AI-DRIVEN COMPETITIVE INTELLIGENCE AND NEXT-GENERATION SECURITY

Editors:
Suneeta Satpathy
Sachi Nandan Mohanty
Subhendu Kumar Pani

Bentham Books

Applied Artificial Intelligence in Data Science, Cloud Computing and IoT Frameworks

(Volume 4)

AI-Driven Competitive Intelligence and Next-Generation Security

Edited by

Suneeta Satpathy
Center For Cybersecurity, SoA Deemed to be University, Bhubaneswar, Odisha, India

Sachi Nandan Mohanty
School of Computer Science & Engineering, VIT-AP University, Andhra Pradesh, India

&

Subhendu Kumar Pani
Computer Science & Engineering Krupajal Engineering College BPUT, Odisha, India

Applied Artificial Intelligence in Data Science, Cloud Computing and IoT Frameworks

(Volume 4)

AI-Driven Competitive Intelligence and Next-Generation Security

Editors: Suneeta Satpathy, Sachi Nandan Mohanty and Subhendu Kumar Pani

ISSN (Online): 3029-2247

ISSN (Print): 3029-2255

ISBN (Online): 979-8-89881-213-3

ISBN (Print): 979-8-89881-214-0

ISBN (Paperback): 979-8-89881-215-7

First published in 2025.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

FOREWORD

The integration of Artificial Intelligence (AI) with Data Science, Cloud Computing, and the Internet of Things (IoT) is transforming the way organizations derive insights, drive innovation, and secure digital infrastructures. In this fourth volume, Applied Artificial Intelligence in Data Science, Cloud Computing, and IoT Frameworks: AI-Driven Competitive Intelligence and Next-Generation Security, the editors present a comprehensive exploration of AI's role in shaping competitive intelligence and enhancing cybersecurity.

AI-driven frameworks are redefining competitive intelligence by uncovering hidden patterns, predicting trends, and enabling strategic decision-making at unprecedented speed and scale. Simultaneously, the expansion of connected systems has introduced increasingly sophisticated cyber threats. This volume highlights how AI serves as both a proactive defense mechanism and an enabler of secure, adaptive digital ecosystems.

The chapters bring together cutting-edge research and practical applications, offering insights across business intelligence, cloud platforms, IoT networks, and security solutions. They provide readers with a clear understanding of AI's dual potential: driving innovation while fortifying next-generation security frameworks.

This volume serves as an essential resource for researchers, industry leaders, and policymakers aiming to harness AI in a responsible and strategic manner. By highlighting AI's profound influence on contemporary technologies, it provides a clear framework for building intelligent, secure, and sustainable digital ecosystems. I applaud the editors and contributors for assembling a forward-thinking collection that not only drives innovation but also enriches the understanding of AI's critical role in shaping the future of competitive intelligence and next-generation security.

Ming Yang
Kennesaw State University
USA

PREFACE

In today's hyper-connected and rapidly evolving global economy, the ability to harness artificial intelligence (AI) for competitive intelligence has become a cornerstone of strategic decision-making in business and finance. Organizations increasingly rely on advanced AI and machine learning (ML) techniques to not only analyze vast volumes of structured and unstructured data but also to anticipate market trends, optimize operations, and maintain a competitive edge. Equally critical is the next-generation security landscape, where sophisticated cyber threats challenge enterprises, financial institutions, and governments to adopt resilient, intelligent defense mechanisms.

This volume, **AI-Driven Competitive Intelligence and Next-Generation Security**, brings together a collection of research contributions, case studies, and applied frameworks that explore the convergence of AI, data analytics, and cybersecurity. The chapters cover a diverse range of topics, including predictive financial modeling, automated market analysis, fraud detection, risk assessment, and AI-enabled threat intelligence. By bridging the domains of business intelligence, financial analytics, and cybersecurity, the volume highlights innovative methodologies that not only enhance decision-making but also safeguard critical assets in an increasingly digital ecosystem.

We believe this volume will serve as a valuable resource for researchers, practitioners, and policymakers seeking to understand the transformative potential of AI in shaping competitive strategies while addressing emerging security challenges. The insights presented here reflect the collective expertise of leading scholars and industry professionals, providing readers with practical approaches and forward-looking perspectives that will drive sustainable growth and resilient security in the digital age.

Suneeta Satpathy
Center For Cybersecurity, SoA Deemed to be University
Bhubaneswar, Odisha, India

Sachi Nandan Mohanty
School of Computer Science & Engineering
VIT-AP University, Andhra Pradesh, India

&

Subhendu Kumar Pani
Computer Science & Engineering, Krupajal Engineering College BPUT
Odisha, India

List of Contributors

A. Ezil Sam Leni	Alliance School of Advanced Computing, Alliance University, Karnataka, India
Akhand Tiwari	Department of Commerce, CHRIST University, Lavasa Campus, Pune, India
Anjaiah Adepu	Department of CSE, IC Polytechnic, Maulana Azad National Urdu University, India
Amjan Shaik	Department of CSE, St. Peter's Engineering College, Hyderabad, Telangana, India
Akhil Singampalli	Department of Computer Science and Engineering, Vignan's Institute of Information Technology, India
Anil Pise	Cumulus Solutions, Johannesburg, South Africa
Arushi Sharma	Department of Commerce, CHRIST University, Lavasa Campus, Pune, India
Aryan Gupta	Department of Commerce, CHRIST University, Lavasa Campus, Pune, India
Bikash Chandra Naik	School of Computer Science and Engineering, Odisha University of Technology and Research, Bhubaneswar, India
Blesson Varghese James	Department of Commerce, CHRIST University, Lavasa Campus, Pune, India
D. Gousiya Begum	Department of CSE, BEST Innovation University (BESTIU), Andhra Pradesh, India
Dharma Teja Singampalli	Sagility, Bangalore, India
Gurpreet Singh Chhabra	Computer Science and Engineering, Gandhi Institute of Technology and Management, Vishakhapatnam, India
Jyotirmayee Rautaray	Department of Computer Science & Engineering, Odisha University of Technology and Research, Bhubaneswar, Odisha, India
Kavin Velavan G.	Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India
K. Nagajyothi	R&D, BEST Innovation University (BESTIU), Andhra Pradesh, India
Lijo Thomas	Department of Management, CHRIST University, Pune Lavasa Campus, India
Lalmohan Pattnaik	Sri Sri University, Cuttack, Odisha, India
Meenakshi Kandpal	School of Computer Science and Engineering, Odisha University of Technology and Research, Bhubaneswar, India
Mano Paul P.	COE in iOS App Development, Dept of CSE, Alliance University, Bangalore, Karnataka, 562106, India
Manikandan S.	Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India
Mukesh Chaudhary	Parul University Vadodara, Gujarat, India
Mary Analiya Babu	Department of Management, CHRIST University, Lavasa Campus, Pune, India

M. Shrahith	Alliance School of Advanced Computing, Alliance University, Karnataka, India
Purnamita Baral	Department of Computer Science & Engineering, Odisha University of Technology and Research, Bhubaneswar, Odisha, India
Pranati Mishra	Department of Computer Science & Engineering, Odisha University of Technology and Research, Bhubaneswar, Odisha, India
P. Uma Devi	Computer Science and Engineering, Gandhi Institute of Technology and Management, Vishakhapatnam, India
Preethi Nanjundan	Department of Data Science, CHRIST University, Lavasa Campus, Pune, India
R. Manik	Department of Computer Science & Engineering, Lovely Professional University, Jalandhar, India
Sruti Nayak	Department of Computer Science & Engineering, Odisha University of Technology and Research, Bhubaneswar, Odisha, India
Subhasmita Pradhan	School of Computer Science and Engineering, Odisha University of Technology and Research, Bhubaneswar, India
Sameer Khan	Alliance School of Advanced Computing, Alliance University, Karnataka, India
Shrishtee Khabra	Department of Commerce, CHRIST University, Lavasa Campus, Pune, India
S. Nonita	Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India
Sriram K.	Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India
Surrenther I.	Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India
Sathya K.	Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India
Saswati Chatterjee	Parul University Vadodara, Gujarat, India
Suneeta Satpathy	Center For Cyber Security, SoA Deemed to be University, Bhubaneswar, Odisha, India
Tony Alosius S.	Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India
Virendra Kumar Shrivastava	Centre of Excellence in Computer Vision, Department of Computer Science and Engineering, School of Advanced Computing, Alliance University, Bangalore, Karnataka, 562106, India
Vijaykumar Jayantibhai Solanki	Government Engineering College Bharuch, Gujarat, India
Vrushali Deshpande	D&M Tech, Pune, India
Y. Gokul	School of Computer Science and Engineering, VIT-AP University, Amaravati, India
Yogesh Khandokar	Beamline Scientist MX, Australia

Section 1
Competitive Intelligence in Business and Finance

CHAPTER 1

Revolutionizing Financial Futures: The AI Impact on Forecasting and Risk Management

Preethi Nanjundan[1,*], **Mary Analiya Babu**[2] and **Lijo Thomas**[2]

[1] *Department of Data Science, CHRIST University, Lavasa Campus, Pune, India*

[2] *Department of Management, CHRIST University, Lavasa Campus, Pune, India*

Abstract: For forecasting and risk management, the financial sector has historically depended on statistical models and historical data. Artificial intelligence (AI), on the other hand, is poised to completely transform traditional methods. This book examines how artificial intelligence (AI) can revolutionize risk management and financial forecasting. The book explores the ways in which artificial intelligence (AI) methods, such as machine learning and deep learning, may analyse enormous volumes of data from various sources to spot intricate patterns and relationships that conventional approaches might overlook. As a result, risk assessments and projections become more precise, empowering financial institutions to make more educated choices. The book also discusses the difficulties in integrating AI in finance, such as obstacles related to regulations, data quality, and model explainability. It offers suggestions on how to get past these obstacles and successfully incorporate AI into financial processes. Financial organizations can obtain a major competitive edge by utilizing AI. Anyone interested in the future of finance and the potentially disruptive power of artificial intelligence should read this book.

