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

Shikhar Pandey[1*], Ali Al-Sinayyid[1*], Luice Khamboo[2†], Sameul Adewumi[2†], Vishnu Vardhan Sheri[2†], Rohith Reddy Battula[2†]

[1*]West Virginia State University, Institute, 25112, WV, USA. [2]CyberSecurity Innovation Center.

*Corresponding author(s). E-mail(s): spandey@wvstateu.edu; ali.alsinayyid@wvstateu.edu; Contributing authors: lkhamboo@wvstateu.edu; sadewumi@wvstateu.edu; vsheri@wvstateu.edu; rbattula@wvstateu.edu;
[†]These authors contributed equally to this work.

Abstract

Identity theft is a major threat to both individuals and critical sectors such as financial services, government sector and so on where stolen personal data can cause serious financial and operational damage. This study reviews past research on identity theft detection, focusing on methods, performance, and application areas. Advanced techniques like Graph Neural Networks (GNN) are highlighted for their high effectiveness in detecting attacks such as phishing, hacking, and social engineering. The review also shows that detection performance varies with the type of attack, the targeted sector and potential damage, and that response time is crucial for timely mitigation. These findings emphasize the need for adaptive, context-aware detection strategies. By synthesizing existing studies, this review provides a foundation for developing robust systems that enhance the detection of identity theft and strengthen protection of sensitive data in critical sectors.

Keywords: Identity theft, cybercrime, critical sectors, financial fraud, phishing, Graph Neural Networks (GNN), detection systems, data protection, cybersecurity, response time

1 Introduction

In recent years, Identity theft has become one of the most widespread and damaging cybercrimes [1], affecting millions of people around the world. This crime involves stealing personal information such as Social Security numbers, bank account details, and credit card information, and using it for fraudulent purposes. As digital technology continues to grow, cybercriminals are developing more advanced techniques, making it harder to protect personal and organizational data. Identity theft threatens not only individuals but also critical sectors such as banking, healthcare, and government services [2]. Criminals can exploit stolen data to disrupt operations, steal resources, or commit

large-scale fraud. Reports show that financial losses from fraud have increased significantly in recent years, and demand for identity protection services is also rising sharply.Most cases of identity theft are committed for financial gain. Criminals may open fake credit accounts, drain bank balances, file false tax returns, or misuse medical insurance information. In some cases, stolen identities are used to gain employment or hide criminal activities. Victims often face not just financial loss but also emotional and psychological stress. The process of recovering your identity and repairing credit can be long and frustrating. Businesses also suffer consequences such as reputational damage, legal action, and loss of public trust when data breaches occur [3]. This research paper aims to examine the scope and impact of identity theft, explore its various forms, and emphasize the urgent need for effective detection techniques and preventive measures to protect both individuals and national infrastructure.

1.1 Concerns Surrounding Identity Theft

Identity theft brings serious consequences for both individuals and organizations. One of the most common problems is financial loss. Thieves may use stolen identities to make purchases, open unauthorized bank accounts, or take out loans, causing long-term financial strain for the victim. Victims often spend months or even years trying to fix the damage. In addition to financial issues, many victims suffer from emotional stress. They may feel anxious, overwhelmed, or unsafe. Damage to credit scores can make it harder to rent a home, apply for jobs, or qualify for a loan. Some criminals also target medical records, using them to receive treatment or medications under another person's name [4]. This can lead to false entries in a victim's health records, which may cause serious problems later. In other cases, stolen identities are used in criminal activities, putting innocent people at risk of legal trouble. With the rise of digital platforms, hackers use various techniques like phishing emails, fake websites, and data breaches to access large amounts of personal data. Many people are unaware of how to protect their information online, and some companies and government systems still lack strong security practices [5].As the use of the internet, artificial intelligence, and smart devices continues to grow, it becomes easier for criminals to collect and misuse personal data. That's why it's important for individuals, companies, and governments to work together, promote cybersecurity awareness, and implement strong protection strategies.

1.2 Identity Theft and Critical Infrastructure Risks

Identity theft does not only affect individuals. It can also cause serious problems for critical infrastructure, which includes systems like power grids, water supplies, hospitals, airports, and communication networks [6]. If someone gains access to these systems using a stolen identity, the consequences can be extremely dangerous. For example, hackers could disable power lines, interfere with hospital equipment, or manipulate transportation systems. Since many of these systems are now connected to the internet, they are more exposed to cyberattacks. It is vital to protect the personal data of people who work in these sectors. Organizations should use secure passwords,

limit access, verify users, and ensure that only trusted individuals can interact with sensitive systems [7]. Protecting identities in these areas is essential for maintaining public safety and national stability.

