MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

A comparative study of identity theft protection frameworks enhanced by machine learning algorithms

Harish Kumar Sriram, Lead software engineer,
Global Payments, ORCID ID : 0009-0008-2611-2904

Abstract

A data breach occurs when sensitive or confidential data is compromised, leading to the risk of identity theft and other criminal or financial outcomes associated with loss of privacy and confidentiality. The extreme proliferation of data sharing has paradoxically compounded the risk of identity theft. Legislative responses and preemptive questions raised about the ethical implications of sharing data in cybersecurity response cooling-off periods have sought to increase raises and calm those broached questions. Considering the relatively new psychological phenomenon of cognitive load, this postponing of legislation had a cooling-off effect on ethical implications. Even though such processes are considered as temporary, the additional burden created by cognitive load can lead to impulsive decision-making processes and closure, therefore limiting the ability of individuals to correctly evaluate the ethical implications. Such decisions may include the calculation of potential risk of identity theft when sharing or accessing sensitive or confidential data. Though the current regulatory environment encourages the implementation of freezing services as means of risk minimization, these services are not available in all circumstances. Moreover, such services require preemptive action should stakeholders predict the risk of data compromise.

To counter some of the concerns raised by this study, the deployment of intelligent or smart algorithms in either preventing risk of identity theft or flagging potential ongoing identity theft is proposed. The term intelligent in this context refers to decision-support algorithms that are either designed to assist an expert decision-maker, or have themselves been made smarter through reinforcement learning processes. The objective is to supplement the responsibility of individuals and banks entrusted with preventing identity theft with decision-support systems. Enhanced by revision support algorithms deployed by banks as second-line analysis services, the number of confirmed cases of identity theft is significantly likely to decrease.

Keywords: Data Breach, Identity Theft, Confidential Data, Privacy Loss, Data Sharing, Ethical Implications, Cognitive Load, Impulsive Decision-Making, Risk Evaluation, Freezing Services, Risk Minimization, Regulatory Environment, Preemptive Action, Intelligent Algorithms, Smart Algorithms, Reinforcement Learning, Decision-Support Systems, Cybersecurity, Expert Assistance, Second-Line Analysis.

1. Introduction

Identity theft is the act of stealing an individual's personal information, such as their name, Social Security number, address, credit card numbers, etc. to commit fraud for financial gain. In identity theft, an individual's identity can be obtained through different means, including theft of documents such as driver's license, passport, and identity cards; data mining; hacking; social engineering; physical stealing; phishing; and pretext calling. Identity theft is the most widespread type of cybercrime, disrupting millions of lives in the process. The pandemic compelled millions of people to work from home and resulted in the most

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

extensive digitization of processes in both private and public sectors. Such rapid and inevitable digitization has opened many new avenues for hackers to commit crimes, including identity theft.

Computers are very ubiquitous in the modern era. This has led to the rising threat of cybercrime and the introduction of several digital measures to secure a user's system. Earlier software-based solutions were sufficient to help defend against these threats. However, hackers have gradually become more adaptive to counter such measures. This led to the development of intelligent systems using machine learning tools. These systems have proven their worth when it comes to cybercrime detection and have evolved to detect new types of crime, including identity theft. Machine learning systems have now been incorporated with different social networks and online services to regularly monitor behavior on the services to help users be better prepared against detection. The remarkable accuracy of machine learning systems led to their adoption for use with different sectors, including banking, e-commerce, and healthcare.

1.1. Background and Significance of Identity Theft

Protection of personal privacy through identity status is one of the foundations for any society's development. Although identity theft has been traditionally considered a minor crime, it currently represents one of the most serious threats to security, and there is a wide consensus that countries must create an inter-country strategy to modify the current situation. Identity theft is considered a serious crime, especially due to its use for international terrorism financing, leading to the creation of several laws that define the conditions under which identity data can be considered privileged and declare illegal obtaining, storing and using this type of data without the data owner's consent. International terrorism financing through identity theft is not limited to national security established by potential loss of life, but also to the disruption of a nation and international economy through necessary compensative measures for vulnerable entities, private companies and public administration, or banks reporting unlawful transactions, credit report mistakes, or loss of data. The economic disruption is mainly due to trust loss in the systems involved, leading to long-term crises in their operations.

Although several sensationalized cases related to multimillionaire values have been presented, there has been very few well-researched analyses published. As a consequence, currently used methodologies are mostly intuitive and experience-based, or use pre-existent data mining methods, prone to deliver erroneous results, as high values of noise are present due to the difficulties of labeled data for identity theft issues. This absence of coherent and efficient technologies has also driven the proliferation of private companies offering identity theft protection as a service. These companies store and synchronize their clients' data in the most relevant private and public data systems to generate alerts when any activity, using one of their clients' data, is recognized, thus allowing the client to act in a timely manner to protect its identity.

Fig 1 : Preventing Identity Theft With Machine Learning

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

2. Understanding Identity Theft

Identity theft is a malicious crime that occurs when a person or an organization obtains the financial or personal information of someone else without consent. The stolen information is used to impersonate someone else for financial gain or for other illegal actions. In order to accomplish this, the criminal can falsify another person's identity documents by copying the details using equipment such as scanners. Unfortunately, these documents are very easy to forge as there is a complete lack of verification procedures when using them. For example, no one can distinguish the counterfeit identity card unless the performer is a specialist, equipped with the necessary validation tools, who checks all the details of the counterfeited ID card. Very few people, however, are equipped with the necessary expertise. Therefore, the use and acceptance of forged identity cards, social security cards, etc., become really easy thus helping in the successful completion of the crime.

There are several ways to steal someone's identity: simply stealing wallets, purses, credit cards, passports, personal checks; stealing personal information through computers via fraud phishing spam; stealing checks and credit cards through postage mail; stealing personal data through phones; accessing financial documents, tax returns or credit reports. The safeguards introduced for safeguarding important documents have not deterred the wicked intentions of the identity thieves. Modern technology provides additional sophistication to the schemes used to impersonate someone else, so also do the painstaking attacks which the imposters carry out. The identity thieves have now become increasingly sophisticated in purchasing data credit files, which are still stored crudely with very few security checks, and feed their phishing scams into people's email accounts for inciting them into disclosing their personal information, such as passwords, account numbers and social security details. The chances of making the impersonation successful are very high compared to detection.

2.1. Definition and Types of Identity Theft

Identity theft is a deliberate and illegal act committed by an individual to gain a benefit or advantage. This act usually goes unnoticed and can even affect powerful institutions and individuals. Identity theft is described when a person assumes the identity of another in order to take on some type of benefit or service in the name of the other and for personal enrichment. Accordingly, the victim loses control over their identity and the assumed identity uses the data to commit acts against the law. It can also take the form of identity deception, especially through the theft of passwords to access social networks or banking accounts. Cybercriminals impersonate someone else or hack their accounts, publish slanderous phrases, incite violence, etc. The types of identity theft can vary based on the purpose of the act. For example, when any individual tries to change their identity to avoid the judiciary or social sanctions, it is called "identity disguising"; when a hacker tries to assume someone else's account in a social network to make offensive comments, it is called "identity deception"; and "biometric impersonation" or theft of biometric data, usually associated with the theft of passwords, is called when someone bypasses the biometric authentication installed on the digital accounts of a company or an individual.