Keywords: Artificial intelligence (AI), Big data, Deep learning, Financial forecasting, Machine learning, Pattern recognition, Predictive analytics, Risk management, Regulatory challenges.

INTRODUCTION TO AI IN FINANCE

Artificial Intelligence (AI) has become a disruptive force in the financial industry, reshaping conventional procedures and transforming the way decisions are made. Artificial intelligence has become essential for risk management and financial forecasting because of its unparalleled speed at which it can analyse massive volumes of data and identify intricate patterns. Businesses need to get ready for the next wave of digital disruption that artificial intelligence is about to unleash. It

[*] **Corresponding author Preethi Nanjundan:** Department of Data Science, CHRIST University, Lavasa Campus Campus, Pune, India; E-mail: preethi.n@christuniversity.in

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

is now more important than ever for other businesses to speed up their digital transitions since we are witnessing tangible benefits for a select group of early adopting companies [1]. The evolution of financial forecasting has been marked by a shift from sophisticated artificial intelligence approaches to conventional statistical methodologies. Because machine learning models can learn from previous data and produce highly accurate predictions, they have become popular. Examples of these models are regression, decision trees, and random forests [2]. By identifying intricate links in data that produce deeper insights, deep learning techniques—such as neural networks—have further increased prediction potential. Furthermore, novel approaches to mine unstructured data sources—such as news articles, social media, and incoming calls—for insightful information have been made possible by natural language processing, or NLP. NLP-based algorithms can analyze text data to forecast market movements, gauge the impact of news events, and gauge market sentiment [3]. Artificial intelligence has not only greatly improved forecasting but also risk management procedures in the financial industry. Credit and market risks can be evaluated and reduced by institutions through the use of predictive analytics.

Additionally, investors can design diversified portfolios that are suited to their risk tolerance and financial objectives with the aid of AI-based portfolio optimization tools. The extensive application of AI in banking is not without difficulties, though. Data security, legal compliance, and ethical concerns all demand that AI technologies be used carefully and responsibly. Notwithstanding these obstacles, artificial intelligence has a bright future in banking, and more advancements could significantly alter the sector's structure.

The Evolution of Financial Forecasting

The practice of financial forecasting has changed dramatically throughout the years, moving from an intuitive to a technologically advanced era. In the beginning, traders made educated forecasts based on prior trends and market whispers by using their instincts and experience. Despite its shortcomings, this method cleared the path for more methodical approaches. The 20th century saw the advent of the data-driven age, in which analysts started to spot trends by looking back at previous price, volume, and economic indicator trends. Time series models were developed to better forecast by capturing the subtleties of financial data, and moving averages were used to reduce volatility and identify short-term patterns. The Monte Carlo simulations gained prominence in the 1960s and are still very important today. Risk could be evaluated and simulated by analysts.

The Role of AI in Modern Finance

Artificial Intelligence (AI) is being rapidly incorporated into the operations of the financial industry, resulting in a huge transformation. AI is having a wide range of effects on the sector, from bettering investor decisions to automating backend chores. Enhanced Efficiency and Risk Management: Artificial Intelligence (AI) frees up human specialists for more strategic work by automating repetitive processes like fraud detection and loan application processing. Large volumes of financial data may be analyzed by AI algorithms to find trends and forecast hazards related to investments, loans, and even money laundering. As a result, organizations are able to decide more quickly and intelligently. An organizational culture that welcomes human and machine collaboration is necessary to reap the long-term benefits of artificial intelligence. Here, trust is a crucial facilitator. The relationship between a machine's internal operations and the output it generates can become fairly hazy because of the interaction between training and inference in artificial intelligence [4].

AI gives financial experiences to clients and institutions a personalized touch. Banks can use artificial intelligence (AI) to comprehend client behaviour and provide individualized financial products or wealth management guidance. In a similar vein, AI-driven robo-advisors evaluate each client's risk tolerance and investing objectives before generating automated investment plans. To forecast future market movements, investment and artificial intelligence algorithms can examine social media data, news sentiment, and market patterns. This gives hedge funds and investment firms the ability to make data-driven judgments about their investments and maybe increase profits. AI-powered algorithmic trading has the ability to complete deals extremely quickly and take advantage of short-lived market opportunities. Financial services are becoming more widely available thanks to AI-powered financial solutions. For those without the funds to hire a traditional financial counsellor, robo-advisors offer investing advice.

Furthermore, AI can evaluate creditworthiness from non-traditional data sources, giving institutions access to populations that were previously unbanked. Even though artificial intelligence (AI) has a lot of promise, ethical issues and potential biases in algorithms must be addressed. In general, AI is bringing about a new era of intelligent finance that will be characterized by increased accessibility to financial services, efficiency, and personalization.

AI TECHNIQUES FOR FINANCIAL FORECASTING

For a very long time, financial forecasting has been an essential instrument for managing market volatility. These days, Artificial Intelligence (AI) is changing this area by providing strong methods that improve precision and reveal hidden

CHAPTER 2

Forecasting Demand in Retail Supply Chain Management: A Comparison of Deep Learning and Machine Learning Methodologies

Sruti Nayak[1], Purnamita Baral[1], Jyotirmayee Rautaray[1,*], Pranati Mishra[1] and **Meenakshi Kandpal[2]**

[1] *Department of Computer Science & Engineering, Odisha University of Technology and Research, Bhubaneswar, Odisha, India*

[2] *Department of Computer Science & Engineering, KIIT, Bhubaneswar, India*

Abstract: The paper explores supply chain management, emphasizing the importance of accurate demand forecasting. The word supply chain refers to the product journey from supplier to consumer. Demand forecasting is the anticipation of the market's demand for a product. Various models that can be used for accurate prediction include ARIMA, LSTM, STL, Prophet, GBM, SVM, KNN, Neural Networks, *etc.*This paper compares five algorithms from the available algorithms pool: ARIMA, LSTM, FB-Prophet, XGBoost, and Decision Tree Regressor. Two datasets, sourced from Yahoo Finance, spanning a decade and including real-time sales data of Walmart and Amazon, are used for the study. The optical model for demand forecasting depends upon specific evaluation metrics and the nature of the dataset. Taking MAE (Walmart sales data: 0.036588, Amazon sales data: 0.066181) into account, FB-Prophet is a suitable model for both datasets. ARIMA can also be considered an appropriate model for linear data. Moreover, considering the diverse evaluation metrics, LSTM distinguishes itself as a formidable choice among other models for capturing complex relationships and predicting accurate demand.

Keywords: Demand forecast, Evaluation Metrics, LSTM, MSE, MAE, Retail, RMSE, Supply chain, Time Series.

INTRODUCTION

In the dynamic retail industry, precise demand forecasting is essential. Knowing the customer needs and preferences enables effective inventory management (low inventory cost throughout the entire supply chain), resource allocation, and strategic decision-making. Supply chain management is the method of managing a

* **Corresponding author Jyotirmayee Rautaray:** Department of Computer Science & Engineering, Odisha University of Technology and Research, Bhubaneswar, Odisha, India; E-mail: jyotirmayee.1990@gmail.com

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

service or product, from purchasing raw materials to efficiently distributing the finished product.

Supply chain management efficiently manages the movement of products and services on time and within budget [1]. A crucial aspect of supply chain management is demanding forecasting. Demand forecasting is the process that involves a set of activities for estimating the quantity of different kinds of goods and services for the future based on past data and present circumstances. There are two approaches used in demand forecasting: Qualitative method and Quantitative method. In the case of the Qualitative method, no mathematical computation is used. On the other hand, the Quantitative method is based on Mathematical Computations. The demand forecasting techniques include internal and external demand forecasting, long-term and short-term forecasting, and passive and active forecasting. Demand forecasting is helpful for long-term strategic planning and short-term decision-making. It is also beneficial in minimizing the effect of the *Bullwhip Effect*. Order variations are likely to increase as one progresses up the supply chain, a phenomenon known as the effect [2]. Various factors affect accurate demand forecasting, such as the existing condition of an organization, industry conditions, customer psychology, economic environment, and product life cycle. This work offers a thorough analysis of several machine learning and deep learning techniques, like Autoregressive integrated moving average (ARIMA), Long short-term memory (LSTM), FB Prophet, Extreme Gradient Boosting (XG Boost), and Decision Tree regressor, applied to retail sales data of Walmart and Amazon extracted from Yahoo. Finance. As shown in Fig. (**1**), our study's structure involves essential steps of data collection, preparation, and analysis, emphasizing the evaluation of different model performances.

The paper is organized in the following sequence: The literature assessment of several proposed models is presented in section 2. The suggested processes, which include flowcharts, are described in Section 3. Section 4 is subdivided into two parts, 4.1 and 4.2, where 4.1 demonstrates the implementation of the proposed model and section 4.2 represents the result analysis of the model. Finally, section 5 highlights key findings as the conclusion of this study.

LITERATURE REVIEW

Machine learning and deep learning for sales forecasting are gaining popularity due to their ability to predict future sales accurately. The purpose of this literature study is to clarify the various methods and models that have been put forth and used in this field, emphasizing their effectiveness and predicted accuracy [3].