1.3 The Role of Detection Algorithms in Combating Identity Theft

As identity theft continues to grow in scale and sophistication, traditional prevention methods alone are no longer sufficient. To effectively combat this evolving threat [8] the use of intelligent detection algorithms has become essential. These algorithms are designed to analyze user behavior, transaction patterns, access logs, and other digital indicators to identify suspicious or unusual activities that may signal identity theft [9].Machine learning and artificial intelligence techniques are increasingly being applied to improve detection performance. For example, models can learn from historical data to recognize fraud patterns, detect anomalies in real time, and automatically flag high-risk activities for further investigation. However, detection algorithms must strike a balance between sensitivity and precision. High false positive rates can cause frustration and unnecessary alerts, whereas false negatives allow fraud to go undetected. Furthermore, cybercriminals constantly adapt their tactics, which means algorithms must be regularly re-trained and updated to remain effective [10]. This study aims to critically evaluate the effectiveness of various identity theft detection algorithms, highlight their challenges, and explore potential improvements. By focusing on the algorithmic side of identity theft prevention, this research contributes to building smarter, faster, and more reliable solutions to secure personal and institutional data.

2 Literature Review

The paper Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders by Piquero et al. [11] reports an estimated 26 million American citizens per year have been victims of an identity-based crime. It emphasizes the need for a shift toward recovery. It highlight financial sector were more effected. Technologies such as biometric scanning, dark web monitoring, and AI-based tools show promise, highlighting the essential balance between security and ease of transactions. However, the study reveals gaps in prior research, particularly the limited understanding of how protective technologies are applied in practice.

The study by Zou et al. [12] highlight Users frequently struggle to adhere to expert-recommended security and privacy practices, indicating a need for better recommendations and alignment with user needs. It shows 11.3% had been victims of identity theft among all cyberattack Also study show security practices were adopted more widely than privacy or identity theft practices. It may be limited by social desirability bias and a focus on only 30 predefined practices, while its findings are primarily relevant to online safety, cybersecurity, and identity theft protection for general consumers only.

The paper proposed by Wang et al. [13] focuses on addressing the difficulty of detecting online identity theft in scenarios where available user data is scarce or of low quality, specifically within Online Social Networks (OSNs).The authors found an ”insightful result” demonstrating a complementary effect among these different dimensions of records (online content and offline location) for modeling a user's behavioral patterns and the comprehensive performance (efficacy, response latency, and robustness) of the model is validated by extensive evaluations. The relative anomalous score (S_r) approach outperformed the logarithmic anomalous score (S_l). The method only concentrates on the dependency between a user's check-in location and tip-posting content, disregarding the impact of specific occurring time due to low resolution/missing time intervals in real-life OSN datasets.

The paper Modeling Access Environment and Behavior Sequence for Financial Identity Theft Detection in E-Commerce Services paper by Ye et al. [14] proposed hybrid approach named Envi which is introduced for detecting financial identity theft in Online-to-Offline (O2O) e-commerce platforms. This method integrates heterogeneous graph-based relationships (capturing access environment factors) with historical behavioral sequence analysis to enhance detection accuracy. The paper round around whether a verified account in an O2O e-commerce service is being used by a fraudster by modeling the access environment and behavior sequence, framed as a binary classification problem or not. From the approach Envi outperformed all baselines (LSTM, GRU, GAT, HAN, etc.) got overall good performance The models heavily relies on its components parts and the future research were not explicitly detailed beyond the overall effectiveness demonstrated.

Study done by Wyre et al. [15] examines the identity theft response system from the victim's perspective by applying the sociotechnical systems methodology to analyze the core social actors, tasks, and information flows involved in recovery. Paper is around to establish empirical details regarding its social, task, and information requirements to address the needs of victims. It employs the Event Analysis of Systemic Teamwork (EAST) methodology, which examines three interconnected networks that is Social (actors), Task (activities), and Information (data communicated) and this applies content analysis alongside social network analysis metrics (e.g., sociometric status).The study found no coordinated response system, leaving victims to link disconnected actors. That must detect fraud, investigate, enhance security, and report incidents often proving identity with the same compromised credentials. A key limitation is that two-thirds of clients declined participation, reducing representativeness.
Another gap lies in the low emphasis on proactive measures (e.g., credit bans), reflecting limited public awareness of effective protections. Additionally, the task network is only a simplified representation.

