WEST VIRGINIA STATE UNIVERSITY
1891
CyberSecurity Innovation Center

2026 URDC

Detection of Identity Theft in Critical Sectors: A Comprehensive Literature Review

Shikhar Pandey & Ali Al-Sinnayid (Mentor)

Department of Mathematics and Computer Science, West Virginia State University

WEST VIRGINIA STATE UNIVERSITY
1891

Abstract:

Identity theft has become one of the most rapidly growing cyber threats, significantly impacting critical sectors including finance, healthcare, e-commerce, and government systems. The increasing digitization of services and interconnected infrastructure has expanded the attack surface for malicious actors, leading to financial losses, operational disruptions, and long-term security risks. This study presents a comprehensive literature review of identity theft detection approaches, examining their effectiveness across high-risk sectors. The analysis compares algorithmic performance using key evaluation metrics such as accuracy, sensitivity, and precision. Findings reveal that detection performance varies depending on sector-specific challenges and attack types, with no single approach universally outperforming others. The results emphasize the importance of adaptive, context-aware detection strategies to enhance cybersecurity resilience and protect sensitive information within critical infrastructure environments.

Introduction:

Identity theft is the unauthorized acquisition and misuse of personal or sensitive information for fraudulent purposes, and it has become one of the fastest-growing cybercrimes worldwide. As digital transformation accelerates across financial institutions, healthcare systems, e-commerce platforms, and government services, the volume of sensitive data stored and transmitted online continues to expand. This rapid digitization has increased exposure to sophisticated cyberattacks, resulting in financial losses, reputational damage, operational disruption, and long-term security risks. Traditional security mechanisms are often insufficient against evolving attack strategies such as phishing, synthetic identity fraud, and large-scale data breaches. Consequently, effective detection and prevention strategies are essential to safeguard critical infrastructure. This research examines identity theft detection approaches and evaluates their effectiveness across high-risk sectors to identify strategies that enhance cybersecurity resilience.

Acknowledgment

We sincerely thank the CyberSecurity Innovation Center (CIC) for providing this valuable research opportunity. We are especially grateful to Dr. Ali Al-Sinayyid for his mentorship and guidance throughout this study.