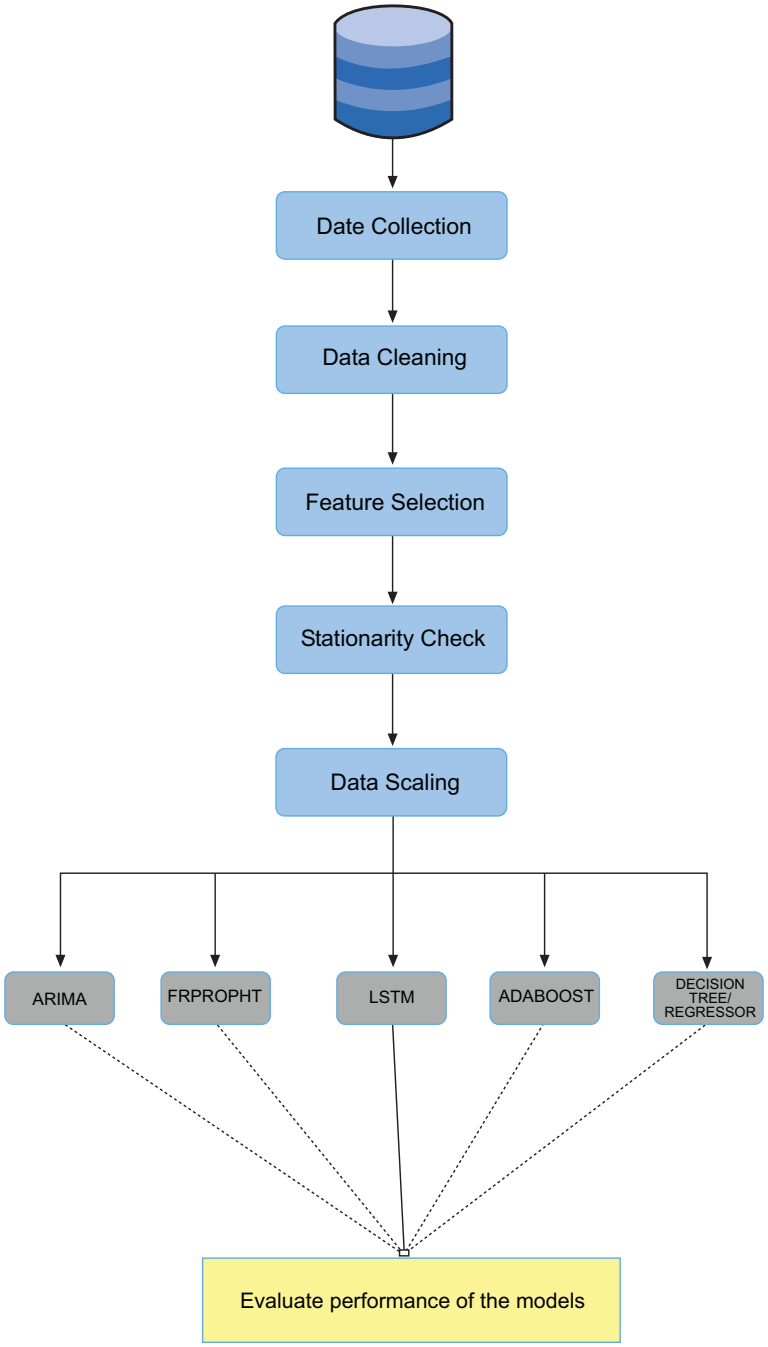

Fig. (1). Flowchart of proposed methodology for demand forecasting.

CHAPTER 3

Assessing the Optimal Deep Learning Model for Predicting Financial Insolvency

Bikash Chandra Naik[1], Meenakshi Kandpal[1,*], Jyotirmayee Routray[1], Pranati Mishra[1] and **Subhasmita Pradhan[1]**

[1] *School of Computer Science and Engineering, Odisha University of Technology and Research, Bhubaneswar, India*

Abstract: This research presents a groundbreaking Deep Learning-Based Model for Financial Distress Prediction, leveraging advanced neural network architectures to enhance the accuracy and reliability of forecasting financial distress. The model is designed to autonomously learn intricate patterns and relationships within extensive financial datasets, addressing the limitations of traditional methods in capturing complex, non-linear dependencies. Key to its efficacy is the incorporation of different deep learning models like CNN, ANN, LSTM, BiLSTM and XGBoost, enabling the model to grasp sequential dependencies within financial time series data. This temporal awareness is crucial for understanding the evolving nature of financial indicators over time, providing a more nuanced perspective on potential distress signals. The model's strength lies in its ability to automatically extract relevant features, eliminating the need for manual feature engineering, which is a common challenge in traditional models. As financial markets continue to grow in complexity, the Deep Learning-Based Model offers a proactive and innovative response to the evolving challenges of risk management.

Keywords: ANN, BiLSTM, CNN, Financial distress, LSTM, Neural network architecture, XGBoost.

INTRODUCTION

Bankruptcy is a situation of liquidation where the original company is unable to repay its loan amount to creditors. When a company's debt is higher than average and the situation remains unchanged for a long time; as a result, the company is not able to pay back the obligation, this situation is called as Bankruptcy. In other instances, businesses go bankrupt right after experiencing a problem, such as significant fraud. The company which is announced bankruptcy is taken as a failed company. Bankruptcy affects the company’s reputation as well as the profit

* **Corresponding author Meenakshi Kandpal:** School of Computer Science and Engineering, Odisha University of Technology and Research, Bhubaneswar, India; E-mail: meenakshikandpal14@gmail.com

made by individual stakeholders, and as a result, it further affects the economic expansion of the business.

Therefore, bankruptcy prediction is taken as a global-level issue. Such forecasting helps banks avoid providing financial support to companies that have a higher probability of going bankrupt in the near future. Additionally, investors can protect themselves from financial loss by avoiding investments in such companies. The failure of a company does not come overnight; it gradually arrives through several stages slowly. Prediction of this bankruptcy will help to warn the company about the danger knocking on their door and take actions accordingly, modifying their course of action. Therefore, bankruptcy prediction (BP) has been the subject of much research for the past fifty years.

This paper presents novel Deep Learning-Based Models for Financial Distress Prediction, leveraging advanced neural network architectures to analyze extensive datasets with a focus on capturing nonlinear relationships and temporal dependencies. The key strength of deep learning lies in its ability to autonomously extract relevant elements, eliminating the need for manual feature engineering, which is a common challenge in traditional models. The deep learning-based approach is designed to adapt and evolve as market conditions change, making it inherently more robust in capturing the dynamic nature of financial markets.

Moreover, the model's incorporated include *ANN, CNN LSTM, BiLSTM* and *XGBoost* networks. The accuracy of all the given models was then compared to identify the most accurate model, which was found to be the most successful in predicting bankruptcy.

As financial markets continue to grow in complexity and interconnectivity, the deployment of a Deep Learning-Based Model for Financial Distress Prediction represents a proactive and innovative response to the evolving challenges of risk management. This paper explores the methodology, performance, and implications of such a model, aiming to contribute to the advancement of predictive analytics in finance and fortify the financial industry's resilience against uncertainties.

RELATED WORK

Abror *et al.* [3] implemented a data set compiled by the Taiwan Economic Journal that trained an estimated 6,819 machines using machine learning algorithms and methods for classification. In this paper, the author found a categorization technique that provided the best accuracy outcomes. The author focused simply on forecasting the occurrence of bankruptcy and did not take into account the socio-economic ramifications of the traditional bankruptcy prediction models [2].

As a result, the motive of the research was to incorporate the viewpoints through the machine-learning (ML) modeling technique in order to account for the various costs associated with bankruptcy [6]. An approach for processing small-sample domestic company financial data was also presented [3]. To solve the problem of getting the prediction accuracy of companies, the author explored instance of random sampling of companies through an approximate entropy and an optimization threshold based on AUC [4].

Adisa *et al.* [2] implemented self-learning and multi-learning strategies to develop the cognitive and social learning parts of the PSO algorithm. Moreover, the algorithm used by PSO identified the best LSTM settings. The author's final method for bankruptcy prediction combined optimal feature selection with the LSTM model. As a result, an improved feature selection approach for the LSTM model was devised [4, 5, 7]. Five feature selection strategies to produce datasets with fewer duplicate characteristics in order to determine which feature selection methods perform most effectively in bankruptcy prediction were evaluated and employed [5].

The author investigated the Taiwanese Bankruptcy dataset from the Taiwan Economic Journal. Then, for dealing with imbalanced datasets, the author employed an artificial minority oversampling strategy that used GA-SVM to select the best feature, then the classifier was stacked and extreme gradient boosting was applied as a meta-learner. As a result, it was demonstrated that the proposed strategy could forecast bankruptcy with high accuracy [6, 14]. The author also proposed a transfer learning-based model and the test was using a self-collected and cautiously labelled dataset [7]. The LSTM model assumptions were used to generate machine learning models on both the primary and K-Means SMOTE balanced datasets.

Valaskova *et al.* [8] focused on developing a model for forecasting bankruptcy data from 20,693 firms from all sectors that functioned in Visegrad group countries over time (2020-2021), also to find key predictors of bankruptcy. Further, the author stated that to avoid losses caused by an enterprise's economic crisis, multiple discriminatory evaluations could be used to create individual prediction models for every Visegrad and an intricate individual model for overall Visegrad group [8, 9]. The author implemented the Black-Scholes asset pricing model for combining conceptual and professional evaluation to pinpoint the financial ratios and macroeconomic variables impacting bankruptcy [9].

The evaluation of multilayer artificial neural networks to examine the trustworthiness of the outcome in determining and prioritizing the factors influencing the prediction of bankruptcy revealed that the least significant

CHAPTER 4

An Enhanced Bank Loan Approval Prediction using Machine Learning Approach

Virendra Kumar Shrivastava[1,*], Mano Paul P.[2], A. Ezil Sam Leni[3], M. Shrahith[3] and **Sameer Khan[3]**

[1] *Centre of Excellence in Computer Vision, Department of Computer Science and Engineering, School of Advanced Computing, Alliance University, Bangalore, Karnataka 562106, India*

[2] *COE in iOS App Development, Dept of CSE, Alliance University, Bangalore, Karnataka 562106, India*

[3] *Alliance School of Advanced Computing, Alliance University, Karnataka, India*

Abstract: Bank loans are essential finance tools that enable individuals to capitalize on investments, purchase, or improve the family's economy by covering unseen expenses. Nowadays, banks are actively offering loans to support business growth through various investment strategies—ranging from low to high risk—with the aim of improving individuals' lifestyles and social status. Transactions play an essential role in processing debit, credit, internet banking, and other modes of payment and play a vital role in today's processing either in bank or gold transfer or online transfer and even in digital currencies and market trends to predict share market business stocks. The number of loan applications is increasing daily for loan processing to verify the customer base for loan approval. Bank policies are also stringent in selecting genuine or fake applicants by selecting various parameters for loan approval. Based on a few parameters about eligibility and the Cibil score, the bankers must decide whether they are eligible for loan approval. In this study, machine learning algorithms were applied to predict whether an individual is eligible or ineligible for a loan based on previous related records of the person on whom the loan was previously accredited and initiated by the naive Bayes classifier and supported Support Vector classifier. This study employed further classification using an extreme gradient classifier algorithm and proceeded by boosting this classifier using XGB boosting methods for the prediction with maximum choices with ensemble learning. Finally, text analysis methods are used to identify the accuracy, false positive rates, true favorable, and F1 scores. The proposed prediction model provides 98.5% accuracy for bank loan approval with the educated level, namely graduated and un-graduated levels.