A comparative study of identity theft protection frameworks enhanced by machine learning algorithms by Sriram et al. [16] comparative analysis of identity theft protection frameworks, focusing on their enhancement using machine learning (ML) algorithms (supervised, unsupervised, and hybrid methods) to improve detection and minimize fraud. It show traditional security methods often fail, making ML algorithms necessary

to detect and mitigate evolving threats. Paper proposed three identity protection frameworks (A, B, C) and multiple Machine Learning approaches (Supervised, Unsupervised, Reinforcement Learning) and comparative metric (C_j) was used, integrating Accuracy (A_j), Real-time Responsiveness (R_j), and False Positive Rate (FPR_j) the findings show that ML enables advanced authentication, but long-term resilience demands integrated, proactive strategies. The key challenge lies in designing generalizable models that balance recognition accuracy with performance trade-offs.

Bilge et al. [17] research highlights social networking sites are rapidly gaining popularity and house millions of registered users who share personal information. This growth attracts criminals, making security solutions critical. It developed a prototype attack system called incliner, which includes a Crawler, Profile Creator, Message Sender, and a CAPTCHA Analyzer. To identify identical users across sites, the system used Google searches to compare the top three hits for matching names/institutions the experiments demonstrated that both Profile Cloning and Cross-Site Profile Cloning attacks are effective and feasible in practice. The automated system was successful at breaking CAPTCHAs used by sites like StudiVZ, MeinVZ, and Facebook. But the attacks rely on the high degree of trust users place in social networks which only offers suggestions on how social networking sites can improve security.

The paper examines the growing threat of cyberattacks on critical infrastructure across pivotal sectors more focusing on vulnerability assessment and the value of compromised data it also highlight importance of maintaining trust in financial institutions. The author shaji et al. [18] show Cyberattacks are rapidly increasing in scale and sophistication (quadrupling from 2010–2021) with projected losses reaching $10.5 trillion annually by 2025. Critical infrastructure sectors (representing over 50% of U.S. GDP) are highly vulnerable paper analysis comparative Framework based on five criteria: 1) Financial Loss Exposure, 2) Sensitivity of Compromised Data, 3) Reliability and Safety Impacts, 4) Cyber Readiness, and 5) Regulatory Requirements. The framework highlights acute vulnerabilities in the finance sector, where compromised customer data drives identity and new account fraud, with mitigation through measures like NIST standards, MFA, segmentation, and encryption. The gaps such as legacy systems, talent shortages, and the inability of a single framework to fully address cross-sector cyber risks remain unresolved.

The Research done by Alarfaj et al. [19] utilizes Graph Neural Networks (GNNs) and Autoencoders to enhance business practices and reduce fraudulent activities in large organizations, demonstrating that these deep learning methods effectively detect fraud with a balance of precision and recall and improve the efficiency of banking systems and it proposes a methodology that combines architectural frameworks and advanced neural network models to handle both massive historical data and continuous transaction streams more focused in critical sector specially financial .The GNN model performed optimally with two layers. The model achieved high classification under that model , However it fell short on addressing the critical need for real-world accuracy demanded by financial institutions, as both the GNN and Autoencoder models demonstrated

insufficient accuracy, explicitly noted as less in terms of accuracy which cannot be used in the real world.

Enhanced credit card fraud detection based on attention mechanism and LSTM deep model research done by Benchaji et al. [20] focuses on developing a novel and robust system for credit card fraud detection (CCFD) that effectively addresses the major challenges in the payment industry, particularly the sequential and imbalanced nature of transactional data it uses a hybrid deep learning and preprocessing methodology to develop a novel credit card fraud detection system this paper proposed LSTM-Attention deep model is a highly effective and superior alternative to existing classification methods for credit card fraud detection (CCFD), specifically due to its ability to model sequential data and selectively focus on critical transactions. based on paper result its heavy reliance on a multi-stage preprocessing pipeline (feature selection, SMOTE, UMAP) for feature robustness, which complicates real-time operational deployment, and the implied architectural sub-optimality of the LSTM foundation, which the authors acknowledge by planning future work solely based on non-recurrent attention/transformer architecture.

The study by Saikrishna et al. [21] paper highlights the limitation of current research, which often focuses on only a single facet of user behavior (e.g., keystroke, click stream, UGC), making detection susceptible to insufficient data quality. It emphasizes a necessary paradigm change in favor of composite behavioral modeling to effectively detect oblique patterns suggestive of identity theft. The study employs a Composite Behavior Model (CBM), a Bayesian network–based generative model that integrates online (UGC) and offline (check-in) activities to detect identity theft in OSNs. It delivers strong results with high AUC scores (0.956 on Foursquare, 0.947 on Yelp) and recall (up to 72.2%), while keeping the false positive rate under 1%. However, the evaluation is limited to established OSN datasets (Yelp, Foursquare) it lacking on validation proprietary or dynamic real-world data. Moreover, the model has not been thoroughly assessed for computational complexity or real-time latency, raising concerns about its feasibility in production-grade response systems.