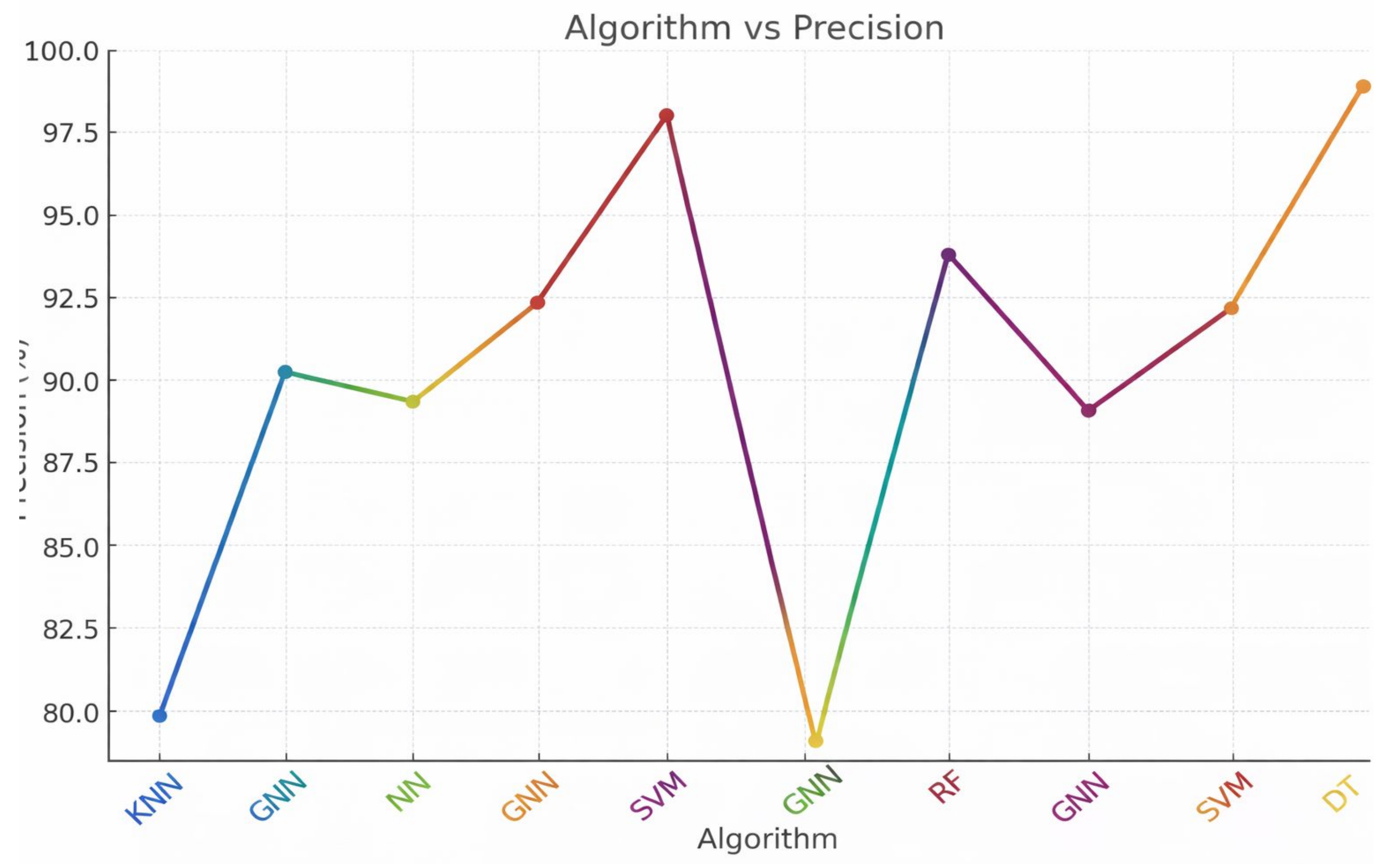


Fig-1: Algorithm and precision comparision