Keywords: Artificial neural network, Credibility limits, Loan approval, Loan prediction, Machine learning.

[*] **Corresponding author Virendra Kumar Shrivastava:** Centre of Excellence in Computer Vision, Department of Computer Science and Engineering, School of Advanced Computing, Alliance University, Bangalore, Karnataka 562106, India; E-mail: Virendra.shrivastava@alliance.edu.in

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

INTRODUCTION

In today's dynamic financial landscape, the ability to accurately predict loan approvals is crucial for lenders and borrowers. Our system harnesses the power of advanced ML techniques and algorithms to analyze vast datasets of diverse profiles, financial histories, and market trends. By leveraging sophisticated predictive models, our system can assess applicants' creditworthiness with unprecedented precision, providing lenders with invaluable insights to make decisions effectively. Whether it is assessing risk, streamlining approval processes, or enhancing customer experience, our Loan Approval Prediction System offers a comprehensive solution tailored to meet the evolving needs of the lending industry. The loan system allows us to jump on the application that deserves approval on a priority basis, whether the candidate is educated or uneducated, based on their graduation status. With today's evolving trends in the bank loan approval process, several key parameters are typically used for prediction. These include loan ID, loan amount, loan terms, credit history, property area, applicant income, employer details, educational qualifications, marital status, number of dependents, gender, and other features. Loan approval decisions are often supported by predictive models and further validated using a credit score—such as the CIBIL score—which represents an individual's standard creditworthiness

LITERATURE SURVEY

To perform a prediction, technical machine learning algorithms exceptionally work and will assert the prediction about the approval or disapproval shortly; we impose the machine learning strategy for predictions made frequently by people with many of these conjectures, while some are highly serious and calculated and based on scientific calculations. In many ways, prediction aids our ability to calculate what will transpire in the future, whether a year from now or so. Here, a methodology called predictive analytics is used, which is a subset of advanced analytics that analyses current data and generates forecasts using a variety of methods from data mining, exploratory analysis, statistics, and modeling, which is used with the algorithms for learning and used in artificial intelligence—Arun Kumar *et al.* [1] engaged in the task of predicting housing prices. They employ PSO (particle swarm optimization) and regression analysis to forecast property prices. Through loan default prediction, banks can lower their non-performing assets. This emphasizes the importance of investigating this issue. Previous studies have demonstrated that reduced loan defaults may be studied using various methodologies. However, because accurate forecasting is crucial for optimizing earnings, it is critical to examine the characteristics of the project.

The data collection process was accomplished using the Kaggle dataset for analysis and forecasting purposes to predict approval. The application of Logistic Regression models calculated various performance metrics. There are test and training datasets in the bank customer dataset. Compared to the test crop yield dataset, which has 250 or more rows and 10 or more columns but lacks the target variable, the training dataset has about 600 more rows and 12 more columns. Because the datasets are already tiny, the mean, mode, and median fill the missing, null, and vacant values in the rows rather than eliminating the rows. Both datasets contained vacant values in their rows. The project was advanced to exploratory data analysis using feature engineering methodologies.

This project's primary goal is to forecast the safety of granting a loan to an individual. This is structured into four parts: gathering data, comparing predictive models on the data, training the system using the most promising model, and testing. In this study, we employ machine learning techniques, including gradient boosting, decision trees, classification, and logic regression, to forecast the loan data. The bank must work hard to analyze and predict whether the customer (defaulter or non-defaulter) can repay the loan balance within the allotted time. This paper aims to find out about the client's past, character, and loan application. Our method for addressing the issue of accepting or denying a loan request, or, more succinctly, loan prediction, is exploratory data analysis.

This paper's primary goal is to decide whether to authorize a loan provided to a specific individual or organization. Adyan Nur *et al.* [2] focus on the modeling of house prediction, which follows a machine learning algorithm, and Rao R *et al.* [3] focus on anomaly detection *via* a machine learning algorithm, which describes the removal of duplicate data from the rows, which is a record. Quinlan, J. Ross, *et al.* [4] used a regression analysis approach to create a prediction for supervised learning methods. Sentimental analysis was shown by S. Liao *et al.* [5], which provides the convolution neural network to understand the semantics *via* sentimental analysis Singhal *et al.* [6] described medical data and Jingle *et al.* [7] focused on the prevention of attacks in networks and to develop high-performance systems. In machine learning, supervised learning approaches were given with optimization imposed by Mohamed EI *et al.* [8], who stated that supervised learning schemes, Saha *et al.* [9] focus on text analysis by reducing false positives. Supriya P *et al.* [10] process datasets and classify with decision tree algorithms stated by Quinlan *et al.* [11] describes the decision tree approach in the classification prediction models; Rahmani *et al.* [12] state the efficient indexing algorithms which transform the data for the quick access with the help of keys. Madane *et al.* [13] focused on the decision tree for loan prediction and didn't classify the result as boosting its performance at output levels. Kumar *et al.* [14] provide AI techniques for predictive analysis, which inculcate the features of

CHAPTER 5

Exploring Consumer Awareness within Electronic Payment Systems

Blesson Varghese James[1], Preethi Nanjundan[2,*], Akhand Tiwari[1] and **Shrishtee Khabra[1]**

[1] *Department of Commerce, CHRIST University, Bengaluru, India*

[2] *Department of Data Science, CHRIST University, Bengaluru, India*

Abstract: This paper presents a comprehensive review of the literature on the adoption of electronic payment (E-Payment) systems in the Indian context. Through an extensive examination of existing studies, the paper explores the various factors influencing E-Payment adoption, including perceived usefulness, ease of use, facilitating conditions, and system credibility. Moreover, their study investigates the role of demographic factors—such as gender, education, employment status, age, and technological literacy—as moderators influencing individuals' attitudes toward e-payment. A key finding is the need for targeted interventions to enhance digital payment literacy among young consumers, suggesting opportunities for educational initiatives and user experience enhancements. The paper concludes with recommendations for policy makers, businesses, and researchers to address the identified gaps and foster wider adoption of E -Payment solutions in India's evolving digital economy. The findings highlight the significance of addressing trust, security concerns, and technological literacy to foster greater acceptance of E-Payment systems. Moving forward, further research is recommended to explore emerging trends and innovations in the digital payment landscape, ensuring the continued relevance and effectiveness of interventions aimed at driving E-Payment adoption in India.

Keywords: Consumer awareness, Digital payment, E-Payment adoption, India, Technology acceptance.

INTRODUCTION

"E-payment" denotes payment methods facilitated through the Internet. It encompasses a collection of elements and processes that enable two or more parties to conduct financial transactions exclusively over the web. Examples of electronic payment systems include online credit card transactions, electronic wallets (e-wallets), electronic cash (e-cash), and digital currencies [1]. With this

* **Corresponding author Preethi Nanjundan:** Department of Data Science, CHRIST University, Bengaluru, India; E-mail: preethi.n@christuniversity.in

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

shift, the currency is no longer constrained in its usage, and appropriate procedures are employed to diminish the reliance on physical cash. The significance of digital transactions is heightened, offering the population an alternative solution from various perspectives [2]. The latest stage reflects a notable transformation in how payments are made and received. Ongoing changes in daily infrastructural activities indicate a shift in policies. Everyone must recognize that India's future is moving towards a "cashless economy" for the overall welfare of society [3].

The Digital India program stands as a flagship initiative of the Government of India, aiming to metamorphose the country into a digitally empowered society and knowledge economy. One of the proclaimed objectives of Digital India is to make processes "Faceless, Paperless, Cashless." This implies a transition toward administrative processes that eliminate physical interactions, reduce paperwork, and minimize reliance on bank visits and ATM withdrawals. The emphasis is on replacing physical wallets with digital alternatives, making transactions more convenient and reducing reliance on cash. E-payment apps play a pivotal role in this transition, enabling individuals to send money and make purchases at shops seamlessly. A notable trend in India is the rapid introduction and widespread acceptance of various mobile wallets (m-wallets). This shift is pushing the payment trend away from traditional Cash on Delivery (COD) models to "Payment on Delivery" or "Payment On Order," with mobile phones serving as the primary medium for these transactions. This signifies a significant paradigm shift towards the mobile wallet space in recent times, highlighting the increasing preference for digital payment solutions [4]. The provided text discusses the current landscape of payment methods in Vietnam, emphasizing the predominant use of cash in transactions. The State Bank of Vietnam's data from 2008 indicates that cash remains the primary method of payment, especially among individuals, constituting over 90 percent of retail payments. The text also highlights that a significant portion of the population, less than 15 percent, uses bank services regularly, and less than 30 percent have savings in banks [5].

The global trends of liberalization, globalization, and Vietnam's integration into the World Trade Organization (WTO) are acknowledged, presenting both opportunities and threats to the country's economy and banking sector. To participate more actively in the global economy, there is a need for a shift in payment transaction habits among Vietnamese citizens. The text notes the emergence of new business models like e-commerce and e-business, requiring the integration of information technology (IT) into banking systems to enhance service quality [6].

Various modern banking applications, including online transactions, ATMs, POS systems, payment cards, and Internet banking, are now present in Vietnam. Efforts by the State Bank of Vietnam to reduce cash transactions are mentioned, with a project spanning 2006-2009 aimed at increasing the issuance of non-cash transactions. Despite progress in e-payment, the text notes that the preference for cash persists, with concerns about security, lack of information on e-payment methods, and hesitancy to shift from traditional to electronic methods. The public's attitude towards e-payment has improved in recent years, encouraged by the increase in bank card users and the expansion of ATM and POS networks, particularly in major cities like Hanoi and Ho Chi Minh. However, challenges remain as the public grapples with the security implications and unfamiliarity associated with electronic payment methods [7].