The Paper proposed by Abdelhalim et al. [22] examine the threat of "black hat Google hacking" that is mining publicly available online data for committing application fraud (e.g., fraudulent applications for credit cards or passports). They emphasize that identity theft is rapidly growing, fueled by the Internet's vast repository of sensitive PII, while prior research has largely focused on transactional fraud, leaving application fraud underexplored. The authors adopt a two pronged approach: an exploratory study using "white hat" Google hacking and the design of an Application Fraud Detector tool. Findings highlight the alarming accessibility and volume of personal data online, confirming the threat's severity; however, the proposed solution remains a blueprint rather than a fully developed system.

A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions done by Afriyie et al. [23], focuses on studying and comparing the performance of three supervised machine learning models used to classify, predict, and detect fraudulent credit card transactions. The analysis utilized a dataset of simulated

credit card transactions from the western side of the United States of America spanning January 1, 2020, to December 31, 2020. Based on the finding on methodology, Random Forest was determined to be the most appropriate machine learning algorithm for predicting and detecting fraud in credit card transactions however, acking in the current findings are a comparison against a broader range of machine learning algorithms and the use of national or inter-regional real-world data

The Study done by Mitchell et al. [24] Develops an identity theft prediction model using supervised machine learning and historical U.S. identity theft victim data, employing a design science research approach to address the gap in proactive prediction.Paper main concern is, Can supervised machine learning be used to successfully create an identity theft prediction model to detect and prevent future identity theft by using historical victim data or not for that they employ a Design Science Research (DSR) methodology supported by inferential statistics. The key artifact is a newly constructed dataset used to train a supervised ML model. To analyze relationships, multiple linear regression was applied between the total number of victims and the three most common fraud types, with random sampling conducted on the derived dataset of 1,300 records. The study found a statistically significant relationship, with the training dataset showing strong potential for identifying identity theft victims. However, it did not fully capture the complexity of variable interactions and lacked gender-based analysis, pointing to the need for validation on test data and practical application development.

The research done by Sholademi et al. [25] analyzes the risks posed by AI-generated deep fakes (hyper-realistic fake video, image, and audio content) in facilitating financial crimes and identity theft, while also evaluating AI-driven countermeasures. It highlights the problem of AI's rapid evolution, which has introduced deep fake technology as a potent tool for fraud, leading to significant financial losses, reputational damage, and erosion of trust in digital financial systems.AI-driven systems, such as anomaly detection algorithms and behavioral analytics, are shown to enhance real-time detection and mitigation of deep fakes. The paper also notes limitations of existing technologies, ethical dilemmas arising from the dual-use nature of AI, and the necessity for robust regulatory frameworks.

The study by Chakraborty et al. [26] compares traditional classifiers (SVM, Neural Networks, Logistic Regression, Decision Tree, Bayesian Network, CBR) with a proposed Multilayer Mining Algorithm, comprising Territory Detection and Suspicion Score Detection to detect synthetic identity fraud in credit applications. The approach emphasizes resilience, adaptivity, and quality data, aiming to complement existing detection systems although the algorithm is specific to credit application fraud, and traditional classifiers are unsuitable for real-time detection due to reliance on known fraud labels.

The Paper by Al-Smadi et al. [27] proposes a secure online payment system for credit cards, combining a one-time credit card number generation method with a Machine Learning based fraud detection algorithm to combat database breaches and identity

theft. The system was tested on a real European credit card dataset and six artificially generated datasets, integrating ML algorithms (Decision Tree, SVM, Random Forest, Logistic Regression, Na¨ıve Bayes) for robust detection. Logistic Regression achieved the best performance, while Random Forest had the worst time efficiency.Previous systems often addressed only one security factor. SVM and Na¨ıve Bayes showed poor performance and efficiency, and future work should tackle emerging cyber threats like Man-in-the-Middle attacks and database breaches.

The evolution of fraud: ethical implications in the age of large-scale data breaches and widespread artificial intelligence solutions deployment [28] paper examines the evolution of fraud in the context of large-scale data breaches and advanced deep learning techniques, predicting the emergence of "Identity Theft 2.0." Through conceptual analysis of data brokers, the mosaic effect, and AI, it highlights risks from combining disparate datasets for targeted fraud and emphasizes the need for global collaboration, public awareness, and stricter privacy regulations although its hard to creating a global regulatory body with enforcement powers is challenging, and the opacity of deep learning decisions complicates accountability.

