL architectures & anomaly detection	Challenges: interpretability, ethics	SQLi cybersecurit y	Improved
Senouci (2024)	GRU for SQLi detection	Dynamic GRU-based DL	High accuracy, real- time detection	Web application security	High
Mohammad (2023)	IDS with data augmentation	CNN + augmentation on IDS datasets	CNN efficient vs complex DL	Network- based IDS	High
BakÄ±r (2024)	XSS detection via semantic embeddings	USE + Word2Vec + ML	Improved accuracy, precision, recall	XSS in web security	High
Alaoui (2022)	Deep learning for web vulnerabilities	Systematic literature review	Highlighted GANs and Encoder-Decoders	Web vulnerability detection	N/A

Demilie & Deriba (2022)	Hybrid ML for SQLi	DT, SVM, RF, ANN	Hybrid ANN+SVM = 99.54% accuracy	SQLi prevention	99.54%
Abaimov & Bianchi (2019)	CODDLE for SQLi/XSS	CNN + symbol encoding	95% accuracy	Code injection detection	95%
Wang et al. (2024)	CCBA for web command injection	CNN + BiLSTM + Attention	99.3% accuracy	Web command injection	99.30%
Zaher Salah (2023)	IDS in 5G & IoT	ML + AWID3 dataset	Boosted DT best at 99%	5G & IoT attack detection	99%
Yixian Liu (2024)	BERT+LSTM for SQLi detection	Transformer + RNN	High accuracy; issues with obfuscation	Network SQLi traffic	High
Yazeed Abdulmalik (2021)	Review of SQLi types/detection	Categorical analysis	Hybrid static + dynamic best	SQLi threats	N/A
Ding Chen (2021)	DL for SQLi detection	Word2Vec + CNN + MLP	Reduced false positives	Web application security	High
Divya Gangwani (2020)	ML in cloud security	Review of ML models	Supervised/unsupervised methods effective	Cloud security	N/A
Erdal Ozdogan (2024)	ML for IDS in IoT	Dataset preprocessing + ML	Balanced data boosts detection	IoT networks	High

Adeyinka Ayodeji Mustapha (2024)	SQLi detection in e-commerce	Compare LR, NB, RF, ANN	RF best on imbalanced data	E-commerce SQLi	High
Khazane, H. (2024)	Adversarial ML in IoT	Review of defense mechanisms	Need for IoT-specific solutions	IoT ML security	N/A
Ntayagabiri, J.P. (2025)	Supervised ML for IoT attack detection	Compare 10 ML models	RF: 99.29%, XGBoost: 99.26%	CICIoT2023 dataset	99.29%
Noman, H.A. (2023)	Code injection in wireless IoT	Implementation + Counter measures	Need robust IoT frameworks	Wireless IoT systems	N/A

STATISTICS

The methodology review highlights various machine learning (ML) approaches, with ML appearing most frequently (10 times), emphasizing its central role. Deep learning (3), SVM (3), and RF (3) are commonly evaluated models, showcasing diverse classification techniques. IDS-related methods appear twice, reflecting a focus on intrusion detection. The presence of CNN, ANN, LSTM, NLP, IoT, datasets, and auto encoders, though not as frequent, indicates a broad spectrum of techniques used, including deep learning architectures, hybrid models, and AI-driven security frameworks. The study covers supervised and unsupervised learning, anomaly detection, data augmentation, and hybrid semantic embeddings, illustrating a comprehensive and evolving approach to cybersecurity and AI applications. As show in figure 1:

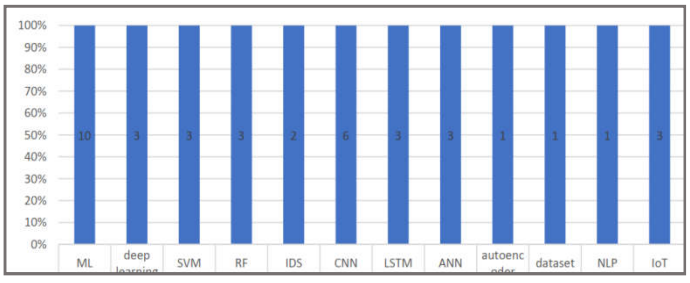

Figure1: frequency for methodology

The key findings emphasize accuracy as the most frequently mentioned aspect (11 times), highlighting its critical role in evaluating ML and AI models. Security (5) and detection (4) are also major concerns, reflecting the focus on enhancing cybersecurity frameworks. Deep learning and hybrid models consistently outperform traditional methods, with CNNs, GANs, and neural

networks proving effective in anomaly detection. Feature selection, data augmentation, and adversarial ML attacks are key considerations, while Random Forest (RF) demonstrated strong performance with high accuracy rates. The study also underscores the necessity of continuous learning, updated datasets, and multi-layered security approaches to combat evolving threats. As show in figure 2:

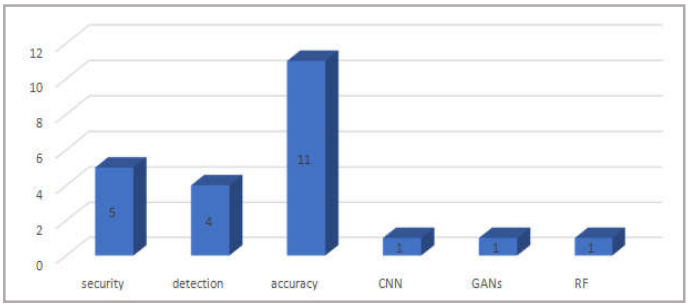

Figure 2: frequency for key findings

The cybersecurity topics provided have been categorized into broader groups based on their focus areas. SQL Injection & Web Security has the highest frequency (7), covering threats like SQLi attacks, web vulnerabilities, and code injection. Cybersecurity Threats & Detection follows with 4 mentions, including network attack detection and cyber threat analysis. Cybersecurity Automation & AI and Cloud & Database Security both appear twice, reflecting interests in AI-driven cybersecurity and cloud security. IoT & 5G Security covers 5 distinct IoT-related threats, while Cybersecurity Research, Urban Computing Security, Network Security, and E-commerce & Online Security each appear once. This categorization helps , with SQLi and web ecurity being the most emphasized. As show in figure.

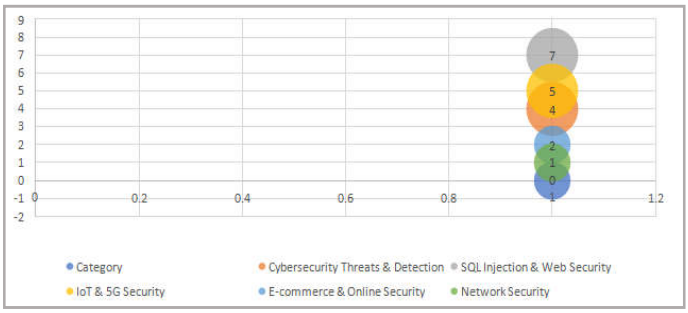

Figure 3: frequency for Context

RECOMMENDATIONS

1. **Standardize Datasets**: Create open-access, diverse, and realistic SQLi datasets for better model training and academic benchmarking.
2. **Adopt Hybrid Models**: Use combinations of deep learning, classical ML, and generative models to improve detection accuracy and robustness.
3. **Enhance Adversarial Defense**: Implement adversarial training to defend against obfuscated and evasion-based SQLi attacks.
4. **Enable Real-Time Detection**: Deploy lightweight AI models on cloud/edge systems for fast and efficient SQLi mitigation.
5. **Ensure Explainability (XAI)**: Make AI decisions interpretable using tools like SHAP or LIME to build trust and support ethical use.
6. **Address Privacy & Ethics**: Apply data anonymization and follow ethical AI principles to protect user data and rights.
7. **Use Generative AI for Data Augmentation**: Employ GANs and VAEs to create synthetic attack samples and balance datasets.
8. **Scale AI Solutions**: Design adaptive models that work across different digital platforms (web, cloud, IoT).
9. **Promote Collaboration**: Encourage cross-sector partnerships between researchers, practitioners, and policymakers.
10. **Continuously Evaluate Models**: Benchmark performance with real-world logs and public datasets, focusing on false positives and adaptability.