Identity theft can be perpetrated through the impersonation of official documents, such as passports or driver's licenses. In these cases, the victim's account can be hacked, information and photos are changed, and false identities are created. Information can also be purchased on the Dark Web. The stolen account usually belongs to someone famous or relevant within a company or institution. This type of account is often used to expose confidential information or commit fraud on a larger scale. Financing is a type of

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

identity theft when someone impersonates a lender or financial entity to commit fraud. In this case, the request is usually made through emails that impersonate the lender.

Equation 1 : Identity Threat Probability Estimation using ML

$$P(\text{threat}_i \mid X_i) = \sigma\big(f_\theta(X_i)\big)$$

where
- $P(\text{threat}_i \mid X_i)$: Probability that user i is under identity threat
- X_i: Input features (e.g., login behavior, device fingerprint, access patterns)
- f_θ: ML model with parameters θ
- σ: Sigmoid activation for binary classification

2.2. Impact of Identity Theft on Individuals and Organizations

Most of us share our identity in order to enjoy its privileges, but at the same time we rely on its confidentiality to protect it from criminals who would misuse it for their own gains. When the identity of an innocent person is disclosed and later exploited, it is known as identity theft. Identity theft captures our sympathy as no man is an island and the emotional and social consequences touch innocent bystanders, friends, and especially, family members. The sense of sympathy is likely augmented by the fact that impersonation is often a means to gain access to other privileges, the result of which will touch either physically or financially someone we know. Making matters worse, the people making use of the stolen identities may have no relationship whatsoever with the victims. Worst still, virtual-identity related crimes such as sextortion have the tendency to first affect those closest to the victims, the family and/or close friends, or eventually become public domain.

In financial terms, the overall losses are staggering. The identity theft industry is a multi-billion dollar business and it has an effect on companies and customers. It is a factor which businesses take into consideration when deciding whether or not to conduct business online. Identity theft takes on many guises, such as fraud and dishonest disbursement, identity theft for profit, identity theft to gain temporal or lasting advantages, especially in the case of natural disasters, or identity theft by criminal justice offenders in order to avoid arrest or imprisonment. Most of these crimes touch the physical or financial property of others. Some originate or lead to cyber-crime such as cyberstalking, which may periodically or permanently incapacitate the victims.

Fig 2 : Protect from Identity Theft Attacks

3. Overview of Identity Theft Protection Frameworks

In conjunction with advances in information technology, identity theft protection frameworks have quickly evolved from manual security to a more autonomous process leveraging multiple security layers.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

Traditional identity theft protection methods are based on classic security mechanisms like (i) identification and validation, (ii) strong cryptography, (iii) digital signatures, (iv) digital certificates, (v) access control, and (vi) secure network communication for exchanged identity information, among others. Identity information is usually protected with established techniques such as username/password pairs, smart cards, biometrics, etc. Nonetheless, these mechanisms have fundamental limitations, including potential theft or loss of identity information, cloned or counterfeited biometric data; risk of unauthorized access to protected identity information within federal, state, or private repositories; and improper creation, management, and loss of digital certificates, among others. Furthermore, identity information theft is generally perpetrated without alerting victims or protected entities, so most methods are not able to act before the theft occurs.

Emerging technologies addressing identity theft protection focus on facilitating the detection of identity information theft to minimize the detection time and impact in order to provide a layer of identity information protection. For example, some infrastructures combine advantages of intrusion detection systems with digital certificate forensics in order to detect potential abuses perpetrated by users, systems, or corporations who possess the users' digital certificate; thereby acting before actual theft occurs. Other approaches rely on intervention in social networks, banks or public registry databases as an attempt to stop unauthorized use of identity information prior to the crime's completion. However, they suffer from similar limitations to those traditional methods; i.e., their use is restricted to network and bank transactional data, with a focus on an identity loss prediction from past behavior, or, either on an identity detection prediction after a probable loss is registered.

3.1. Traditional Identity Theft Protection Methods

In recent decades, several traditional methods have been implemented as preventative measures to reduce the likelihood of identity theft fraud. These include credit monitoring services, telephone call identities with social security bans, consumer spending gatekeeping controls, risk-shifting techniques such as the placement of fraud alerts on consumer databases, and controls to protect the identity of persons unlikely to engage in fraudulent activities, such as the elderly. Detecting liability for frauds perpetrated against lenders or merchants, punishment of offenders through civil liability or criminal prosecution, and protection against losses through insurance are also deterrent measures to be applied. Fraud alert methods allow a volunteer to protect his or her information without specialized expertise and without special expense of public funds. However, all of these traditional tools have seen various degrees of criticism for their effectiveness and efficiency and thus merit discussion in greater detail.

While consumers may want credit-monitoring services to alert them to unusual activity in their credit history that may reflect identity theft fraud against them, those alerts may not prevent actual fraud. Similarly, address-change services do not block an impostor from accessing or opening new lines of credit. Methods that would serve as other preventative deterrent measures are the placement of a fraud alert on consumer databases or a system of notification or approval needed for sensitive identity records, like a birth certificate. A fraud alert does require the consumer to notify the three main credit bureaus of any suspect appearance of unusual activity on their records. However, it is much less than desirable to rely on such notification by the consumer in order to trigger preventative engine programs run by the bureaus. Such an alert would possibly only be used in the event of identity theft fraud or other rare events.

3.2. Emerging Technologies in Identity Theft Protection

Advances in technologies such as Big Data, the Internet of Things, Cloud Computing, and Mobile Computing enabled new sophisticated ways of identity management and authentication. However, as the

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

dependence on technologies and networks increased, so did the vulnerabilities related to identity verification. Consequently, the necessity of adequate protection increased, which led to the integration of diverse technologies to privacy enhancement strategies. Biometric data handling, Encryption, and Identity and Access Management are some of the proposed techniques for ITP. Nevertheless, the existing models are still subject to security failures, even with the integration of additional technology techniques in the ITP domain. Recently, Machine Learning algorithms are being integrated into ITP to offer a more accurate approach to detecting potential privacy threats before applied at risk.

Machine learning algorithms can be divided into three different categories: supervised, unsupervised, and hybrid ML. Supervised models learn from labeled datasets where potential risks are previously identified, classifying new data based on the knowledge generated during training. On the other hand, unsupervised models identify hidden patterns in datasets with no predefined labels, considering all data as normal until an unusual behavior appears. Most models applied in ITP belong to the supervised model category. Hybrid models combine techniques from both supervised and unsupervised paradigms. The hybridization is created with the objective of overcoming some disadvantages of unsupervised models, which is the difficulty in recognizing normal behavior without a labeled dataset available when the system is deployed. Therefore, some hybrid models use supervised learning for dataset labeling after receiving knowledge from labeled potential identity thefts.