Medapati et al [29] study the application of machine learning (ML) and deep learning (DL) algorithms for identity theft detection, particularly in credit card fraud, emphasizing pattern recognition and outlier detection. It discusses a wide range of algorithms, including SVM, Random Forest, Logistic Regression, Decision Tree, ANN, Naive Bayes, XGBoost, CNN, and specialized models like LDA, highlighting that ML classifiers often outperform traditional approaches. The study omits implementation challenges, lacks country-specific datasets, and does not provide a comprehensive comparison of alternative algorithms beyond autoencoders and CNNs.

The paper by Lorimer et al. [30] proposes a decentralized, participatory framework for identity theft detection on mobile social platforms using mobile edge computing. Less-complex computational tasks are delegated to a user's connections/followers, and results are aggregated by a trusted node, employing a Decision Tree ensemble to achieve efficient and responsive detection. Simulations show high detection rates (¿90% ITDR) and early anomaly detection within the second time window.The framework assumes a trusted aggregator node, and the effects of varying feature sets, participant numbers, weights, and time windows remain underexplored.

3 Methodology

This study uses a structured literature review to consolidate existing research on identity theft detection and prevention. Rather than introducing new datasets or algorithms, it synthesizes prior findings with a focus on methodologies, performance outcomes, and application domains. A systematic search was conducted in IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar using keywords such as "identity theft," "fraud detection," "machine learning," and "cybersecurity."Most of the selected works are recent peer-reviewed journal articles and conference papers, while purely theoretical studies were excluded.

Table 1 Comparison Table

Cite	Algorithm	Targeted Sector	Attack Type	Attack Damage	Response Time	Accuracy (%)	Precision (%)	Sensitivity (%)
13	KNN	Social	Phishing	Identity Theft	Low	97	79	72
14	GNN	E-commerce	Phishing	Financial	Low	94	90	93
16	NN	Financial	Hacking	Identity Theft	Low	92	89	91
17	GNN	Financial	Social Engineering	Identity Theft	High	99	-	-
19	GNN	Financial	Phishing	Financial	High	99	92	99
20	SVM	Financial	Hacking	Financial	High	97	98	91
21	GNN	Social	Phishing	Identity Theft	Low	97	79	72
23	RF	Financial	Phishing	Financial	Low	96	94	97
24	LR	Financial	Hacking	Identity Theft	-	97	-	-
25	GNN	Financial	Phishing	Identity Theft	High	-	92	93
26	GNN	Financial	Hacking	Financial	High	98	89	91
27	LR	Financial	Hacking	Financial	High	98	-	97
28	GNN	Social	Data Breach	Identity Theft	-	-	99	-
29	SVM	Financial	Phishing	Identity Theft	Low	99	92	91
30	DT	Social	Social Engineering	Identity Theft	High	95	99	90

The table provides a comparative overview of various studies on identity theft and cybersecurity attacks, highlighting the algorithms used, targeted sectors, attack types, attack damage, response time, and performance metrics. Algorithms include KNN (K-Nearest Neighbors), GNN (Graph Neural Network), NN (Neural Network), SVM (Support Vector Machine), RF (Random Forest), and DT (Decision Tree). Targeted sectors span SOCIAL (social networks), E-COMMERCE, and FINANCIAL institutions, with attack types such as PHISHING, HACKING, and SOCIAL ENGINEERING. Attack damage ranges from low to high, and response time reflects the system's mitigation speed. Performance metrics, namely accuracy, precision, and sensitivity, are reported in percentages. Overall, GNN and SVM exhibit consistently high accuracy, precision, and sensitivity, while NN and RF perform well in financial sector attacks. KNN and DT are applied mainly in social sectors with moderate effectiveness.

3.1 Comparison of Algorithm and Accuracy

Based on the provided table, a comparison of algorithms with respect to accuracy shows the following insights. The table lists multiple algorithms including K-Nearest Neighbors (KNN), Graph Neural Networks (GNN), Neural Networks (NN), Support Vector Machines (SVM), Random Forest (RF), and Decision Trees (DT). The accuracy for each algorithm varies across different attack types and targeted sectors. Focusing