This study aims to explore the variables impacting the uptake of electronic payments in the Indian setting. Its objectives are to determine how much consumer knowledge there is about using electronic payment systems and to investigate security issues related to online financial transactions. Through an examination of these aspects, the research aims to offer a significant understanding into the complex dynamics of electronic payment uptake in India. These insights will be instrumental for policymakers, businesses, and financial institutions in developing tailored strategies to foster increased acceptance of digital financial services while addressing institutions in developing tailored strategies to foster increased acceptance of digital financial services while addressing security concerns and enhancing consumer awareness.

Literature Review

In the Information Systems (IS) literature, examinations of Mobile Payments (M-Payment) usage predominantly centre around three key factors: behavioural beliefs, social influence, and personal traits [8]. Study delves into the implementation of enterprise integration to promote a cashless revolution in Pakistan [9]. The study likely explores the technical aspects and potential benefits of enterprise integration in transitioning towards a cashless economy. Notably, a limited number of studies have explored the impact of awareness regarding mandatory payments as a significant driver in the context of M-Payment adoption, and yet, only a few studies have delved into its influence [10]. While the study explores users' intentions, a potential research gap lies in explicitly addressing the awareness levels and preferences of young consumers [11].

INFLUENCE OF GENDER IN UNDERSTANDING E-PAYMENT

In a seminal work that explores consumer awareness among young minds in e-payment, it is essential to examine potential gender-related variations in the

Section 2
Future-Ready Security with AI & ML

CHAPTER 6

A Comprehensive Survey of Deep Learning Methods in Network Intruder Detection System

P. Uma Devi[1,*] and **Gurpreet Singh Chhabra**[1]

[1] *Computer Science and Engineering, Gandhi Institute of Technology and Management, Vishakhapatnam, India*

Abstract: The increasing prevalence of cyberattacks and intrusions in the digital era has made it crucial for organizations to invest in adequate security systems. Intruder Detection Systems (IDS) are designed to identify and prevent unauthorized access to networks and sensitive information. Network intrusion detection systems are a crucial component of network security, enabling the prevention and detection of network attacks. Traditional ML methods for intruder detection systems, such as rule-based systems, have limitations in detecting complex and evolving threats. These systems rely on predefined rules and signatures, making them less adaptable to detect new attacks. Deep learning is emerging as a powerful technique in IDS, significantly enhancing their ability to secure networks and devices. This review paper examines DL-based applications in intruder detection systems (IDS) and describes how Deep Learning techniques can detect intrusions in cyber-attacks.

Keywords: Convolutional neural networks (CNN), Deep learning (DL), Generative adversarial networks (GANs), Intruder detection systems (IDS), Long short-term memory (LSTM), Machine learning (ML).

INTRODUCTION

In today's digital world, with the rapid evolution of technology, computer security concerns are becoming increasingly important. Intruder detection systems (IDSs) are vital in identifying attacks that differ from normal user activities in the computer security ecosystem. The IDS assumes that attackers have different behaviors from regular users, as shown in Fig. (**1**). The primary function of (IDS) intrusion detection systems is to detect intruders, attacks, or cybersecurity breaches at both network and host levels. Based on their design, intrusion detection systems are categorized into three types: network-based, host-based, and hybrid.

[*] **Corresponding author P. Uma Devi:** Computer Science and Engineering, Gandhi Institute of Technology and Management, Vishakhapatnam, India; E-mail: upeddabu@gitam.in

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

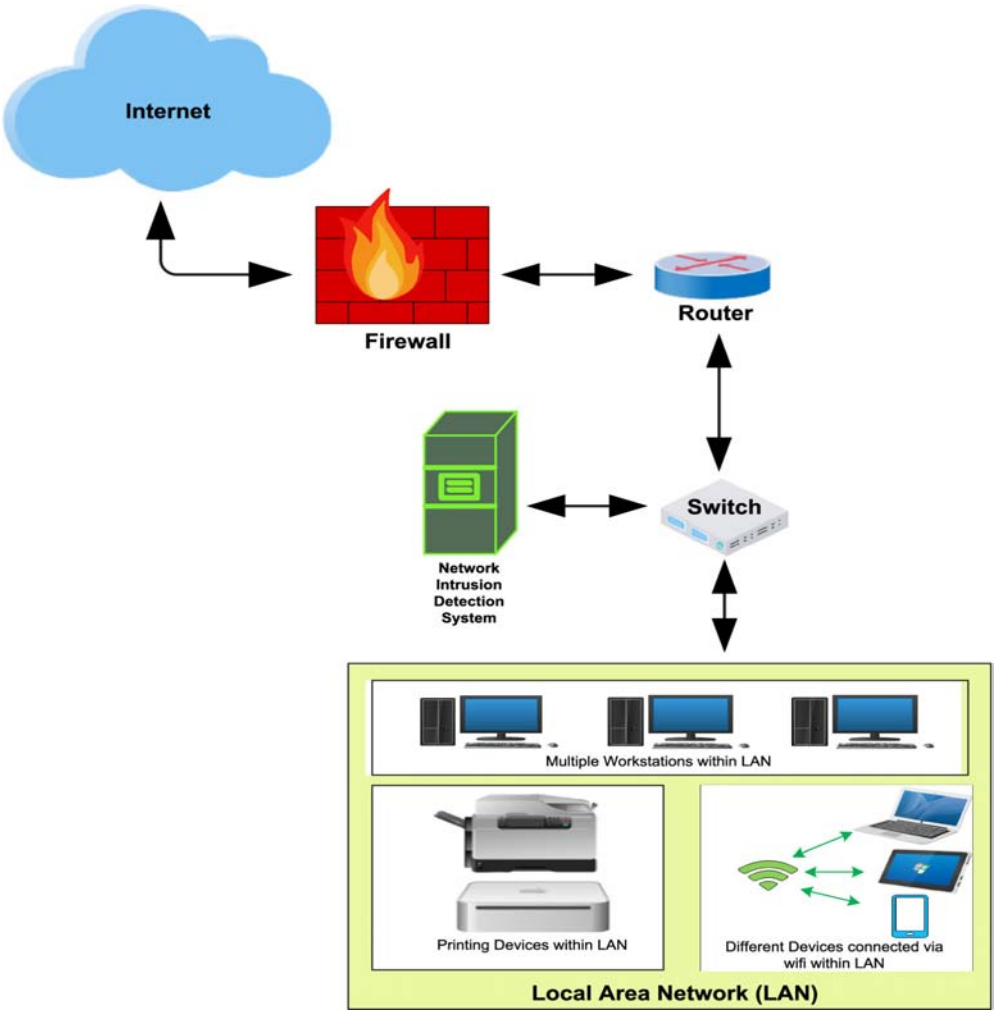

Fig. (1). Intrusion detection systems.

A host-based IDS software application monitors and analyses system behavior on a host machine. The majority of intrusion detection systems utilize a system at the host level, such as event log files, to detect intrusions [1]. Furthermore, Intrusion detection systems (IDS) are categorized into three methodologies: stateful protocol analysis detection, signature-based detection, and anomaly-based detection. The Intruder Detection System (IDS) analyzes data using a commonly used approach known as signature-based detection, which matches monitored data to known attack patterns [2]. This technique is successful and dependable. While log-based detection excels at identifying previously encountered threats, it struggles to adapt to novel attacks.

Anomaly-based detection tackles this challenge by establishing a profile of expected system behavior. This allows it to flag deviations from this baseline, potentially uncovering zero-day attacks that bypass traditional methods. This approach can identify risks, but it also generates numerous false alarms. Due to the increasing volume and diverse threats, anomaly-based intrusion detection systems have been a significant area of research over the past two decades. Different machine learning methods have been used to identify misuse and abnormalities, but they are rarely applied in real-world applications. This approach remains misuse/anomaly detection, which is often considered the key cause for the limited use of anomaly-based IDS due to its high false positive rate [3]. Indeed, even a small percentage of false favorable rates can result in a significant number of false alerts on high-traffic networks; the volume of alerts generated by anomaly-based detection can overwhelm administrators, making practical analysis difficult, as shown in Fig. (**2**). Computers and networks had been vulnerable to attacks from hackers, viruses, and worms and other malicious software, according to Evans. Because the number of intrusions is also drastically increasing year by year, securing these devices and the data that move between them is a task that is difficult to accomplish [4]. A significant number of recent studies have demonstrated the application of various machine-learning strategies in the context of anomaly detection and misuse identification [5]. One of the main limitations of machine learning techniques is the scarcity of training datasets. These methods typically rely on manually extracted features, making it challenging to apply them to various applications.

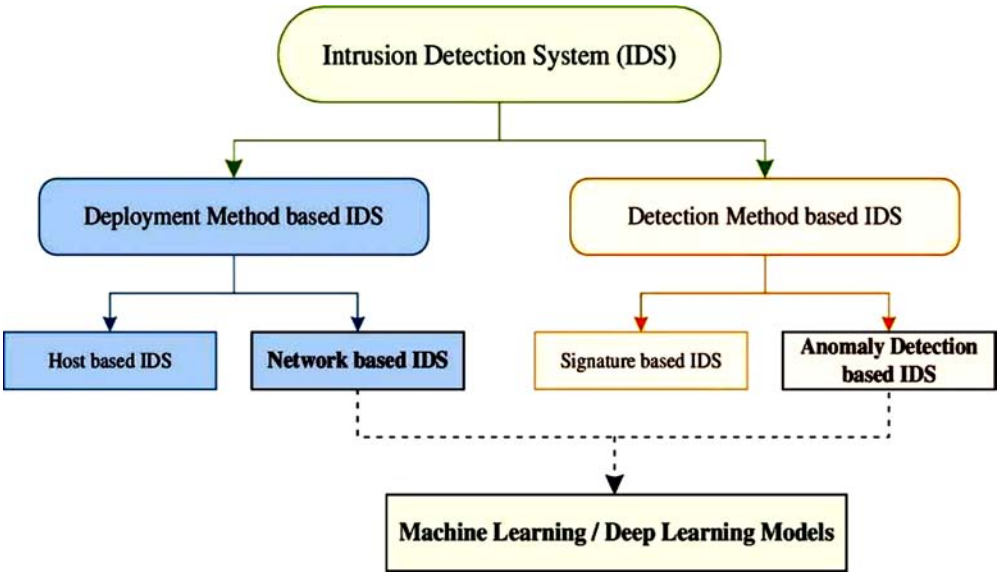

Fig. (2). Classification of intrusion detection system.

