Research

SN	Topic	Ref	Problem Statement	Methodology	Outcome
1	Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity	Kuzlu, Murat, Corinne Fair, and Ozgur Guler. "Role of artificial intelligence in the Internet of Things (IoT) cybersecurity." *Discover Internet of things* 1, no. 1,pp.7, 2021.	IoT systems, with their multiple attack surfaces and lack of standardized security protocols, are highly vulnerable to cyberattacks. Traditional security measures are insufficient to address sophisticated threats such as man-in-the-middle attacks, false data injection, and botnets. This research investigates how AI can be used both as a defense mechanism to protect IoT systems and as a tool exploited by attackers, underlining the dual-edged role of AI in IoT cybersecurity.	• **Literature Review**: • Analyze existing studies on AI and IoT cybersecurity, focusing on common attacks and defense mechanisms. • **Attack Analysis**: • Review different IoT attack methods, such as physical attacks, man-in-the-middle attacks, and botnets, to understand vulnerabilities. • **AI Techniques for Cybersecurity**: • Evaluate AI approaches, including: ○ Machine learning models for intrusion detection. ○ Decision trees and rule-learning techniques for	• Development of robust AI-based models to enhance the security of IoT systems. • Comprehensive understanding of common IoT attacks and their AI-driven countermeasures. • Guidelines for integrating AI into IoT cybersecurity frameworks to address both existing and emerging threats. • Insights into the risks posed by adversarial AI and strategies to mitigate its impact on IoT security. • Contribution to the advancement of secure IoT ecosystems through the use of intelligent, scalable, and proactive cybersecurity measures.

				identifying anomalies. ◦ Artificial neural networks for adaptive threat detection. • **Experimental Validation**: • Test AI-based detection and mitigation models against simulated IoT attack scenarios using datasets like CICIDS2017. • **Exploration of Adversarial AI**: • Examine how attackers use AI for tasks like automating vulnerability detection and executing input attacks. • **Defense Strategies**: • Propose AI-driven defensive frameworks and validate their effectiveness using benchmarks such as accuracy, false positive	

				rates, and response time.	
2	Data Science and its Relationship to Big Data and Data-Driven Decision Making	Provost, Foster, and Tom Fawcett. "Data science and its relationship to big data and data-driven decision making." *Big data* 1, no. 1,pp.51-59, 2013.	Despite its growing popularity, data science is often misunderstood or oversimplified, leading to challenges in its practical application. Organizations struggle to fully leverage data due to the complexities of managing Big Data and integrating insights into decision-making processes. This research addresses the gap in understanding the fundamental principles of data science and its application in optimizing decision-making through Big Data.	• **Literature Review**: • Analyze foundational concepts in data science, Big Data technologies, and data-driven decision-making frameworks. • **Case Studies**: • Examine real-world examples where data science and Big Data have been successfully integrated to enhance decision-making. • **Data Collection and Analysis**: • Use secondary datasets to apply data science techniques for predictive analysis and decision-making simulations. • **Framework Development**: • Develop a structured framework connecting data science principles	• Clear understanding of the relationship between data science, Big Data, and decision-making. • Identification of best practices for integrating data science methodologies into organizational processes. • Development of a comprehensive framework that outlines how to systematically apply data science for decision optimization. • Demonstration of the business value of data-driven approaches using case studies and simulations. 1. • Contribution to academic and industry discussions by offering fundamental principles and applications of data science.

				to Big Data applications for decision-making improvements. • **Evaluation**: • Assess the effectiveness of the proposed framework through performance metrics like accuracy, ROI, and decision efficiency.	

3	Supervised machine learning algorithms: classification and comparison	Osisanwo, F. Y., J. E. T. Akinsola, O. Awodele, J. O. Hinmikaiye, O. Olakanmi, and J. Akinjobi. "Supervised machine learning algorithms: classification and comparison." *International Journal of Computer Trends and Technology (IJCTT)* 48, no. 3 ,pp.128-138, 2017.	With numerous supervised machine learning algorithms available, selecting the most appropriate one for a given task remains a challenge. Variations in data characteristics, such as size, dimensionality, and feature types, further complicate this decision. This research addresses the need for systematic classification and comparative	• **Literature Review**:
				
				  • Analyze existing studies on supervised learning algorithms, focusing on their theoretical foundations and practical applications.
				