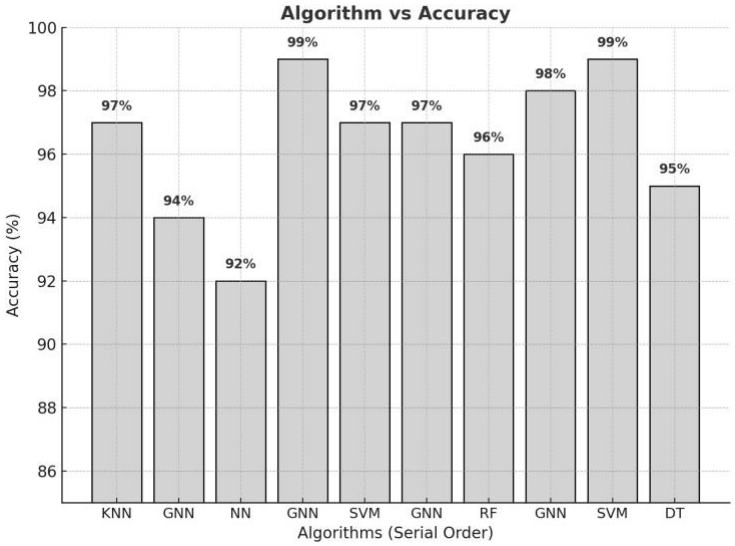

Fig. 1 Comparison of different algorithms based on their accuracy.

on GNN and SVM, both algorithms achieve 99% accuracy, indicating that in terms of raw accuracy, GNN and SVM perform similarly, making it difficult to definitively state which algorithm is superior solely based on this metric. Other algorithms like KNN, NN, RF, and DT also perform well, with accuracies ranging from 92 to 97%, showing that while they

are effective, they are slightly lower than GNN and SVM in this context. Overall, the analysis suggests that while accuracy is a useful measure, it alone is insufficient to determine the best algorithm, especially when multiple algorithms achieve comparable values, as in the case of GNN and SVM.

3.2 Comparison of Algorithm and Sensitivity

When comparing algorithms based on sensitivity, the studies show that Graph Neural Networks (GNN) perform exceptionally well, achieving 99% sensitivity in some cases. This indicates that GNN is highly effective at correctly identifying true positive cases, making it the best-performing algorithm in terms of sensitivity according to several research studies.

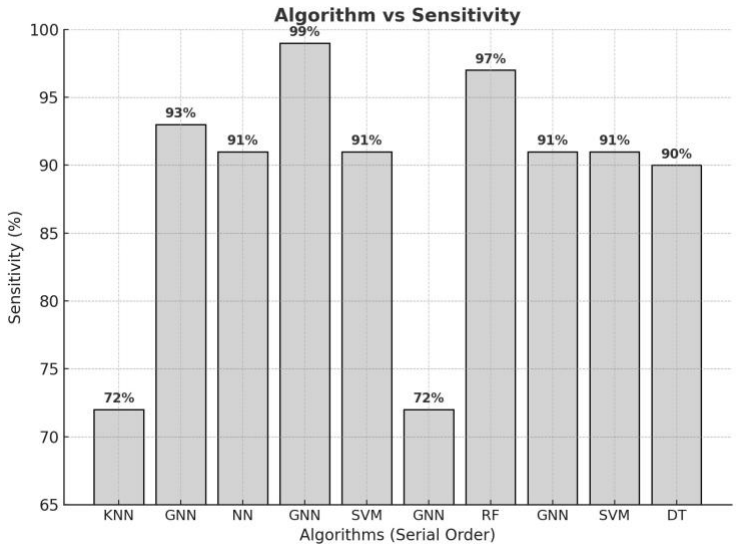

Fig. 2 Comparison of different algorithms based on their sensitivity.

However, it is important to note that performance can vary depending on the type of attack or targeted sector. While GNN excels in certain contexts, other algorithms may perform better for specific scenarios such as hacking detection or social engineering attacks. Therefore, although GNN demonstrates overall superior sensitivity, the optimal choice of algorithm may depend on the specific use case and attack type being addressed.

3.3 Comparison of Algorithm and Precision

As our analysis of algorithm performance shows, precision varies significantly across different detection methods. Algorithms such as SVM, DT, and RF achieve higher precision, reflecting their effectiveness in accurately identifying identity theft, phishing, and other attacks with minimal false positives. In contrast, KNN, NN, and GNN exhibit

slightly lower precision but often compensate with faster response times. This demonstrates that choosing the right algorithm requires balancing precision with detection speed, depending on the severity of the attack and the criticality of the targeted sector.