CHAPTER 7

Fake Profile Detection in Social Media: Incremental Greedy Ensemble Approach

S. Nonita[1,*], Monika Mangla[2], Y. Gokul[3] and **R. Manik[4]**

[1] *Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India*

[2] *Department of Information Technology, Dwarkadas J. Sanghvi College of Engineering, Navi Mumbai, India*

[3] *School of Computer Science and Engineering, VIT-AP University, Amaravati, India*

[4] *Department of Computer Science & Engineering, Lovely Professional University, Jalandhar, India*

Abstract: The proliferation of social networking sites has significantly improved long-distance communication and fostered a more interconnected global community. However, it also allows intruders to engage in surveillance and fraudulent activities. There has been a significant increase in such instances involving fake profiles, especially in recent years. To detect such profiles, this work presents a novel iterative greedy approach for detecting counterfeit profiles on social media networks. The work has considerable societal implications, as most antisocial behaviors on social networks are primarily carried out through fake accounts. The proposed methodology is implemented on three popular datasets. During the experimental setup, the base classifiers used are Support Vector Machine, Decision Tree, Logistic Regression, Gaussian Naïve Bayes, and k-Nearest Neighbor. The optimized ensemble model utilizes two decision trees and one k-Nearest Neighbor. The yielded ensemble model is also compared with base classifiers and traditional ensemble models, and it is observed that the proposed ensemble model outperforms base classifiers and traditional ensemble models in terms of F-score and accuracy.

Keywords: Classifiers, Ensemble model, Fake profile detection, Greedy approach, Social media.

INTRODUCTION

Social media sites are now one of the most vulnerable points for spying, sending mischievous links, and carrying out financial scams used by cybercriminals.

[*] **Corresponding author S. Nonita:** Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India; E-mail: nsnonita@gmail.com

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

Cybercriminals widely use such platforms as they allow them to establish a connection with their targets [1]. Additionally, it is worth noting that there has been a massive surge in the frequency and impact of cybercrimes [2 - 4]. Considering the societal, emotional, and financial implications of such fraudulent activities, it is imperative to devise a robust and efficient method for identifying fake users on social networking sites. Fake profile detection involves identifying and removing fake or fraudulent profiles from online platforms, primarily focusing on social media sites, dating apps, and marketplaces. The detection process consists of analyzing user profiles, user-generated content, and user activity to determine whether the account is authentic. The different methods for detecting fake profiles are as follows:

- Social network analysis: This involves analyzing the user's friends, followers, and connections network to identify anomalies or patterns that predict the account is fake.
- Image analysis: Fake profiles often use images from other sources, such as photos from social media profiles. Image analysis can detect fake profiles by checking if the same image is used across multiple profiles.
- Text analysis: Fake profiles often use generic or overly optimistic language or may contain spelling and grammar errors. Text analysis can help identify fake profiles by detecting such patterns.
- Behavior analysis: Fake profiles often indulge in suspicious activities such as sending messages or friend requests to many users. Such activities can be traced to the detection of fake profiles.

Machine Learning (ML) algorithms can recognize fake profiles by finding anomalies in text, behavior, usage of keywords, timing of user activities, *etc.* ML is a technique that predicts future results based on historical data, using which a classifier is trained to find out patterns, identify anomalies, test hypotheses, and verify assumptions [5]. The growth in the field of ML has opened avenues for its deployment in various aspects of human life. It has become an indispensable part of human life, as we use it even without realizing it in applications like Google Maps, Google Assistant, and Alexa, among others.

Considering the efficiency of ML, this paper aims to employ ML to design an efficient predictive model for fake profile prediction. The authors of this work propose an ensemble model, a relatively new technique widely adopted to improve the performance of ML models [6]. Ensemble models enhance the efficiency of predictive models by implementing multiple models rather than relying solely on the predictions of a single model. Consequently, this work

proposed an ensemble model combining popular ML models to enhance effectiveness and efficiency further.

As discussed, ensemble learning combines the results of various models. It generates a standard set of outputs based on specific parameters, significantly improving the accuracy of the results. There are two variations of ensemble models: homogeneous and heterogeneous. The homogeneous ensemble model combines results from the same base model, while the heterogeneous ensemble model uses different base models. An ensemble model ensures that the predicted outcome is the best among all base models and can be determined using three fundamental techniques: maximum voting, averaging, and weighted averaging [7]. Here, max voting is used for classification problems, while averaging and weighted averaging are used for regression problems.

An ensemble model can be passed through a voting classifier, which selects the output suggested by the majority of models. Here, it is worth noting that averaging and weighted averaging can also be used in cases involving categorical variables to calculate probabilities of nominal values.

Ensemble techniques can be further categorized into three categories: Bagging, Boosting, and Stacking. Bagging trains multiple weak learners in parallel and outputs the aggregated results of all base models. The sample dataset used to train each weak learner may or may not be identical, as it is fetched using the replacement technique. Random Forest is an example of a bagging algorithm that significantly reduces overfitting compared to its base learner, *i.e.*, the Decision Tree. Unlike bagging, base learners depend on each other's output in boosting, as the production of one base model is fed to another sequentially. Additionally, it does not assign equal importance to all base learners, as incorrectly classified data points are given more weight in training the next model. Gradient boosting and AdaBoost are standard boosting algorithms. In stacking, two or more base models are trained, and the results are sent to a meta-model to aggregate predictions. The meta-models are trained on data that was not sent to base-models. Stacking occurs in levels where base models are at level 0, and meta-models are at level 1. In the current research work, the authors used an ensemble model with a dynamic programming approach.

Optimization in ML is the process of adjusting hyperparameters to improve performance. These hyperparameters are optimized to maintain a balance between bias and variance, and can be achieved through various techniques, such as gradient descent and stochastic gradient descent. The gradient Descent technique minimizes the cost function, thereby reducing the error. The goal is to reach a local minimum where the cost function cannot be further reduced. Furthermore,

CHAPTER 8

An Analysis of the Effectiveness of MANET Routing Algorithms using Machine Learning

D. Gousiya Begum[1,*], Anjaiah Adepu[2], Amjan Shaik[3] and **K. Nagajyothi[4]**

[1] *Department of CSE, BEST Innovation University (BESTIU), Andhra Pradesh, India*

[2] *Department of CSE, IC Polytechnic, Maulana Azad National Urdu University, Bihar, India*

[3] *Department of CSE, St. Peter's Engineering College, Hyderabad, Telangana, India*

[4] *R&D, BEST Innovation University (BESTIU), Andhra Pradesh, India*

Abstract: Mobile Ad Hoc Networks (MANETs) are a dynamic and self-configuring wireless communication system that is essential in a wide range of applications, including military operations and disaster recovery situations. The effectiveness and dependability of communication in MANETs are greatly contingent upon the routing algorithms utilized. This study provides a thorough examination of the efficacy of MANET routing algorithms, using the capabilities of machine learning methodologies. The chapter begins by examining current MANET routing protocols, highlighting their fundamental attributes and challenges in dynamic and unpredictable network environments. To adapt to the changing characteristics of Mobile Ad hoc Networks (MANETs), machine learning algorithms are employed to forecast network circumstances, including connection quality, node mobility, and congestion. These factors have a substantial influence on the efficiency of routing. To assess the suggested method, comprehensive simulations are carried out employing well-known MANET routing protocols and diverse machine learning techniques. Performance measures, such as packet delivery ratio, end-to-end latency, and network throughput, are used to evaluate the efficiency of routing algorithms in various situations. The simulations yield valuable insights on the flexibility and robustness of routing protocols when combined with machine learning predictions. Moreover, the research examines the consequences of incorporating machine learning into MANET routing algorithms, taking into account aspects such as the computational burden and resources limitations inherent in mobile devices. Additionally, it examines the possibility of utilizing adaptive learning techniques to modify routing algorithms in response to current network circumstances flexibly. The study findings contribute to the ongoing discussion on enhancing the efficiency of Mobile Ad hoc Networks (MANETs) by providing a detailed understanding of how machine learning can be utilized to improve routing algorithms. The suggested method presents a hopeful path for future investigation and advancement in the field of mobile ad hoc networks, with possible uses in enhancing communication dependability and efficiency in various changing situations.

[*] **Corresponding author D. Gousiya Begum:** Department of CSE, BEST Innovation University (BESTIU), Andhra Pradesh, India; E-mail: 2022pcse058@bestiu.edu.in

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

Keywords: Adaptive learning, Machine learning, MANETs, Network conditions prediction, Performance evaluation, Routing algorithms.

INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are now recognized as a flexible and essential part of modern wireless communication systems. They provide a dynamic and self-organizing architecture that functions without requiring a pre-existing network backbone. These networks, renowned for their malleability and versatility, are utilized in a diverse range of fields, including military operations, disaster recovery, and everyday civilian communication. The efficacy of communication in MANETs is closely tied to the efficiency of the routing algorithms used, since these algorithms manage the unexpected and frequently changing network topology inherent in mobile ad hoc environments.

The intricate nature of MANETs, characterized by the movement of nodes, fluctuating connection quality, and possible network divisions, poses a significant obstacle for creating and executing reliable routing protocols. Conventional routing algorithms, although widely used, often struggle to cope with the inherent uncertainties and variations in network conditions. To enhance the flexibility and effectiveness of MANET routing, researchers have recognized the need for innovative solutions and have consequently employed machine learning as a supplementary tool.