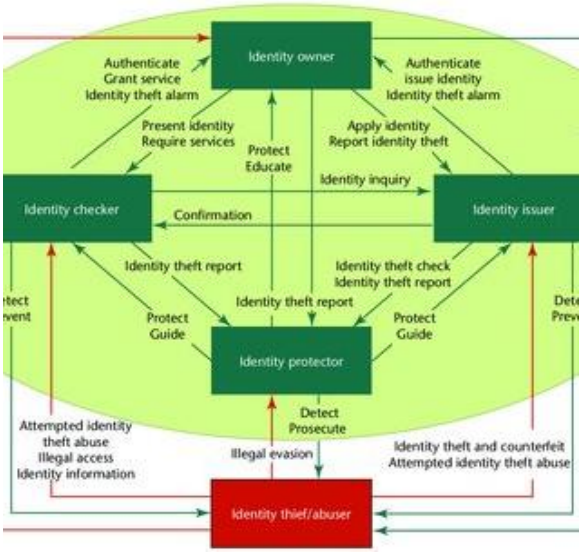


Fig 3 : The contextual framework for combating identity theft

4. Role of Machine Learning in Cybersecurity

Introduction to Machine Learning As defined, Machine Learning (ML) algorithms are programs that analyze data and learn to predict the value of a particular outcome. Alternative definitions suggest that machine learning is an artificial intelligence sub-area that learns to identify patterns in data and can predict outcomes from new data. The most cited definition states that a computer program is said to learn from experience with respect to some class of tasks and performance measure, if its performance at tasks improves with experience. Programs using traditional AI methods solve specific problems by evaluating a number of rules or by reasoning about the information related to the solution. ML programs analyze data to learn how to relate input data to output values or class memberships from the examples of input/output

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

pairs. When presented with new input data, ML programs can predict the related output or assign the input data to one of the defined classes.

Machine learning is currently the widest and most used form of artificial intelligence, and finds application in a wide number of areas, such as computer vision, natural language processing, robotics, games, and social network analysis. The security field is among the main domains where machine learning is heavily employed, proving particularly suitable for pattern recognition and classification tasks, and exhibiting good performance for several specific cybersecurity issues, such as malware detection, classification, and prevention; spam detection and filtering; intrusion and anomaly detection, prevention, and response; network traffic analysis; traffic classification and modeling; identifying phishing websites; program vulnerability detection; attack prediction; cyber deception; cyber threat intelligence; user behavior analysis; and imaging forensics. The success of machine learning methods in cybersecurity issues is mainly due to their ability to timely analyze huge datasets, as those generally available in the cybersecurity domain. In this way, potential problems can be detected before any damage occurs, allowing the implementation of countermeasures, such as alerts and quarantines.

4.1. Introduction to Machine Learning

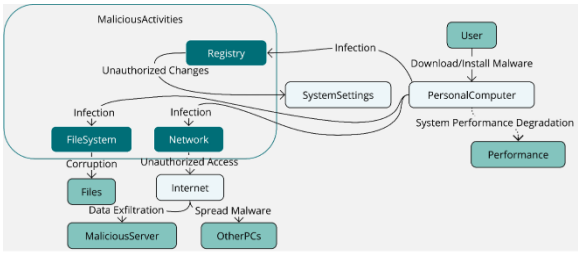
Machine learning is a specialized function that enables systems to learn from historical data and improve their performance over time on a specific problem without being explicitly programmed. Several examples of machine learning in our daily lives include chatbots that guide people around to complete tasks, optimization techniques that help delivery optimization, sentiment analysis to analyze flaming, and fake news detection. Organizations are reliant on real-time decision-making, which cannot be supported by conventional programming. The potential of machine learning has led to a surge in the number of requests for its adoption, many of which have not been fruitful because of a plethora of reasons. Cybersecurity is one area where numerous machine learning techniques have been adopted with varying degrees of success. Machine Learning utilizes computer algorithms that improve automatically through experience. A computer program is said to learn from experience with respect to some class of tasks and performance measure, if its performance at tasks in that class, as measured by the performance measure, improves with experience. In this definition, experience is defined as the task-specific experience available in the form of prior examples or tasks, and the class of tasks are all the tasks that the program is capable of performing to very high levels of performance. For example, implicit experience in the form of vast amounts of specific examples can endow a machine-learning algorithm with the ability to understand spoken, written and visual data, while tasks such as determining the number of stories in a page, answering questions online, and recognizing faces have been mastered.

4.2. Applications of Machine Learning in Cybersecurity

Machine learning has rapidly become an important weapon in the cybersecurity arsenal. The growth of cybercrime as a service and attacks on the financial systems that underpin the economy have brought urgency to bear on the problem. The current state of cybersecurity has many data backlogs with stale information. Machine learning may be able to update cyber teams to the current operations, anticipate inbound threats, mitigate those risks, and recover from the events. Machine learning may also be a substitute for scarce resources for forensics personnel.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

Fig 4 : Applications of Machine Learning in Cyber Security



For example, some machine learning systems are being deployed in IT operations to aid recovery and service restoration. Others are in use to speed incident response for alert management.

Machine learning is causing a shift in the state of play in the network and endpoint protection units at some of the biggest cybersecurity suppliers. Those organizations are doing a lot of machine learning development work and applying those capabilities across their vendor portfolios. Those vendors are not capable of using off the shelf machine learning tools to respond to the rising volume of attacks that are powered by the increased processing capabilities of cloud, the growing volume of financial data kept in corporate hands, and the rapid growth of the dark web. Security Information and Event Management platforms may be integrating machine learning models into the data pipeline to classify abnormal events according to threat types. Machine learning may enable those SIEM applications to provide alerts to cyber teams.

5. Comparative Analysis of Frameworks

This section provides a comparison of the three frameworks in order to understand their strengths and weaknesses. This would allow others to become aware of research gaps and areas for improvements, and further their own research. Also, works in senior individual studies must have an original contribution to the field of study are an important aspect of delivered pieces. Thus, an explanation of the compared aspects found to be the most relevant in the literature would give this work originality.

The main contribution to identity theft protection is a network analysis detection model. The latter model is focused primarily on transactions to detect suspicious behavior from other people who would be attempting to impersonate criminals. The proposed method is to utilize neural networking together with known transactions to detect possible potential criminals in a persona involved and martial training, but also the enhancement of the detection model. For data gathering, it is suggested to use not only previous transaction correlations provided for the neural network, but also of other "known" persons from the persona involved point of view.

In comparison to this fraud detection-centric method, the focus is on consumer protection to allow safe n cognitive information while creating a personal space. This space will create data that is for limited use and not limited from one's innermost personal being. This new concept is fundamental in the protection of the identity creation space. There are traits found not only in biometrics that conditions the attribute. The attributes must of course be to some extent also under control by the owner of the attribute, but can also be formed by authentication details found from the security of a personal identity document, or from a possible e-purse.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

Equation 2 : Comparative Performance Score of Frameworks

$$C_j = w_1 \cdot A_j + w_2 \cdot R_j - w_3 \cdot FPR_j$$

where

- C_j: Composite performance score of framework j
- A_j: Accuracy or AUC of model j
- R_j: Real-time responsiveness or latency efficiency
- FPR_j: False positive rate
- w_1, w_2, w_3: Tunable weights based on evaluation priority

5.1. Framework A: Description and Features

In the presented town house, network, economic, computer, physical, and personal security concerns surrounding identity are recognized and addressed by integrating advancements in machine learning with pre-existing solutions. The model specifies which credentials and identity attributes to protect in order to avoid misuse. Once the owner of the credential or attribute has been identified, the model can be used to protect its use or association with identity. The model has been designed to prevent or mitigate loss that occurs as a consequence of misuse, and thus encompasses all areas of identity management. By embedding it within these areas processes such as certification, authentication, access and privilege authorization, identification, verification, monitoring, and recovery in a use case specific manner, leveraging work completed in earlier phases of the framework, making it complementary to the existing area based models. Framing identity protection in recognition-protection-performance mode terms allows for complex models to be constructed that balance the trade-offs in all identities for people that undergo multiple iterations in their lifetime. Although this enrichment does not make model construction trivial, it does mean that it is more flexible. Thus it can be tuned to suit individuals some of whom are general identity abusers while others conduct crime using others' identities; there are very few negative aspects of using the new model that almost all complexity is ushered in the need for defining the trade-offs between recognition-protection-performance mode terms, with approximate methods needed to balance and tune the solutions for the new model being needed for the generalization phase of the use of the model.

