Critical Analysis of Papers 1 to 10 (Rotated, Enlarged, Limited Rows per Page)

	to digital interconnectivity.	ies.	strategies.	emphasized AI's dual role in enabling and defending attacks.	specific insights.
2. Ransomware Trends	Statistical analysis of ransomware attacks over a decade.	Attack logs and financial impact data (2010-2022).	Quantitative analysis using statistical models.	Ransomware increased by 400%; healthcare and financial sectors most affected.	Limited geographic focus (U.S. and Europe); third-party data biases.
3. Social Engineering	Explores human vulnerabilities exploited by social engineering.	Case studies, surveys, and psychological experiments.	Qualitative and experimental with a psychological focus.	Human error causes 85% of breaches; emotional triggers like urgency exploited.	Narrow focus on phishing; small experimental sample sizes.
4. AI for Malware Detection	Analyzed AI's role in detecting malware.	Malware datasets (e.g., VirusShare).	Experimental with AI models (ML, anomaly detection).	Behavioral analysis outperformed signature-based methods; achieved 95% accuracy.	High false positives; computationally intensive.
5. Zero Trust Architecture	Conceptual exploration of Zero Trust Architecture (ZTA).	No datasets; relied on theoretical models and case studies.	Conceptual analysis with examples of ZTA implementations.	Reduces insider threats; emphasizes long-term benefits.	Lacks quantitative validation; high implementation complexity.
6. Economics of Cybersecurity	Examines financial impacts of cybersecurity breaches.	Financial data from breach reports and industry surveys.	Economic modeling for cost-benefit analysis.	Average breach cost: $4.35M; proactive strategies save 20-30% in costs.	Relies on self-reported data; limited SME focus.
7. Rhysida Ransomware Case Study	Analyzed the 2023 ransomware attack on the British Library.	Incident reports, leaked data, and audits.	Forensic analysis of attack lifecycle.	Exploited outdated systems; reinforced need for patch management.	Single case study limits broader applicability.
8. Anatomy of Phishing	Evaluates the lifecycle of phishing attacks.	Historical phishing data (e.g., APWG).	Descriptive focus on phases, attacker types, and countermeasures.	SMS and social media phishing on the rise; human education most effective countermeasure.	Overemphasis on email phishing; lacks experimental validation.
9. AI for Spear Phishing Defense	Investigates AI's role in spear phishing defense.	Email datasets, including phishing examples.	Experimental with AI models (ML, NLP).	AI achieves 90-95% accuracy; behavioral analysis detects internal threats.	High false positives; data diversity dependency.
10. AI in Spear Phishing Defense	Systematic review of 30 studies on AI in cybersecurity.	Reviewed existing datasets; no new ones generated.	Literature review and thematic synthesis.	NLP and deep learning improve detection; integration with user education	Secondary data reliance; adaptability to evolv-