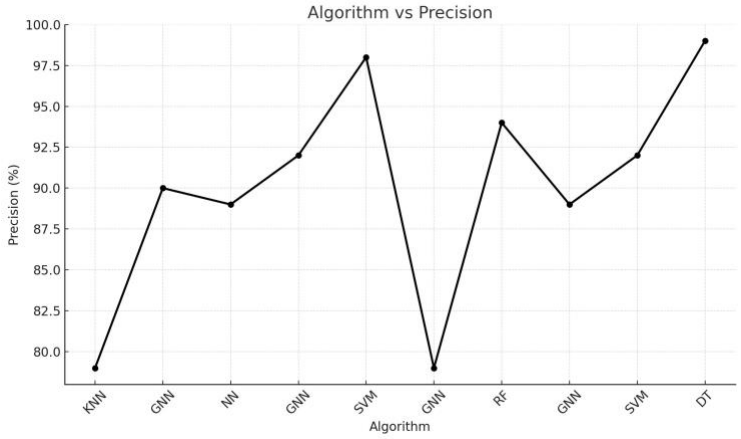

Fig. 3 Comparison of different algorithms based on their precision.

3.4 Targeted Sector

From the data Table 1, it is clear that the financial sector and e-commerce sector are among the most affected. Many algorithms, including GNN, SVM, and NN, are applied to detect attacks in these sectors. The primary attacks involve phishing, hacking, and identity theft, which can lead to financial loss or compromise of sensitive personal information. The recorded attack damage is generally low to moderate, but even lowlevel attacks in financial systems can have significant consequences due to the volume of transactions and the sensitivity of data. In contrast, sectors like social networks are also affected, particularly by phishing and identity theft, but the damage tends to be less direct in monetary terms, often impacting personal information or reputation.Overall, while all sectors experience threats, the financial and e-commerce sectors are more critical due to the potential for high-impact losses, making accurate and responsive algorithms essential for detection and mitigation.

4 Future work

To better protect critical infrastructure, future work should prioritize the development of scalable, real-time identity theft detection systems that can effectively process complex, imbalanced data from diverse industrial environments. Enhancing model transparency and explainability will be vital for adoption by security teams and compliance officers. Industry-driven solutions combining behavioral analytics, graph-

based techniques, and deep learning hold promise against sophisticated threats such as synthetic identity fraud and deepfakes. Furthermore, aligning detection systems with regulatory requirements and privacy standards will ensure responsible deployment. Collaboration between industry practitioners, researchers, and policymakers will be key to creating resilient and adaptive defenses that meet the evolving challenges of identity theft.

5 Conclusion

This review of the literature critically examined previous research on identity theft detection in high-risk sectors, with a particular focus on financial and e-commerce domains, which are the most frequently targeted and heavily affected. The analysis demonstrates that Graph Neural Networks (GNNs) achieve consistently strong sensitivity and accuracy, making them highly effective in detecting diverse identity theft attempts, including phishing and financial fraud. However, algorithms such as Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF) often deliver higher precision, highlighting an important trade-off between accuracy/sensitivity and precision across different methods. Simpler attacks such as phishing and low-damage identity theft are generally identified rapidly, while more complex attacks, including hacking and social engineering, require extended processing to ensure reliable detection. These findings indicate that no single method offers universal effectiveness; instead, the efficiency of detection strategies depends on the attack type, the targeted sector, and the potential level of damage.Overall, this synthesis underscores the importance of adopting context-aware and adaptive detection approaches that balance sensitivity, accuracy, and precision, while also considering response time. Such balanced strategies provide a solid foundation for developing robust identity theft detection systems, ultimately strengthening the protection of critical sectors and safeguarding sensitive personal and financial information.

References

[1] Koops, B.-J., Leenes, R.: Identity theft, identity fraud and/or identityrelated crime. Datenschutz und Datensicherheit - DuD https://doi.org/10.1007/ s11623-006-0141-2

[2] Anifalaje, K.: A legal approach to the protection of customers of banks and other financial institutions from identity theft in nigeria. Northern Ireland Legal Quarterly, 187–214 (2024) https://doi.org/10.53386/nilq.v75i2.1163

[3] Borketey, B.: Identity theft – the root cause of widespread fraudulent activities. International Journal of Automation, Artificial Intelligence and Machine Learning **5**, 26–28 (2025) https://doi.org/10.61797/ijaaiml.v5i1.406

[4] Anderson, K.B., Durbin, E., Salinger, M.A.: Identity theft. Journal of Economic Perspectives **22**(2) (2008)

[5] Whitley: A review of the complex interplay between information systems, identification and identity. European Journal of Information Systems **23**(1) (2014)

[6] Al Smadi, B., Min, M.: A critical review of credit card fraud detection techniques. In: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0732–0736 (2020). IEEE