5.2. Framework B: Description and Features

In this section, we shall introduce the work done. In this work, the authors designed a framework named Identity Theft Protection Neural Network (ITPNN) which used the classification and predictive capabilities of ANN's (Artificial Neural Networks) to detect identity theft attempts early in their development. The INN utilizes a high number of Sensitive Activities (SA) during the training session. It begins with many SA marked as Zero or Non-Counter SA of an Identity Theft Classification (ITC) which decrease as the current ITC classifies those activities correctly. The core ITPNN architecture is a hierarchical architecture made of a tree-shaped organization of several fifty hidden neurons 1-level heterogeneous - supervised artificial neural networks. Each of these 1-level networks performs the classification and prediction for some of the ITC classes. The ITPNN output consists of the weighted sum of the 50x1 outputs of each of the 1-level networks. Building a hierarchical architecture in such a way, some neurons get trained only to focus on some specific classes of the ITC, while others neurons get focused on other classes. The detection of identity theft is performed by identifying the significant deviations from the usual characteristics of the activity SA of the individual identity being analyzed.

The INN predictions, when detecting identity theft, are not just about pointing out a theft. It includes the prediction of the time and the IP address of the theft. The output of the ITPNN to perform these types of

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

predictions and detection of anomalies is a two-layer network, with the first layer being 1-level ANN that classifies one of the ITC pre-specified classes only. The second layer uses the output of the 1-level ANN as the unique weighting factor in a 1x50 weighted summation in order to predict the SA time of occurrence. In order to be able to predict the IP address from which the identity theft occurs, an intelligent architectural solution is proposed, where two new 1-level ANNs are added to the design of the 2-layer ITPNN.

5.3. Framework C: Description and Features

The proposed framework is able to predict future course of actions based on the observed behavior of the users without any login and social graph access. It comprises three modules. The first is a user activity tracker, which examines the click patterns and operates separately for each individual user. It notices variations in behavior, such as hitting a different subdomain more frequently or less frequently than average or accessing a new sub-domain and predicts the probability of the user hitting the different sub-domain group in the future. The second is a classifier which illustrates the future course of action without prior behavior knowledge. The last one is a domain controller, which suggests the users by mapping them to the sub-domain with the highest predicted access probability, and updates its knowledge using the suggestions made.

The primary goal is to anticipate future usage patterns for visitors accessing a group of subdomains during the time period when the click analysis cannot be conducted. It is sometimes impossible to notify a user about a possible account hacking immediately. As there is no knowledge of prior behavior, the classifier uses generic popular domains for user classification and those domains would have a default list of noticeable activities that will not be considered while tracking and predicting actions, e.g., login, account validating, or domain selection actions. Keeping track and possibly predicting a user's clicking activity on various sub-domains of a specific web site has numerous applications, on which we only touch very lightly. Therefore, the sub-domains with the lowest predicted visit probability would be suggested for that user, although it would be expected to get fewer suggestions at this stage since any prediction will be relatively wont.

6. Machine Learning Algorithms for Identity Theft Protection

Machine learning has the potential to revolutionize the field of identity theft protection frameworks with trusted identity management. A survey was conducted of machine learning algorithms used for identity theft prevention and detection. Based on the analysis, a large number of supervised classifiers were used, with random forests and neural networks being the most successful ones. The second most popular category are unsupervised learning algorithms, employed for detection purposes. Other classifiers, such as regression and conditional random fields were also reviewed. These algorithms range from simple regression models to more complicated and resource hungry methods. Reinforcement learning is a less popular way to develop an identity theft detection framework.

This section describes the supervised, unsupervised and reinforcement learning algorithms utilized for identity theft protection, being the most commonly adopted categories of machine learning algorithms in academic research. The list of supervised learning algorithms is summarized. Some techniques were employed by more than one source, in which case the results are combined. In the case of two sources employing the same method with different parameters, this source is marked as relevant. The relevant paper provides more information about the supervised method’s different parameters. In addition to supervised classification, the K-nearest neighbors algorithm was actually used for predicting. The second most popular way to develop an identity theft detector refers to its inability to convert previous data in supervision and supervised learning questioning the predictive power of such previous data. Thus, many works opted for an unsupervised manner to develop identity theft detection. Also reported in the earlier literature are techniques

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

within the predicative category labeled as NARX, Wavelet, Genetic Algorithms and Decision Trees. Typically, however, the focus is on the earlier section where supervised methods are elaborated upon, and detect earlier intelligence-based identity theft using a single enterprise data.

6.1. Supervised Learning Algorithms

The supervised machine learning algorithm is the most important category of machine learning. This learning algorithm creates a model from a training dataset using a supervised learning environment. The model is later fed with a second dataset to test the output score of the model. The performance and accuracy of the model is important for a supervised machine learning algorithm. After the evaluation, the machine learning algorithm test selects the best-performing model and uses that for further testing. The accuracy of the input training dataset directly affects the efficiency of the output.

The quality of the data used to train supervised machine learning determines how accurate and efficient a model can be. The better the input, the more accurate the model. Even with large amounts and data, poor quality of data leads a training model to be inefficient. Supervised machine learning achieves tasks by creating a function based on mapping input to the output. Translating input to output decreases the possibility of error when previously unseen data is encountered. Classification tasks and regression tasks are two categories of supervised machine learning.

Pattern recognition of objects according to the training dataset is called classification. The output during the classification task is discrete labels. Classification is used on documents, audio and images where the output can be categories. A function that evaluates input by regression performs a supervised machine learning task. The output relabels the real values or predicts a finite number of real numbers. Regression is mainly used to predict the future of the input data. The classification prediction relies on a decoder and a softmax layer that mimic the probabilities to determine a class. Random forest, logistic regression, Naive Bayes, artificial neural networks and others are different with their implementation yet are supervised algorithms.