				• **Data Selection**:
				
				  • Use a well-structured dataset (e.g., Pima Indians Diabetes dataset) containing both numerical and categorical features for classification tasks.
					• Identification of the most accurate and efficient supervised learning algorithms for specific classification tasks.
					• Insights into the trade-offs between computational complexity and prediction accuracy.
					• Guidelines for selecting algorithms based on dataset characteristics such as size and feature distribution.
					• Case studies demonstrating the practical implications of algorithm selection in real-world scenarios.
					• Recommendations for improving machine learning workflows by integrating optimal

			analysis of supervised learning algorithms to guide their optimal use in predictive modeling.	• **Algorithm Implementation**: • Evaluate seven supervised learning algorithms: Decision Table, Random Forest, Naïve Bayes, SVM, Neural Networks, JRip, and Decision Tree (J48). • Perform experiments using the WEKA tool for consistent and reproducible results. • **Performance Metrics**: • Measure accuracy, precision, Kappa statistic, Mean Absolute Error (MAE), and computational time for each algorithm. • **Analysis**: • Compare performance metrics across algorithms for both large and small datasets. • Examine the effect of varying feature sets and sample sizes on	classification techniques.

				algorithm performance.	
4	Automating CI/CD Pipelines with Machine Learning Algorithms: Optimizing Build and Deployment Processes in DevOps Ecosystems	Tamanampudi, Venkata Mohit. "Automating CI/CD Pipelines with Machine Learning Algorithms: Optimizing Build and Deployment Processes in DevOps Ecosystems." *Distributed Learning and Broad Applications in Scientific Research* 5 ,pp. 810-849, 2019.	Traditional CI/CD pipelines are highly automated but rely heavily on predefined rules and manual interventions, limiting their ability to handle modern software complexities. Issues such as build failures, inefficient rollbacks, and rigid deployment strategies challenge the pace and reliability of software delivery. This creates a need for intelligent, data-driven systems that can optimize these processes and adapt dynamically to changing conditions.	• **Predictive Failure Detection**: Leveraging machine learning models such as decision trees, random forests, and neural networks to identify patterns indicating potential failures using historical build and deployment data. • **Automated Rollbacks**: Implementing AI-driven anomaly detection models and reinforcement learning techniques to detect deviations and trigger rollbacks without manual intervention. • **Adaptive Deployment Strategies**: Utilizing real-time monitoring of key performance indicators (KPIs) like latency and error rates, combined with reinforcement learning and anomaly detection, to adjust deployment processes dynamically. • **Data Collection and Model Training**: Employing robust data preprocessing and feature engineering for building accurate predictive models and conducting continuous training for adaptive capabilities.	• **Increased Reliability**: Predictive models successfully reduce the frequency of failures and downtime by identifying and mitigating potential issues preemptively. • **Efficiency Gains**: Automated rollback mechanisms enhance stability and reduce manual effort, while adaptive strategies optimize resource usage and deployment efficiency. • **Organizational Alignment**: Encourages collaboration between data scientists, DevOps teams, and developers for seamless integration of AI into existing workflows. • **Transformative Impact**: AI-driven CI/CD pipelines accelerate delivery cycles, enhance software quality, and align with agile development practices.
5	Integrated Method of Deep	Guan, Bo, Jin Cao, Xingqi Wang, Zhuoyue	Traditional speech recognition	• **Integrated Framework Design**:	• **Performance Improvements**:

	Learning and Large Language Model in Speech Recognition	Wang, Mingxiu Sui, and Zixiang Wang. "Integrated method of deep learning and large language model in speech recognition." In *2024 IEEE 7th International Conference on Electronic Information and Communication Technology (ICEICT)*, pp. 487-490, 2024.	systems often struggle with complex contexts, accent variability, and background noise. Despite advancements in deep learning and LLMs, a cohesive integration of these technologies to fully utilize their respective strengths for improving system performance remains an unresolved challenge.	- Developed an LLM-HMM hybrid system that combines LLMs for acoustic signal feature extraction with HMM for state transition modeling. - Incorporated CNN to enhance local feature capturing and DNN for posterior probability estimation. **Data and Training**: - Used TIMIT, LibriSpeech, and Common Voice datasets for evaluation, representing various accents, noise conditions, and languages. - Conducted pre-training on broad datasets (e.g., LibriSpeech) followed by fine-tuning on specific datasets like TIMIT. **Performance Metrics**: - Evaluated the models on WER (word error rate) and RTF (real-time factor) to measure accuracy	- Significant reductions in WER across datasets: TIMIT (18.5% → 15.2%), LibriSpeech (10.3% → 8.4%), Common Voice (22.0% → 17.8%). - Enhanced RTF, demonstrating better real-time performance. **Adaptability**: - The integrated model outperformed traditional approaches in handling diverse languages and accents, even in noisy environments. **Future Potential**: - Establishes a foundation for refining speech recognition technologies through advanced integrations

				and processing efficiency. • **Optimization Techniques**: • Applied cross-entropy loss and expectation maximization (EM) algorithms for training and fine-tuning model parameters.	of DL and LLMs.