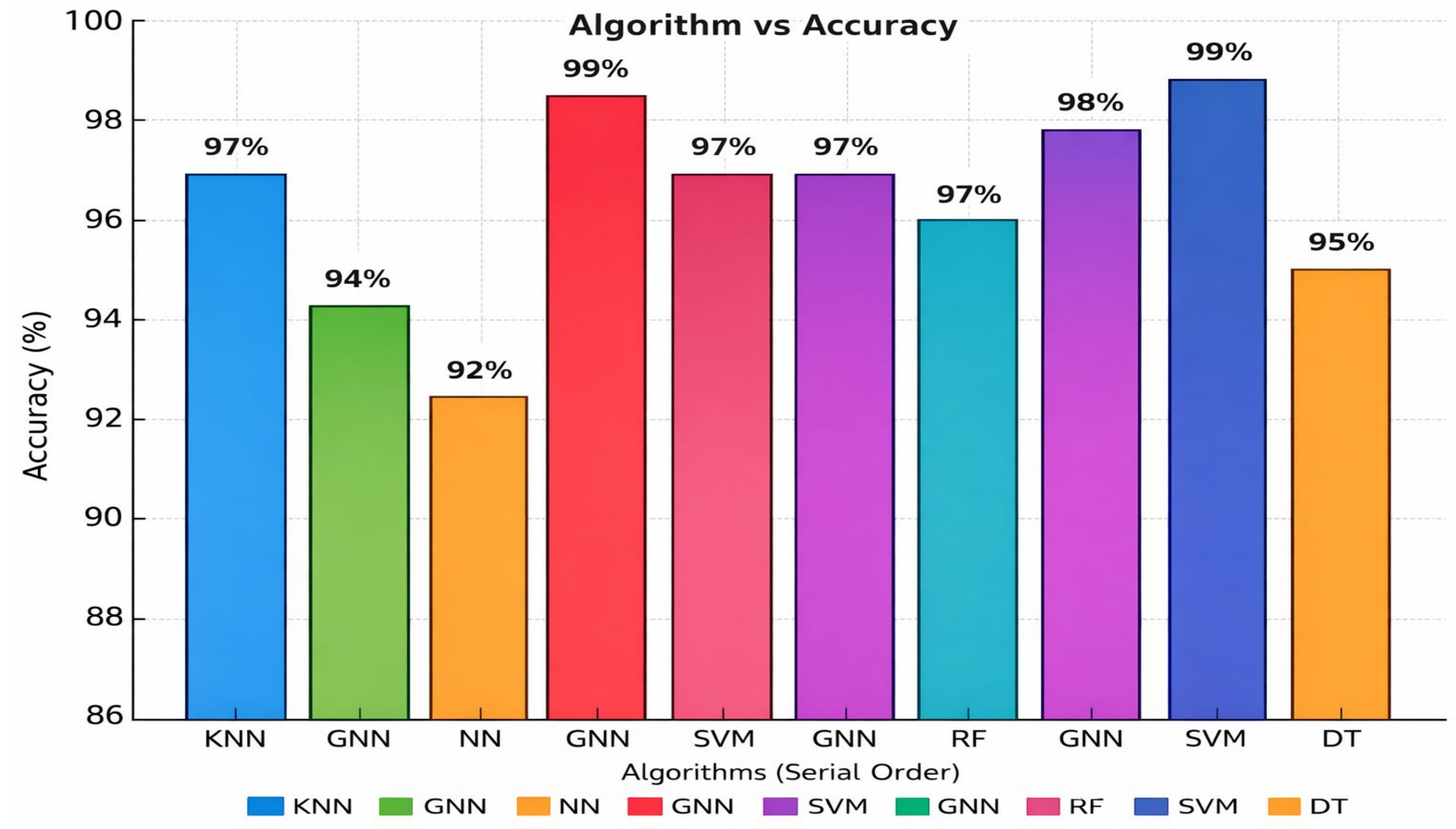
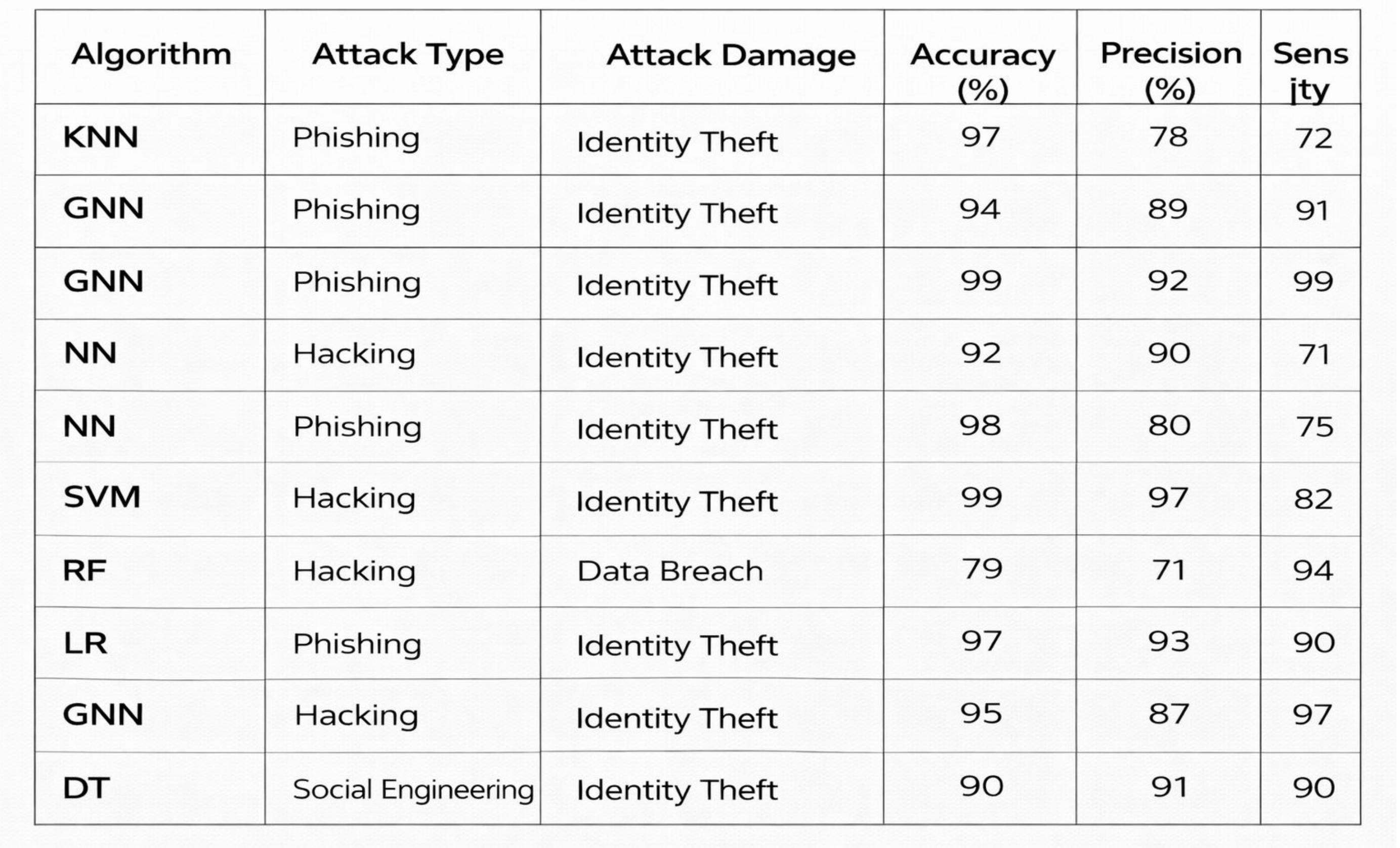