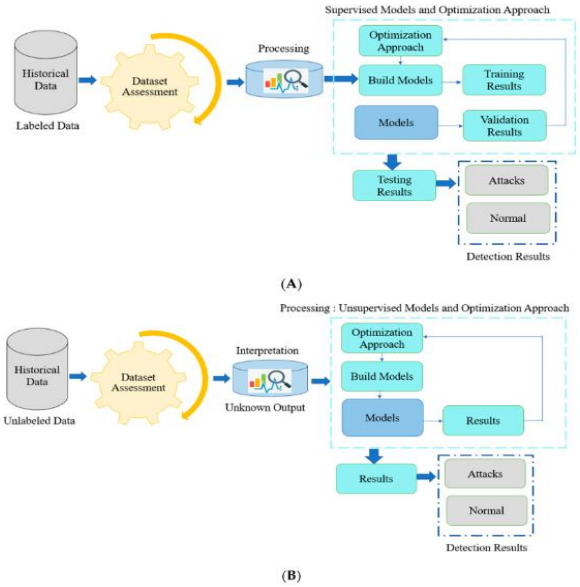


Fig 5 : Supervised and Unsupervised Models for Detecting Attacks

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

6.2. Unsupervised Learning Algorithms

Unsupervised learning algorithms learn from input data without labeled responses. While developing a model using unsupervised learning algorithms, the target variable is unknown; hence models are used to describe the structure in the input data. The goal of unsupervised learning is to find hidden structure in the unlabeled data. Clustering and Association are prominent examples of unsupervised learning. Clustering models group data into different clusters based on their similarities, while Association rules are used to discover the probability of some combinations in a dataset. Unsupervised learning is important for identity theft protection because data is typically unlabeled and does not have any response assigned to it. For unlabeled data, unsupervised algorithms are the most popular method for extracting interesting hidden patterns, making such algorithms valuable in an identity theft prevention context. Autoencoders are a type of unsupervised machine learning method based on neural networks and aim to encode the input data as output. The unsupervised learning model is trained to compress the input data into a lower dimensional representation and is forced to decode the compressed representation accurately. One of the main key advantages of using autoencoders for detecting abnormal patterns in data is that it is not necessary to explicitly indicate which data points represent anomalies.

Different machine learning based approaches like clustering of financial transactions and abnormal pattern detection using machine learning models are proposed to detect individuals undergoing identity theft. One of the goals of identity protection is to expedite concerted rescue actions like cancelling credit cards or freezing bank accounts once a theft has been detected. Since successful fusion of alerts and notifications is critical for timely notifications, a semi-supervised classification panel composed of autoencoders, classifiers and some logistic regression models can help optimize the identity protection.

6.3. Reinforcement Learning Algorithms

Reinforcement learning is a machine learning paradigm often considered as a third category, distinct from supervised and unsupervised learning. In RL, an agent learns an optimal policy mapping from states of the environment to actions so as to maximize the expected total return collected over time. Success in reinforcement learning depends on exploration of the environment, as well as on balancing that exploration with exploitation of the known. RL is also a key component in deep reinforcement learning systems.

Reinforcement learning has recently emerged as an extremely successful paradigm for learning optimal strategies in a variety of complex decision-making problems. Advanced methods that incorporate concepts from deep learning with traditional RL, or deep reinforcement learning, have set state-of-the-art results on a range of challenging problems: They have mastered complex traversal and strategy games, using graphics as the environment to explore decisions and elements related to exploration, as well as key decision-making problems in network management, such as learning to route packets through a network switching fabric or learning where to place various types of content on servers to minimize latencies or maximina costs. One natural application domain to which RL is already naturally well-suited to model is deception detection. Indeed, problems focused on security or where multiple competing agents act based on private information are common in an RL setting, as in the key problem of anomaly detection.

7. Evaluation Metrics for Frameworks

The evaluation of machine learning models is conceptually straightforward. Various metrics, called evaluation metrics, are computed for a trained model, and based on them, the model is deemed suitable for a certain task or not. Usually, domains or problems where such models are employed have existing

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

evaluation metrics. Therefore, a naive approach to this problem is to adopt generic evaluation metrics from the core problem and use them as the basic evaluation metric, for example, the accuracy and precision for classification tasks. However, while this typically suffices, there are instances where naive approaches are inadequate, essentially due to the unique nature of the applied models. Consideration should be lent to the types of models being evaluated, the kind of security data being modeled, and the interpretations of these models.

To use a comparative analysis of identity theft protection frameworks enhanced by ML algorithms for the problem of IDT prediction as our business case, this study has integrated various core and domain-specific evaluation metrics into a set of evaluation metrics. These metrics are applied to several types of ML and cyber threat detection tasks, such as network intrusion detection and speculative execution attack detection. This investigation into the evaluation metrics is not intended to serve as a specific utility for this reconsideration study, whose scope is much wider. Instead, it expands on prior work done by other publications, seriously considering evaluation metrics for ML.

Various evaluation metrics from different domains or studies are integrated into a refined evaluation metric set that includes accuracy, precision, recall, F1 score, runtime, and memory requirements, applying it to a set of common identity theft prevention tasks. This refined evaluation metric set can be used as a guideline for designing data-driven IDT prediction research with successful outcomes, also considering considerations concerning the structure of data-driven prediction models and the datasets they utilize.

7.1. Accuracy and Precision

The performance of the proposed identity theft protection frameworks, as in most machine learning applications, is usually evaluated based on how closely the results of the model match the actual predictions. The ratio of made predictions to the actual predictions is the accuracy, while precision focuses primarily on false positives, and identifies the fraction of results expected true positives correctly predicted.

For a binary classification, both metrics can be defined based on the standard contingency table below:

Predicted

1 0

_____

1 | TP FN |

Actual 0 | FP TN |

Where TP is the count of true positives (actual/positive; predicted positive), TN is the count of true negatives (actual/negative; predicted negative), FP is the count of false positives (actual/negative; predicted positive), and FN is the count of false negatives (actual/positive; predicted negative). Note that the performance of the proposed frameworks was evaluated not only based on accuracy, but primarily on precision and recall since in practice, accurate detection of frauds is much more critical.

Accuracy = (TP + TN)/(TP + FP + TN + FN)

Precision = TP/(TP + FP)

Where accuracy is the proportion of predictions that are correct across all classes, while precision calculates the proportion of positive identifications that were actually correct. One of the main problems with accuracy is that it can be misleading when the class distribution is very imbalanced. With a deeper look into the trade-offs between accuracy and precision, it is important to understand the limitations of classification accuracy as the sole metric because it does not explore the area of confusion, making the user blindly apply classifiers without a comprehensive consideration of what they are doing and what their limitations are.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

7.2. Recall and F1 Score

Model evaluation metrics such as accuracy, precision, F1 score, and recall are used to evaluate user identity detection and fraud detection methodologies. To create the confusion matrix, let's consider a true positive as a detected fraud; a false positive is defined as a legit account that has been incorrectly detected as a fraudulent account; a false negative is defined as a fraudulent account that has been incorrectly detected as a legit user; and a true negative is defined as a legit account that has been correctly identified as a lawful user. The equations for recall and F1 score are presented below, along with the respective explanations.

The recall measures the ability of a model to find all the relevant cases within the data set, meaning that if a model has a low recall rate, it may not be able to detect important frauds and thus produce a low Fraud Detection Rate. In recent years, the F1 score has gained traction as another measure that also takes precision and recall into account. We used the F1 score only when the classes were imbalanced. The F1 score is the harmonic mean of precision and recall. The F1 score helps in figuring out whether the model's precision is increasing as well as its recall. The F1 score, with lower and upper bounds at precision and recall respectively, gives a score higher than, or equal to, the individual precisions and recalls, only when they are both equal. This characteristic makes the F1 score balance precision and recall when the class distribution is imbalanced.