CONCLUSION

This review highlights the crucial role of artificial intelligence and machine learning in advancing cybersecurity, particularly in detecting and mitigating SQL injection (SQLi) attacks. Traditional security mechanisms, such as Web Application Firewalls (WAFs) and signature-based Intrusion Detection Systems (IDS), are no longer sufficient to counter evolving cyber threats. AI-driven approaches, including deep learning models like CNNs, LSTMs, and hybrid models, have demonstrated superior performance in intrusion detection and anomaly recognition. Additionally, reinforcement learning and generative AI models have shown promise in improving security defenses through automated attack pattern detection and data augmentation. However, challenges such as dataset imbalance, adversarial ML attacks, computational costs, and ethical concerns remain significant barriers to widespread adoption. The need for standardized datasets and open-access cybersecurity data is critical to ensuring comparability and reproducibility in academic research. Moving forward, future research should focus on developing robust, scalable, and interpretable AI-driven security models that can effectively adapt to emerging cyber threats. By integrating multiple AI techniques, improving adversarial resilience, and optimizing computational efficiency, the field of AI-powered cybersecurity can achieve greater accuracy, scalability, and reliability in safeguarding digital infrastructures.

REFERENCES

[1] F. Q. Kareem et al., “SQL Injection Attacks Prevention System Technology: Review,” Asian J. Res. Comput. Sci., pp. 13–32, Jul. 2021, doi: 10.9734/ajrcos/2021/v10i330242.

[2] N. Thalji, A. Raza, M. S. Islam, N. A. Samee, and M. M. Jamjoom, “AE-Net: Novel Autoencoder- Based Deep Features for SQL Injection Attack Detection,” IEEE Access, vol. 11, pp. 135507–135516, 2023, doi: 10.1109/ACCESS.2023.3337645.

[3] Y. N. Variya, “SQL Injection Attack Detection using Naive Bayes Classifier”.

[4] H. Khazane, M. Ridouani, F. Salahdine, and N. Kaabouch, “A holistic review of machine learning adversarial attacks in IoT networks,” Future Internet, vol. 16, no. 1, p. 32, 2024.

[5] P. R. McWhirter, K. Kifayat, Q. Shi, and B. Askwith, “SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel,” J. Inf. Secur. Appl., vol. 40, pp. 199–216, Jun. 2018, doi: 10.1016/j.jisa.2018.04.001.

[6] A. Adamova, T. Zhukabayeva, Z. Mukanova, and Z. Oralbekova, “Enhancing internet of things security against structured query language injection and brute force attacks through federated learning,” Int. J. Electr. Comput. Eng. IJECE, vol. 15, no. 1, p. 1187, Feb. 2025, doi: 10.11591/ijece.v15i1.pp1187- 1199.

[7] A. Fatima et al., “Analyzing breast cancer detection using machine learning & deep learning techniques,” J. Comput. Biomed. Inform., vol. 7, no. 02, 2024.

[8] L. Ofusori, T. Bokaba, and S. Mhlongo, "Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction," Appl. Artif. Intell., vol. 38, no. 1, p. 2439609, Dec. 2024, doi: 10.1080/08839514.2024.2439609.

[9] M. Hamidouche, E. Popko, and B. Ouni, "Enhancing IoT Security via Automatic Network Traffic Analysis: The Transition from Machine Learning to Deep Learning," Nov. 20, 2023, arXiv: arXiv:2312.00034. doi: 10.48550/arXiv.2312.00034.

[10] M. Sajid et al., "Enhancing intrusion detection: a hybrid machine and deep learning approach," J. Cloud Comput., vol. 13, no. 1, p. 123, Jul. 2024, doi:10.1186/s13677-024-00685-x.

[11] E. Owusu, M. Rahouti, D. F. Hsu, K. Xiong, and Y. Xin, "Enhancing ML-Based DoS Attack Detection Through Combinatorial Fusion Analysis," Oct. 02, 2023, arXiv: arXiv:2312.00006. doi: 10.48550/arXiv.2312.00006.