[7] Guedes, I., Martins, M., Cardoso, C.S.: Exploring the determinants of victimization and fear of online identity theft: An empirical study. Security Journal, 1 (2022)

[8] Maher, C.A., Hayes, B.E.: Nonfinancial consequences of identity theft revisited: Examining the association of out-of-pocket losses with physical or emotional distress and behavioral health. Criminal Justice and Behavior **51**(3), 459–481 (2024)

[9] Salman, H.M.: Identity theft in the banking system. In: Online Identity-An Essential Guide. IntechOpen, ??? (2024)

[10] Sriram, H.K.: A comparative study of identity theft protection frameworks enhanced by machine learning algorithms. SSRN 5236625 (2024)

[11] Piquero, N.L., Piquero, A.R., Gies, S., Green, B., Bobnis, A., Velasquez, E.: Preventing identity theft: Perspectives on technological solutions from industry insiders

[12] Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., Schaub, F.: Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In: CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI), Honolulu, HI, USA (2020). https://doi.org/10.1145/3313831.3376570

[13] Saikrishna, D., Manisha, D.: Composite behavioral modeling for identity theft detection in online social networks **14**, (2024)

[14] Ye, Q., Gao, Y., Zhang, Z., Chen, Y., Li, Y., Gao, M., Chen, S., Wang, X., Chen, Y.: Modeling access environment and behavior sequence for financial identity theft detection in e-commerce services

[15] Wyre, M., Lacey, D., Allan, K.: The identity theft response system. Trends and Issues in Crime and Criminal Justice (592) (2020)

[16] Sriram, H.K.: A comparative study of identity theft protection frameworks enhanced by machine learning algorithms. MSW MANAGEMENT Multidisciplinary, Scientific Work and Management Journal **34**, 1080–1101 (2024)

[17] Bilge, L., Strufe, T., Balzarotti, D., Kirda, E.: All your contacts are belong to us: Automated identity theft attacks on social networks. In: Proc. 18th Int. Conf. World Wide Web (WWW) (2009)

[18] George, D.A.S., Baskar, D.T., Srikaanth, D.P.B.: Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal (PUIIJ) **02** (2024) https://doi.org/10.5281/ zenodo.10639463

[19] Alarfaj, F.K., Shahzadi, S.: Enhancing fraud detection in banking with deep learning: Graph neural networks and autoencoders for real-time credit card fraud prevention. IEEE Access (2024) https://doi.org/10.1109/ACCESS.2024.3466288

[20] Benchaji, I., Douzi, S., El Ouahidi, B., Jaafari, J.: A novel system for credit card fraud detection based on sequential modeling of data, using attention mechanism and lstm deep recurrent neural networks. Journal of Big Data **8**, 151 (2021) https://doi.org/10.1186/s40537-021-00541-8

[21] Saikrishna, D., Manisha, D.: Behavioral analytics for identity theft detection in social networks: A composite modeling approach **14** (2024)

[22] Abdelhalim, A., Traore, I.: The impact of google hacking on identity and application fraud

[23] Afriyie, J.K., Tawiah, K., Pels, W.A., Addai-Henne, S., Dwamena, H.A., Owiredu, E.O., Ayeh, S.A., Eshun, J.: A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal **6**, 100163 (2023) https://doi.org/10.1016/j.dajour.2023.100163

[24] Mitchell, J. Charles D., Sambasivam, S.: Predictive modeling for identity theft detection: A design science approach using machine learning and historical data. Issues in Informing Science and Information Technology **22**(Article 3) (2025) https://doi.org/10.28945/5506

[25] Sholademi, D.B.: Financial crime in the age of ai: Deep fakes and identity theft risks. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS) **06** (2024) https://doi.org/10.56726/IRJMETS65507

[26] Bhattacharya Chakraborty, S., Shaikh, M.Z.: A comprehensive and relative study of detecting deformed identity crime with different classifier algorithms and multilayer mining algorithm. International Journal of Advanced Research in Computer and Communication Engineering **3** (2014)

[27] Al-Smadi, B.: Credit card security system and fraud detection algorithm. Dissertation, Louisiana Tech University (August 2021)

[28] The evolution of fraud: Ethical implications in the age of large-scale data breaches and widespread artificial intelligence solutions deployment. ITU Journal: ICT Discoveries (2018)

[29] Medapati, S.N.: Identity theft detection using machine learning. International Journal of Research Publication and Reviews **4**, 5033–5037 (2023)

[30] Lorimer, P.A.K., Diec, V.M.-F., Kantarci, B.: Participatory detection of identity theft on mobile social platforms