7.3. Computational Efficiency

Frameworks with high accuracy and low error rates are often identified as the most effective implementations of IT protection operations. However, the most impactful aspect of performance is the time logical overhead in completing these badge operations. In outlining the key elements within this important dimension of performance, it has been posited that "Computational efficiency is a vital property of machine learning as it shows how long a machine learning algorithm takes to process data." Consequently, an important measure of ML technique performance is the time it takes to process a test suite. This represents a combination of the build time for the ML algorithm prototype and the time taken to recognize each subsequent event within the data stream, both of which are important components of ML algorithm performance which requires careful analysis. As a function of detecting high volumes of attacks within limited time frames, prototype recognition times must be kept to a minimum to ensure that as many of the reported attacks as possible generate alerts.

Understanding the factors that influence concurrent label recognition speeds can help to predict an upper limit on how quickly the ML algorithm can respond to attack events. Design implementations which can accurately perform a multi-class labelling task on websites restricted to a limited sub-set of behaviours should be sought. Considerable problems are associated with scaling the supervised class number up and down due to the effect on classification accuracy. The significant optimizing for multi-class tasks employed by standard ML implementations means that generalization performance suffers, and the time taken to identify every data point from the test stream may exceed levels for acceptable production systems for anything other than small relative class label sets.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

Equation 3 : Adaptive Detection via Online Learning $\theta_{t+1} = \theta_t - \eta \nabla \mathcal{L}(f_{\theta_t}(X_t), y_t)$

where

- θ_{t+1}: Updated model parameters after new data at time t
- η: Learning rate
- $\mathcal{L}$: Loss function (e.g., log loss for binary classification)
- y_t: True label for sample X_t

8. Conclusion

The contemporary dependence on digital mediums has laid the groundwork for various cybercrimes and threats caused by technology. Internet access from anywhere, at any time, has become integral to the daily activities of every social sector. However, with this increasing digital interaction, the prevalence of cybercrimes has also increased; specifically, the rate of identity theft is on the rise. While data protection strategies have progressed, the number of security problems continues to mount. Therefore, there is an essential need to safeguard sensitive information from cyber offenders through the foundation of reliable detection models. The automated learning methods of machine learning provide an opportunity to assist the information protection area by helping to generate reliable detection models that are effective in detecting various types of security issues. This work analyzes various ML-based identity theft protection model implementations. The study discusses the process of data collection and preprocessing, and model evaluation. We implement models to assess the impact of model choice on the ability to detect identity theft. This is a broad overview of various machine learning-based identity theft protection models.

After the exploration of the contents and ideas presented in this study, we conclude that while various strategies have been proposed to facilitate detection and prevention, much work is still left to be done. Each system proposed has its advantages and disadvantages, and further work would be needed to sort out the factors governing the performance. There is also the need for further development of longer time frame models that account for the longitudinal effects of identity theft, as well as the analysis of real-world versus test data for models that depend on synthetic data. Further incorporation of ethical and legal factors surrounding identity theft and the use of machine learning in this domain is also required.

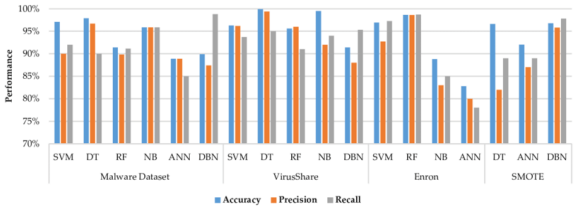


Fig 6 : Analysis of Malware Detection using Machine Learning

8.1. Final Thoughts and Future Directions

The different frameworks we describe protect a person's identity against identity thieves by monitoring such sensitive information and facts, such as credit cards, debit cards, driver's license, births, deaths, addresses, social security numbers, passport numbers, account numbers, bank account balances, bank name, etc. Inconsistencies in some frameworks are fixed by implementing some technological advances in the design. All these implementations with machine learning technologies make all frameworks really perform very well in well time mode, dealing with problems on a proactive basis. In a few cases, when machine

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

learning technology has not been consistent in training the machines, security at a monitoring level has been employed and all these frameworks play extra measure in after-time dealing with the problems. Some advanced and innovative approaches, such as Trusted Computing, Privacy-Aware Security, Block Chain Approach, Genetic Algorithms, and Cloud Computing, have also been described as being in the initial research stages. They are expected to be of help in future developments.

We have compared frameworks that deal with localized aspects of identity theft, such as the social security number, credit card, or bank fraud, and have done an initial effort to incorporate new research levels and further discuss some research directions in framework introspection. However, our effort is small compared to the areas of application inquiry, which is on the demand side. We hope to raise awareness of readers and researchers in the privacy and security lives of achievable capabilities for those affected, and on the development of a more global framework of models for the generation of thorough and grounded content to explain the cycle of outcomes. We expect further research to be motivated towards a new series of layered and more refined research agendas. We also point out that practitioners have a role to play in linking design and moderation so as to help improve end-of-chain technology.

9. References

[1] Sondinti, K., & Reddy, L. (2024). Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth. Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth (December 17, 2024).

[2] Venkata Krishna Azith Teja Ganti ,Kiran Kumar Maguluri ,Dr. P.R. Sudha Rani (2024). Neural Network Applications in Understanding Neurodegenerative Disease Progression. Frontiers in HealthInformatics, 13 (8) 471-485

[3] Sambasiva Rao Suura. (2024). Integrating Generative AI into Non-Invasive Genetic Testing: Enhancing Early Detection and Risk Assessment. Utilitas Mathematica, 121, 510–522. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2046

[4] Venkata Narasareddy Annapareddy. (2024). Harnessing AI Neural Networks and Generative AI for Optimized Solar Energy Production and Residential Battery Storage Management. Utilitas Mathematica, 121, 501–509. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2045

[5] Kannan, S. Revolutionizing Agricultural Efficiency: Leveraging AI Neural Networks and Generative AI for Precision Farming and Sustainable Resource Management.

[6] Harish Kumar Sriram. (2024). Leveraging AI and Machine Learning for Enhancing Secure Payment Processing: A Study on Generative AI Applications in Real-Time Fraud Detection and Prevention. Utilitas Mathematica, 121, 535–546. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2048

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

[7] Karthik Chava. (2024). Harnessing Generative AI for Transformative Innovations in Healthcare Logistics: A Neural Network Framework for Intelligent Sample Management. Utilitas Mathematica, 121, 547–558. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2049

[8] Komaragiri, V. B. The Role of Generative AI in Proactive Community Engagement: Developing Scalable Models for Enhancing Social Responsibility through Technological Innovations.

[9] Siramgari, D. (2024). Metadata Mastery : Charting the Future of Technical and Data Catalogs in the Era of AI and Cloud. Zenodo. https://doi.org/10.5281/ZENODO.14533320

[10] Daruvuri, R., Patibandla, K., & Mannem, P. (2024). Leveraging unsupervised learning for workload balancing and resource utilization in cloud architectures. International Research Journal of Modernization in Engineering Technology and Science, 6(10), 1776-1784.