This work undertakes a thorough investigation of the efficacy of MANET routing algorithms, with a particular emphasis on leveraging the potential of machine learning. The initial step of this work is a comprehensive examination of current MANET routing protocols, elucidating their advantages, constraints, and suitability in various situations. By understanding the complexities of these processes, we lay the groundwork for evaluating their efficiency and identifying areas for improvement. The incorporation of machine learning into MANET routing algorithms brings about a fundamental change in how the difficulties presented by dynamic network conditions are dealt with. Machine learning models have the ability to forecast important factors, including connection quality, node mobility patterns, and network congestion. This allows routing algorithms to make well-informed judgments in real-time. The objective of this technique is to increase the flexibility of MANETs by allowing routing algorithms to react proactively to dynamic circumstances, hence enhancing the overall efficiency and dependability of communication.As part of our analysis, we conduct comprehensive simulations using well-known MANET routing protocols and various machine learning methods. The performance evaluation utilizes key indicators like packet delivery ratio, end-to-end latency, and network throughput.

The outcomes derived from these simulations serve as the foundation for a detailed examination of how machine learning enhances the capacities of current routing algorithms within the setting of MANETs.

In addition to assessing performance, we examine the practical implications of incorporating machine learning into MANETs, considering factors such as the processing burden and resource limitations on mobile devices. In addition, we investigate the possibility of using adaptive learning processes to dynamically modify routing algorithms based on real-time predictions. This might lead to the development of more robust and flexible communication networks.This work offers a thorough investigation of the mutually beneficial connection between MANET routing methods and machine learning. The findings obtained from this analysis contribute to the continuous endeavors to enhance communication in MANETs, providing a promising direction for future research and development in the field of mobile ad hoc networks.

RELATED WORKS

The literature review provides a comprehensive summary of current research efforts that have concentrated on the convergence of Mobile Ad Hoc Networks (MANETs), routing algorithms, and machine learning approaches.

In 2018, Antonio Brogi *et al.* [1] conducted an extensive study that examined several elements of high-performance modeling and simulation within the framework of the COST Action IC1406 cHiPSet. Their work establishes a fundamental basis for understanding the complexities of simulation approaches, offering valuable insights into the broader scope of research related to MANETs. In 2023, T. A. Mohanaprakash *et al.* [2] proposed a deep learning method to forecast the lifespan of a Mobile Ad hoc Network (MANET) by employing Graph Adversarial Network Routing. This novel approach represents a significant advancement in utilizing deep learning to enhance the predictive capabilities of routing algorithms in dynamic and evolving MANET environments. In 2017, Ayushree and Sandeep Kumar Arora [3] did a comparison analysis that specifically examined the widely used routing protocols AODV and DSDV. Their study utilized a machine learning methodology, providing insights on the relative effectiveness of various protocols in different settings inside MANETs. In 2018, Srinath Doss and colleagues [4] introduced the APD-JFAD algorithm, which aims to effectively prevent and detect jellyfish assaults in MANETs. This study focuses on a crucial security issue, demonstrating the importance of integrating sophisticated methods to protect Mobile Ad hoc Networks (MANETs) against malicious assaults.

CHAPTER 9

Autonomous Drone Patrol and Surveillance System using Computer Vision

Tony Alosius S.[1,*], Kavin Velavan G.[1], Sriram K.[1], Manikandan S.[1], Surrenther I.[1] and **Sathya K.[1]**

[1] *Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India*

Abstract: The core objective was to create an innovative Autonomous Surveillance and Patrol System, uniting the realms of computer vision and drone technology. It addresses critical issues such as manual tracking in crowded or hard-to-reach areas, as well as tracking suspects within densely populated zones. The project distinguishes itself by incorporating YOLO v8, a state-of-the-art computer vision model, for precise object detection and facial recognition, thereby enabling effective facial tracking. Coupled with the versatility of the DJI Tello Nano drone, this offers a comprehensive solution to these challenges, adaptable to specific needs, all within a single integrated framework.

Keywords: Computer vision, Drone programming, Facial landmarks, Object detection, Ultralytics volov8.

INTRODUCTION

In an era where security and surveillance play an increasingly vital role in our lives, the development of innovative, efficient, and adaptable systems has never been more crucial. Our project, the "Autonomous Surveillance and Patrol System," represents a pioneering effort to revolutionize surveillance practices. By harnessing the power of cutting-edge technologies such as [1] computer vision and drone technology, we aim to address pressing challenges in surveillance and security.

The primary objective of this project was to create a comprehensive solution for a range of issues. These issues include the manual tracking of crowded zones [2] or areas that are challenging to survey by conventional means, as well as the tracking

* **Corresponding author Tony Alosius S.:** Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, India; E-mail: tony.aloysius.77@gmail.com

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

of suspects within narrow or overcrowded zones. These scenarios have traditionally presented significant difficulties for standard surveillance techniques.

What sets our project apart is the integration of the formidable YOLOv8 computer vision model, renowned for its object detection capabilities, and the Face Recognition model, which boasts a remarkable ability in facial recognition. This integration enables our system to perform precise facial tracking, significantly enhancing the accuracy and efficiency of surveillance efforts. Additionally, we have leveraged the versatility of the DJI Tello Nano drone, as shown in Fig. (**1**), a compact yet powerful aerial platform, to conduct surveillance operations that were previously beyond the scope of ground-based solutions. Small drones are proving to be a new opportunity for the civil and military industries [3].

Fig. (1). Dji tello nano drone.

The strength of our project lies not only in its innovation but also in its adaptability. We have designed the Autonomous Surveillance and Patrol System to be highly customizable, enabling it to meet the specific needs and requirements of various applications. It is a unified and integrated framework that serves as a one-stop solution for diverse surveillance challenges.

We believe that the Autonomous Surveillance and Patrol System holds the potential to redefine the landscape of surveillance and security, offering unparalleled capabilities in safeguarding critical areas and enhancing public safety [4]. A drone can perform tasks that require a lot of time and manpower in a short amount of time, single-handedly. From being fully controlled by humans with the help of a remote, it has now become a self-controlled entity in terms of flight missions.

TECHNOLOGY STACK

Computer Vision

Computer vision is a field of artificial intelligence that focuses on enabling computers to interpret and understand visual data from the world, often using cameras. It involves processing image and video inputs, preprocessing to enhance data quality, feature detection and extraction, object detection and recognition, facial recognition, optical flow for tracking object movement, machine learning models for complex tasks, and post-processing of results. The outcomes of computer vision tasks can be integrated into drone control systems for decision-making, enabling applications such as obstacle avoidance alert systems, object tracking, and autonomous navigation.

Drone Programming

Drone programming encompasses the software stack used to control and operate unmanned aerial vehicles (UAVs) [5]. It includes flight control software for managing drone movement and stability, APIs and SDKs for interaction with drone hardware, navigation and path planning algorithms for autonomous flight, telemetry and communication systems, computer vision integration for visual data processing, remote piloting interfaces, mission planning software for defining flight paths, and simulation environments for safe testing and development. The smaller drones suggested in this paper require less time and resources for maintenance compared to larger UAVs used by the military, and are less prone to false alarms or malfunctions [6].

PATH PLANNING

In the dynamic landscape of modern emergency response, envision a highly sophisticated autonomous drone that not only extends its flight time but sets a new standard for comprehensive vigilance and rapid intervention. This drone, with its remarkable 25–30-minute flight endurance, represents a quantum leap in the field, as it seamlessly integrates a suite of innovative features that elevate its role in safeguarding communities. The human tracking functionality of this drone is a game-changer, empowering it to swiftly and accurately identify potential culprits during crises. It does so with precision and speed, enabling authorities to apprehend suspects or provide critical information to law enforcement in a timely manner. This feature not only enhances the efficiency of emergency response but also significantly improves the chances of identifying and addressing threats effectively.

CHAPTER 10

Security and Privacy Concerns in Smart Systems

Akhil Singampalli[1,*], Anil Pise[2], Dharma Teja Singampalli[3] and **Vrushali Deshpande[4]**

[1] *Department of Computer Science and Engineering, Vignan's Institute of Information Technology, India*

[2] *Cumulus Solutions, Johannesburg, South Africa*

[3] *Sagility, Bangalore, India*

[4] *D&M Tech, Pune, India*

Abstract: The chapter on "Security and Privacy Concerns in Smart Systems" explores the complex landscape of securing interconnected smart technologies. It begins with an elucidation of smart systems, encompassing Internet of Things (IoT), smart homes, cities, and industrial applications, emphasizing their efficiency and convenience. Subsequently, the narrative shifts to outlining the multifaceted security and privacy challenges inherent in these systems, emphasizing the imperatives of user trust and technological optimization. A detailed exposition on common security threats, including cyberattacks and data breaches, is provided, accompanied by illustrative case studies. Privacy concerns, such as data collection, user consent, and surveillance, are scrutinized, and bolstered by pertinent examples. The chapter culminates in a discussion of best practices, emerging technologies, and future trends, advocating for a holistic approach to fortify the security and privacy posture of smart systems in a rapidly evolving digital landscape.

Keywords: Cybersecurity, Cyberattacks, Data breaches, Distributed denial of service (DDoS), Internet of things (IoT), Privacy concerns, Smart systems.

INTRODUCTION

In the digital age, technology has become an integral part of our daily lives, revolutionizing the way we live, work, and interact with our surroundings. The emergence of smart systems has ushered in a new era of efficiency, convenience, and automation, promising to streamline processes and enhance our quality of life. However, amidst this rapid advancement, the spectre of security and privacy concerns looms large, casting a shadow over the potential benefits of these innovative technologies.

[*] **Corresponding author Akhil Singampalli:** Department of Computer Science and Engineering, Vignan's Institute of Information Technology, India; E-mail: singampalliakhil@gmail.com

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

Recent years have witnessed an unprecedented proliferation of smart technologies, revolutionized industries, and the reshaping of daily life. From interconnected IoT devices to sophisticated smart city infrastructures, the integration of technology has promised unparalleled efficiency and convenience. However, amidst this rapid advancement, the spectre of security and privacy concerns looms large [1]. With each innovation, the imperative to safeguard user data and preserve privacy becomes increasingly pressing.

As smart systems become more prevalent, they bring significant security and privacy challenges. These concerns arise from the vast amounts of data collected, the potential for cyberattacks, and the need for robust data protection mechanisms. Ensuring the security and privacy of smart systems is critical to gaining user trust and realizing the full potential of these technologies. Fig. (**1**) shows the integration of network devices and technologies.