[12] A. Adamova, T. Zhukabayeva, Z. Mukanova, and Z. Oralbekova, "Enhancing internet of things security against structured query language injection and brute force attacks through federated learning.," Int. J. Electr. Comput. Eng. 2088-8708, vol. 15, no. 1, 2025.

[13] M. Sajid et al., "Enhancing intrusion detection: a hybrid machine and deep learning approach," J. Cloud Comput., vol. 13, no. 1, p. 123, 2024.

[14] P. R. McWhirter, K. Kifayat, Q. Shi, and B. Askwith, "SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel," J. Inf. Secur. Appl., vol. 40, pp. 199–216, 2018.

[15] M. Hamidouche, E. Popko, and B. Ouni, "Enhancing iot security via automatic network traffic analysis: The transition from machine learning to deep learning," presented at the Proceedings of the 13th International Conference on the Internet of Things, 2023, pp. 105–112.

[16] A. F. Al-zubidi, A. K. Farhan, and E.-S. M. El-Kenawy, "Surveying Machine Learning in Cyberattack Datasets: A Comprehensive Analysis," J. Soft Comput. Comput. Appl., vol. 1, no. 1, Jun. 2024, doi: 10.70403/3008-1084.1000.

[17] A. Odeh and A. A. Taleb, "Ensemble learning techniques against structured query language injection attacks," Indones. J. Electr. Eng. Comput. Sci., vol. 35, no. 2, p. 1004, Aug. 2024, doi: 10.11591/ijeecs.v35.i2.pp1004-1012.

[18] A. Ghosh, S. Diyasi, and S. Chatterjee, "Enhancing SQL Injection Prevention: Ad- vanced Machine Learning and LSTM-Based Techniques".

[19] M. S. Souza, S. E. S. B. Ribeiro, V. C. Lima, F. J. Cardoso, and R. L. Gomes, "Combining Regular Expressions and Machine Learning for SQL Injection Detection in Urban Computing," J. Internet Serv. Appl., vol. 15, no. 1, pp. 103–111, Jul. 2024, doi: 10.5753/jisa.2024.3799.

[20] D. Pandya, A. Jadeja, M. Bhuptani, V. Patel, K. Mehta, and D. Brahmbhatt, "Machine Learning: Enhancing Cybersecurity through Attack Detection and Identification," ITM Web Conf., vol. 65, p. 03010, 2024, doi: 10.1051/itmconf/20246503010.

[21] M. Ghurab, G. Gaphari, F. Alshami, R. Alshamy, and S. Othman, "A Detailed Analysis of Benchmark Datasets for Network Intrusion Detection System," Asian J. Res. Comput. Sci., pp. 14–33, Apr. 2021, doi: 10.9734/ajrcos/2021/v7i430185.

[22] S. I. Abir et al., "Accelerating BRICS Economic Growth: AI-Driven Data Analytics for Informed Policy and Decision Making," J. Econ. Finance Account. Stud., vol. 6, no. 6, pp. 102–115, 2024.

[23] M. Liu, K. Li, and T. Chen, "DeepSQLi: Deep Semantic Learning for Testing SQL Injection," May 24, 2020, arXiv: arXiv:2005.11728. doi: 10.48550/arXiv.2005.11728.

[24] N. S. Dasari, A. Badii, A. Moin, and A. Ashlam, "Enhancing SQL Injection Detection and Prevention Using Generative Models," Feb. 07, 2025, arXiv: arXiv:2502.04786. doi: 10.48550/arXiv.2502.04786.

[25] N. Augustine, A. B. Md. Sultan, M. H. Osman, and K. Y. Sharif, "Application of Artificial Intelligence in Detecting SQL Injection Attacks," JOIV Int. J. Inform. Vis., vol. 8, no. 4, p. 2131, Dec. 2024, doi: 10.62527/joiv.8.4.3631.