[11] Ganesan, P. (2024). AI-Powered Sales Forecasting: Transforming Accuracy and Efficiency in Predictive Analytics. J Artif Intell Mach Learn & Data Sci 2024, 2(1), 1213-1216.

[12] Siramgari, D. R., & Sikha, V. K. (2024). From Raw Data to Actionable Insights: Leveraging LLMs for Automation. Zenodo. https://doi.org/10.5281/ZENODO.14128827

[13] Patibandla, K., Daruvuri, R., & Mannem, P. (2024). Streamlining workload management in AI-driven cloud architectures: A comparative algorithmic approach. International Research Journal of Engineering and Technology, 11(11), 113-121.

[14] Ganesan, P. (2024). Cloud-Based Disaster Recovery: Reducing Risk and Improving Continuity. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-E162. DOI: doi. org/10.47363/JAICC/2024 (3) E162 J Arti Inte & Cloud Comp, 3(1), 2-4.

[15] Chaitran Chakilam. (2024). Revolutionizing Genetic Therapy Delivery: A Comprehensive Study on AI Neural Networks for Predictive Patient Support Systems in Rare Disease Management. Utilitas Mathematica, 121, 569–579. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2051

[16] Murali Malempati. (2024). Generative AI-Driven Innovation in Digital Identity Verification: Leveraging Neural Networks for Next-Generation Financial Security. Utilitas Mathematica, 121, 580–592. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2052

[17] Challa, S. R., Challa, K., Lakkarasu, P., Sriram, H. K., & Adusupalli, B. (2024). Strategic Financial Growth: Strengthening Investment Management, Secure Transactions, and Risk Protection in the Digital Era. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 97-108.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

[18] Nuka, S. T. (2024). Exploring AI and Generative AI in Healthcare Reimbursement Policies: Challenges, Ethical Considerations, and Future Innovations. International Journal of Medical Toxicology and Legal Medicine, 27(5), 574-584.

[19] Burugulla, J. K. R. (2024). The Future of Digital Financial Security: Integrating AI, Cloud, and Big Data for Fraud Prevention and Real Time Transaction Monitoring in Payment Systems. MSW Management Journal, 34(2), 711-730.

[20] Intelligent Supply Chain Optimization: AI Driven Data Synchronization and Decision Making for Modern Logistics. (2024). MSW Management Journal, 34(2), 804-817.

[21] Pamisetty, V. (2024). AI Powered Decision Support Systems in Government Financial Management: Transforming Policy Implementation and Fiscal Responsibility. Journal of Computational Analysis & Applications, 33(8).

[22] Revolutionizing Automotive Manufacturing with AI-Driven Data Engineering: Enhancing Production Efficiency through Advanced Data Analytics and Cloud Integration . (2024). MSW Management Journal, 34(2), 900-923.

[23] Leveraging Deep Learning, Neural Networks, and Data Engineering for Intelligent Mortgage Loan Validation: A Data-Driven Approach to Automating Borrower Income, Employment, and Asset Verification. (2024). MSW Management Journal, 34(2), 924-945.

[24] Lahari Pandiri, Subrahmanyasarma Chitta. (2024). Machine Learning-Powered Actuarial Science: Revolutionizing Underwriting and Policy Pricing for Enhanced Predictive Analytics in Life and Health Insurance . South Eastern European Journal of Public Health, 3396–3417. https://doi.org/10.70135/seejph.vi.5903

[25] Mahesh Recharla, (2024). The Role of Agentic AI in Next-Generation Drug Discovery and Automated Pharmacovigilance for Rare and Neurological Diseases. Frontiers in Health Informatics, Vol. 13(8), 4999-5014

[26] Botlagunta Preethish Nandan. (2024). Revolutionizing Semiconductor Chip Design through Generative AI and Reinforcement Learning: A Novel Approach to Mask Patterning and Resolution Enhancement. International Journal of Medical Toxicology and Legal Medicine, 27(5), 759–772. https://doi.org/10.47059/ijmtlm/V27I5/096

[27] Balaji Adusupalli,. (2024). Agentic AI-Driven Identity and Access Management Framework for Secure Insurance Ecosystems . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 2794–2814. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/2225

[28] Paleti, S., Pamisetty, V., Challa, K., Burugulla, J. K. R., & Dodda, A. (2024). Innovative Intelligence Solutions for Secure Financial Management: Optimizing Regulatory Compliance,

Transaction Security, and Digital Payment Frameworks Through Advanced Computational Models. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 125-136.

[29] Pallav Kumar Kaulwar,. (2024). Agentic Tax Intelligence: Designing Autonomous AI Advisors for Real-Time Tax Consulting and Compliance. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 2757–2775. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/2224

[30] AI-Powered Revenue Management and Monetization: A Data Engineering Framework for Scalable Billing Systems in the Digital Economy . (2024). MSW Management Journal, 34(2), 776-787.

[31] Abhishek Dodda. (2023). Digital Trust and Transparency in Fintech: How AI and Blockchain Have Reshaped Consumer Confidence and Institutional Compliance. Educational Administration: Theory and Practice, 29(4), 4921–4934. https://doi.org/10.53555/kuey.v29i4.9806

[32] Singireddy, J. (2024). Deep Learning Architectures for Automated Fraud Detection in Payroll and Financial Management Services: Towards Safer Small Business Transactions. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 75-85.

[33] Sneha Singireddy. (2024). Leveraging Artificial Intelligence and Agentic AI Models for Personalized Risk Assessment and Policy Customization in the Modern Insurance Industry: A Case Study on Customer-Centric Service Innovations . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 2532–2545. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/2163

[34] Siramgari, D. (2024). Building the Future: Unveiling the AI Agent Stack. Zenodo. https://doi.org/10.5281/ZENODO.14533422

[35] Mannem, P., Daruvuri, R., & Patibandla, K. (2024). Leveraging supervised learning in cloud architectures for automated repetitive tasks. International Journal of Innovative Research in Science, Engineering and Technology, 13(11), 18127-18136.

[36] Ganesan, P. (2023). Revolutionizing Robotics with AI. Machine Learning, and Deep Learning: A Deep Dive into Current Trends and Challenges. J Artif Intell Mach Learn & Data Sci, 1(4), 1124-1128.

[37] The Future of Banking and Lending: Assessing the Impact of Digital Banking on Consumer Financial Behavior and Economic Inclusion. (2024). MSW Management Journal, 34(2), 731-748.

[38] Satyaveda Somepalli. (2024). Leveraging Technology and Customer Data to Conserve Resources in the Utility Industry: A Focus on Water and Gas Services. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.13884891

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

[39] Patibandla, K., & Daruvuri, R. (2023). Reinforcement deep learning approach for multi-user task offloading in edge-cloud joint computing systems. International Journal of Research in Electronics and Computer Engineering, 11(3), 47-58.

[40] Singireddy, S., Adusupalli, B., Pamisetty, A., Mashetty, S., & Kaulwar, P. K. (2024). Redefining Financial Risk Strategies: The Integration of Smart Automation, Secure Access Systems, and Predictive Intelligence in Insurance, Lending, and Asset Management. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 109-124.