Fig-2: Algorithm and Accuracy Comparision.

Analysis The comparative evaluation of identity theft detection approaches reveals notable variations in algorithmic performance across sectors and attack types. Financial and e-commerce environments demonstrate higher vulnerability due to transaction volume and real-time processing demands. Performance metrics such as accuracy, sensitivity, and precision highlight important trade-offs. Some algorithms achieve high overall accuracy, while others demonstrate superior sensitivity in identifying true positive cases, reducing the risk of missed fraudulent activities. Precision-focused models help minimize false positives, which is critical in financial systems where incorrect flagging can disrupt legitimate transactions. The findings indicate that detection effectiveness is strongly influenced by contextual factors, including data characteristics, sector-specific risks, and response time requirements. These results underscore the importance of selecting balanced, sector-aware detection strategies rather than relying on a single universal solution.



Algorithm	Attack Type	Attack Damage	Accuracy (%)	Precision (%)	Sens ity
KNN	Phishing	Identity Theft	97	78	72
GNN	Phishing	Identity Theft	94	89	91
GNN	Phishing	Identity Theft	99	92	99
NN	Hacking	Identity Theft	92	90	71
NN	Phishing	Identity Theft	98	80	75
SVM	Hacking	Identity Theft	99	97	82
RF	Hacking	Data Breach	79	71	94
LR	Phishing	Identity Theft	97	93	90
GNN	Hacking	Identity Theft	95	87	97
DT	Social Engineering	Identity Theft	90	91	90

Fig-3: Comparison Table .

Methodology

This study employs a structured literature review to examine existing research on identity theft detection within critical sectors. Peer-reviewed articles were collected from recognized academic databases, focusing on studies that evaluated detection approaches using measurable performance metrics. The selected research was analyzed based on key criteria, including accuracy, sensitivity, precision, and applicability across sectors such as finance, healthcare, e-commerce, and government systems. Comparative evaluation was conducted to identify strengths, limitations, and sector-specific challenges associated with different detection strategies.

Conclusion

Identity theft continues to pose a significant threat to critical sectors due to increasing digital dependency and evolving cyberattack strategies. The comparative analysis of detection approaches demonstrates that performance varies across sectors and attack types, with no single method universally outperforming others. While some techniques achieve high accuracy, others provide stronger sensitivity or precision depending on contextual demands. These findings highlight the importance of adopting balanced, sector-aware detection strategies that align with specific operational requirements and risk levels. Overall, strengthening identity theft detection mechanisms is essential for enhancing cybersecurity resilience and safeguarding sensitive information within critical infrastructure environments.

.