[26] O. Senouci and N. Benaouda, "Advanced deep learning framework for detecting SQL injection attacks based on GRU Model," Stud. Eng. EXACT Sci., vol. 5, no. 2, p. e11299, Nov. 2024, doi: 10.54021/seesv5n2-596.

[27] R. Mohammad, F. Saeed, A. A. Almazroi, F. S. Alsubaei, and A. A. Almazroi, "Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach," Systems, vol. 12, no. 3, p. 79, Mar. 2024, doi: 10.3390/systems12030079.

[28] R. Bakır and H. Bakır, "Swift Detection of XSS Attacks: Enhancing XSS Attack Detection by Leveraging Hybrid Semantic Embeddings and AI Techniques," Arab. J. Sci. Eng., vol. 50, no. 2, pp. 1191– 1207, Jan. 2025, doi: 10.1007/s13369-024-09140-0.

[29] R. L. Alaoui and E. H. Nfaoui, "Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review," Future Internet, vol. 14, no. 4, p. 118, Apr. 2022, doi: 10.3390/fi14040118.

[30] W. B. Demilie and F. G. Deriba, "Detection and prevention of SQLI attacks and developing compressive framework using machine learning and hybrid techniques," J. Big Data, vol. 9, no. 1, p. 124, Dec. 2022, doi: 10.1186/s40537-022-00678-0.

[31] S. Abaimov and G. Bianchi, "CODDLE: Code-Injection Detection With Deep Learning," IEEE Access, vol. 7, pp. 128617–128627, 2019, doi: 10.1109/ACCESS.2019.2939870.

[32] X. Wang, S. Gao, Y. Zou, J. Guo, and C. Wang, "IH-ViT: Vision Transformer-based Integrated Circuit Appear-ance Defect Detection," ArXiv Prepr. ArXiv230204521, 2023.

[33] Z. Salah and E. Abu Elsoud, "Enhancing Intrusion Detection in 5G and IoT Environments: A Comprehensive Machine Learning Approach Leveraging AWID3 Dataset," Jul. 24, 2023, Computer Science and Mathematics. doi: 10.20944/preprints202307.1565.v1.

[34] Y. Liu and Y. Dai, "Deep Learning in Cybersecurity: A Hybrid BERT–LSTM Network for SQL Injection Attack Detection," IET Inf. Secur., vol. 2024, no. 1, p. 5565950, Jan. 2024, doi: 10.1049/2024/5565950.

[35] Y. Abdulmalik, "An Improved SQL Injection Attack Detection Model Using Machine Learning Techniques," Int. J. Innov. Comput., vol. 11, no. 1, pp. 53–57, Apr. 2021, doi: 10.11113/ijic.v11n1.300.

[36] D. Chen, Q. Yan, C. Wu, and J. Zhao, "Sql injection attack detection and prevention techniques using deep learning," presented at the Journal of Physics: Conference Series, IOP Publishing, 2021, p. 012055.

[37] D. Gangwani, H. A. Sanghvi, V. Parmar, R. H. Patel, and A. S. Pandya, "A comprehensive review on cloud security using machine learning techniques," Artif. Intell. Cyber Secur. Theor. Appl., pp. 1–24, 2023.

[38] E. Ozdogan, "A comprehensive analysis of the machine learning algorithms in IoT IDS systems," IEEE Access, 2024.

[39] A. A. Mustapha, A. S. Udeh, T. A. Ashi, O. S. Sobowale, M. J. Akinwande, and A. O. Oteniara, "Comprehensive review of machine learning models for sql injection detection in e-commerce," World J. Adv. Res. Rev., vol. 23, no. 1, pp. 451–465, 2024.

[40] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. El Makhtoum, “A Comparative Analysis of Supervised Machine Learning Algorithms for IoT Attack Detection and Classification,” J. Comput. Theor. Appl., vol. 2, no. 3, pp. 395–409, 2025.

[41] H. A. Noman and O. M. Abu-Sharkh, “Code injection attacks in wireless-based Internet of Things (IoT): A comprehensive review and practical implementations,” Sensors, vol. 23, no. 13, p. 6067, 2023.

****