[41] Intelligent Technologies for Modern Financial Ecosystems: Transforming Housing Finance, Risk Management, and Advisory Services Through Advanced Analytics and Secure Cloud Solutions. (2024). MSW Management Journal, 34(2), 953-971.

[42] Abhishek Dodda. (2023). NextGen Payment Ecosystems: A Study on the Role of Generative AI in Automating Payment Processing and Enhancing Consumer Trust. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 430-463. https://ijfin.com/index.php/ijfn/article/view/IJFIN_36_06_017

[43] Hara Krishna Reddy Koppolu, Venkata Bhardwaj Komaragiri, Venkata Narasareddy Annapareddy, Sai Teja Nuka, & Anil Lokesh Gadi. (2023). Enhancing Digital Connectivity, Smart Transportation, and Sustainable Energy Solutions Through Advanced Computational Models and Secure Network Architectures. Journal for ReAttach Therapy and Developmental Diversities, 6(10s(2), 1905–1920. https://doi.org/10.53555/jrtdd.v6i10s(2).3535

[44] Kaulwar, P. K. (2023). Tax Optimization and Compliance in Global Business Operations: Analyzing the Challenges and Opportunities of International Taxation Policies and Transfer Pricing. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 150-181.

[45] Paleti, S. Agentic AI in Financial Decision-Making: Enhancing Customer Risk Profiling, Predictive Loan Approvals, and Automated Treasury Management in Modern Banking.

[46] Adusupalli, B., & Insurity-Lead, A. C. E. The Role of Internal Audit in Enhancing Corporate Governance: A Comparative Analysis of Risk Management and Compliance Strategies.

[47] Botlagunta Preethish Nandan, & Subrahmanya Sarma Chitta. (2023). Machine Learning Driven Metrology and Defect Detection in Extreme Ultraviolet (EUV) Lithography: A Paradigm Shift in Semiconductor Manufacturing. Educational Administration: Theory and Practice, 29(4), 4555–4568. https://doi.org/10.53555/kuey.v29i4.9495

[48] Mahesh Recharla, Sai Teja Nuka, Chaitran Chakilam, Karthik Chava, & Sambasiva Rao Suura. (2023). Next-Generation Technologies for Early Disease Detection and Treatment: Harnessing Intelligent Systems and Genetic Innovations for Improved Patient Outcomes. Journal for ReAttach

Therapy and Developmental Diversities, 6(10s(2), 1921–1937. https://doi.org/10.53555/jrtdd.v6i10s(2).3537

[49] Lahari Pandiri, & Subrahmanyasarma Chitta. (2023). AI-Driven Parametric Insurance Models: The Future of Automated Payouts for Natural Disaster and Climate Risk Management. Journal for ReAttach Therapy and Developmental Diversities, 6(10s(2), 1856–1868. https://doi.org/10.53555/jrtdd.v6i10s(2).3514

[50] Anil Lokesh Gadi. (2023). Engine Heartbeats and Predictive Diagnostics: Leveraging AI, ML, and IoT-Enabled Data Pipelines for Real-Time Engine Performance Optimization. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 210-240. https://ijfin.com/index.php/ijfn/article/view/IJFIN_36_06_010

[51] Paleti, S., Pamisetty, V., Challa, K., Burugulla, J. K. R., & Dodda, A. (2024). Innovative Intelligence Solutions for Secure Financial Management: Optimizing Regulatory Compliance, Transaction Security, and Digital Payment Frameworks Through Advanced Computational Models. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 125-136.

[52] Pamisetty, A. (2022). Enhancing Cloud native Applications WITH Ai AND Ml: A Multicloud Strategy FOR Secure AND Scalable Business Operations. Migration Letters, 19(6), 1268-1284.

[53] Reddy, J. K. (2024). Leveraging Generative AI for Hyper Personalized Rewards and Benefits Programs: Analyzing Consumer Behavior in Financial Loyalty Systems. J. Electrical Systems, 20(11s), 3647-3657.

[54] Nuka, S. T. (2024). The Future of AI Enabled Medical Device Engineering: Integrating Predictive Analytics, Regulatory Automation, and Intelligent Manufacturing. MSW Management Journal, 34(2), 731-748.

[55] Malempati, M., Sriram, H. K., Kaulwar, P. K., Dodda, A., & Challa, S. R. Leveraging Artificial Intelligence for Secure and Efficient Payment Systems: Transforming Financial Transactions, Regulatory Compliance, and Wealth Optimization.

[56] Chakilam, C. (2023). Leveraging AI, ML, and Generative Neural Models to Bridge Gaps in Genetic Therapy Access and Real-Time Resource Allocation. Global Journal of Medical Case Reports, 3(1), 1289. https://doi.org/10.31586/gjmcr.2023.1289

[57] Komaragiri, V. B. (2024). Data-Driven Approaches to Battery Health Monitoring in Electric Vehicles Using Machine Learning. International Journal of Scientific Research and Management (IJSRM), 12(01), 1018-1037.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1080-1101

[58] Chava, K., & Saradhi, K. S. (2024). Emerging Applications of Generative AI and Deep Neural Networks in Modern Pharmaceutical Supply Chains: A Focus on Automated Insights and Decision-Making.

[59] Sriram, H. K. (2023). Harnessing AI Neural Networks and Generative AI for Advanced Customer Engagement: Insights into Loyalty Programs, Marketing Automation, and Real-Time Analytics. Educational Administration: Theory and Practice, 29(4), 4361-4374.

[60] Kannan, S., & Seenu, A. (2024). Advancing Sustainability Goals with AI Neural Networks: A Study on Machine Learning Integration for Resource Optimization and Environmental Impact Reduction. management, 32(2).

[61] Annapareddy, V. N., & Sudha Rani, P. (2024). AI and ML Applications in RealTime Energy Monitoring and Optimization for Residential Solar Power Systems. Available at SSRN 5116062.

[62] Suura, S. R. (2024). Generative AI Frameworks for Precision Carrier Screening: Transforming Genetic Testing in Reproductive Health. Frontiers in Health Informa, 4050-4069.

[63] Sondinti, K., & Reddy, L. (2024). Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth. Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth (December 17, 2024).

[64] Polineni, T. N. S., Ganti, V. K. A. T., Maguluri, K. K., & Rani, P. S. (2024). AI-Driven Analysis of Lifestyle Patterns for Early Detection of Metabolic Disorders. Journal of Computational Analysis and Applications, 33(8).

[65] Danda, R. R., Nampalli, R. C. R., Sondinti, L. R. K., Vankayalapati, R. K., Syed, S., Maguluri, K. K., & Yasmeen, Z. (2024). Harnessing Big Data and AI in Cloud-Powered Financial Decision-Making for Automotive and Healthcare Industries: A Comparative Analysis of Risk Management and Profit Optimization.

[66] Maguluri, K. K., Ganti, V. K. A. T., & Subhash, T. N. (2024). Advancing Patient Privacy in the Era of Artificial Intelligence: A Deep Learning Approach to Ensuring Compliance with HIPAA and Addressing Ethical Challenges in Healthcare Data Security. International Journal of Medical Toxicology & Legal Medicine, 27(5).