Fig. (1). Networked devices and technological integrations.

Addressing security and privacy concerns in smart systems is crucial for several reasons. First, it protects sensitive user data from unauthorized access and misuse. Second, it ensures the reliability and integrity of smart systems, preventing disruptions and potential hazards. Third, addressing these concerns fosters user confidence and promotes wider adoption of smart technologies.

SMART SYSTEMS - AN OVERVIEW

Smart systems encompass a wide range of applications and technologies, each designed to enhance our daily lives and optimize various processes. From the IoT to smart homes, cities, and industrial settings, these interconnected systems leverage advanced computing, sensors, and communication technologies to offer improved efficiency, convenience, and automation. Fig. (**2**) illustrates how smart systems have evolved over time.

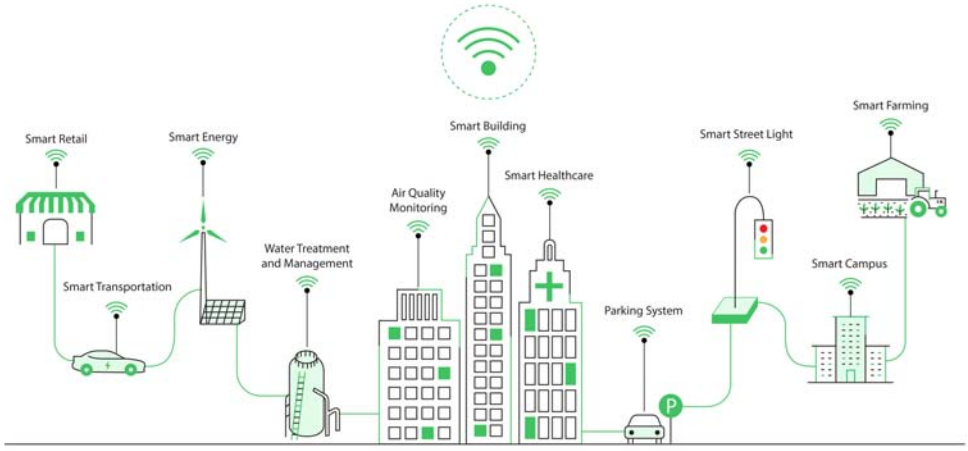

Fig. (2). Image illustrating iot, smart home, smart cities, and industrial iot.

Within the realm of smart cities, initiatives such as Barcelona's implementation of IoT sensors for smart parking and waste management, or Singapore's utilization of data analytics for traffic optimization and urban planning, exemplify the transformative potential of smart technologies in enhancing quality of life and sustainability.

Types of Smart Systems

1. **Internet of Things (IoT):** The IoT refers to a network of physical devices, vehicles, home appliances, and other objects embedded with sensors, software, and connectivity, enabling them to collect and exchange data. IoT devices permeate our daily lives, encompassing a wide range of products, from smart thermostats and wearable fitness trackers to connected vehicles and industrial machinery. These devices can be remotely monitored and controlled, offering enhanced convenience and efficiency.

Within the realm of IoT, examples abound:

CHAPTER 11

Guardians of the Grid: Navigating Security and Privacy in Smart Systems

Anil Pise[1,*], Dharma Teja Singampalli[2], Yogesh Khandokar[3] and **Vrushali Deshpande[4]**

[1] *Cumulus Solutions, Johannesburg, South Africa*

[2] *Sagility, Bangalore, India*

[3] *Beamline Scientist MX, Australia*

[4] *D&M Tech, Pune, India*

Abstract: In the rapidly evolving landscape of technology, the intersection of smart systems and machine learning holds immense potential for shaping the future. This chapter explores the visionary outlook for smart systems and machine learning, envisioning transformative possibilities and pathways to their realization across diverse domains, while addressing the challenges and opportunities that accompany these groundbreaking technologies.

Keywords: Artificial intelligence (AI), Autonomous mobility, Algorithmic bias, Cybersecurity risks, Deep learning, Ethical considerations, Internet of things (IoT), Industry 4.0, Intelligent manufacturing, Machine learning, Personalized healthcare, Precision agriculture, Sustainable urbanization, Smart systems.

INTRODUCTION

As we stand at the cusp of a technological revolution, the integration of smart systems and machine learning emerges as a pivotal force driving innovation and progress. These technologies are poised to revolutionize industries, streamline processes, and enhance human experiences in unprecedented ways. This introductory section sets the stage for exploring the visionary landscape of smart systems and machine learning, their underlying principles, and their far-reaching implications [1].

* **Corresponding author Anil Pise:** Cumulus Solutions, Johannesburg, South Africa; E-mail: anil@cumulussolutions.co.za

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

Understanding Smart Systems and Machine Learning

Smart systems, as shown in Fig. (**1**), encompass a spectrum of interconnected devices and platforms designed to operate autonomously or semi-autonomously, leveraging advanced computational capabilities to perceive, analyze, and respond to their environment intelligently. These systems leverage a range of technologies, including the Internet of Things (IoT), artificial intelligence (AI), and sophisticated sensor networks, to gather and process data from the physical world.

Fig. (1). Smart system architecture.

At the core of smart systems lies machine learning, a subset of AI that enables these systems to learn from data, identify patterns, and make decisions without explicit programming. Machine learning algorithms are trained on vast datasets, allowing them to uncover intricate relationships and patterns that would be challenging or impossible for humans to discern manually.

Techniques such as neural networks, deep learning, and reinforcement learning enable machine learning algorithms to excel in a wide range of tasks, including

image recognition, natural language processing, predictive analytics, and autonomous control [2]. These algorithms continuously refine their decision-making capabilities through iterative learning, adapting to new data and scenarios with remarkable flexibility as shown in Fig. (**2**).

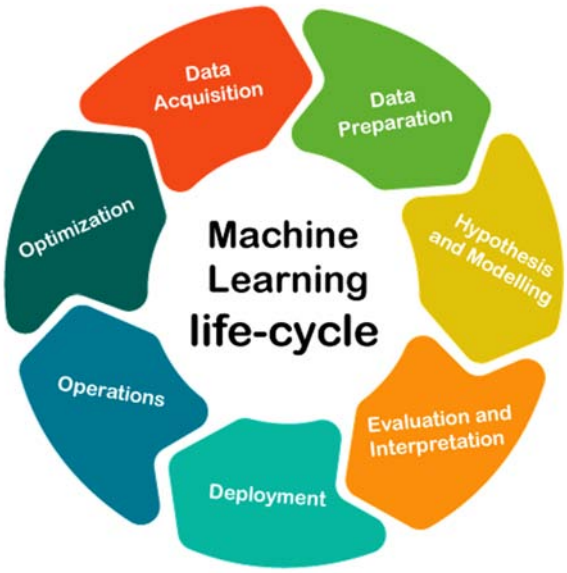

Fig. (2). Machine learning process.

Visionary Applications

The vision for the future of smart systems and machine learning extends across diverse domains, promising to redefine industries and revolutionize human experiences. In this section, we explore several visionary applications poised to reshape our world, highlighting their transformative potential and the profound impacts they may have on our daily lives.

Autonomous Mobility

Autonomous mobility as shown in Fig. (**3**), represents a transformative leap in transportation, where self-driving vehicles navigate roads seamlessly, offering safer, more efficient, and convenient travel experiences. Through the utilization of machine learning algorithms, these vehicles perceive their surroundings using a suite of sensors, including LiDAR (Light Detection and Ranging), radar, and high-resolution cameras, enabling them to make real-time decisions to navigate traffic, avoid obstacles, and ensure passenger safety.

CHAPTER 12

Identifying DDoS Threats in Digital Forensics Using Transfer Learning Techniques

Saswati Chatterjee[1], Vijaykumar Jayantibhai Solanki[2], Lalmohan Pattnaik[3], Mukesh Chaudhary[1] and **Suneeta Satpathy[4,*]**

[1] *Parul University Vadodara, Gujarat, India*

[2] *Government Engineering College Bharuch, Gujarat, India*

[3] *Sri Sri University, Cuttack, Odisha, India*

[4] *Center For Cyber Security, SoA Deemed to be University, Bhubaneswar, Odisha, India*

Abstract: Digital investigations in cybersecurity are crucial for spotting and addressing cyber threats like Distributed Denial of Service (DDoS) attacks. With DDoS attacks becoming more complex and widespread, traditional forensic techniques struggle to keep up with these evolving threats. To tackle this challenge, this chapter suggests a new method for forensics investigation centered on DDoS attacks. By drawing on insights from studies on DDoS attack detection and transfer learning methods, the proposed approach aims to boost the effectiveness and precision of investigations within networking environments. The proposed framework is designed for conducting investigations that cater to the unique aspects of DDoS attacks by integrating expert systems, fuzzy logic, and deep transfer learning. A clustering-enhanced Transfer Learning strategy named CeHTL is implemented to detect connections between known attacks. This method was tested when the test dataset consisted of types or subtypes of attacks not found in the training data. Standard classification models like decision trees and KNN, alongside innovative transfer learning techniques, are used as benchmarks. The outcomes demonstrated enhancements in performance with the proposed CeHTL, utilizing trapezoidal Membership function generation methods, which showcased its effectiveness in identifying new network threats.

Keywords: CeHTL, Machine learning, Network attack threat, Transfer learning.

INTRODUCTION

In recent years, it has become a trend to get agility and cost savings from how organizations manage and deploy their IT infrastructure. Digital transformation

[*] **Corresponding author Suneeta Satpathy:** Center For Cyber Security, SoA Deemed to be University, Bhubaneswar, Odisha, India; E-mail: suneeta1912@gmail.com

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

has created new challenges, the most significant of which is probably cybersecurity. In an era of constantly growing devices and networks, one of the greatest cybersecurity threats organizations face is the Distributed Denial of Service (DDoS) attack. As the type of DDoS attacks designed to compromise internet service availability, they present a widespread threat to all categories of enterprises. DDoS invaders attack the intended systems with harmful congestion, blocking authorized individuals from accessing programs, websites, and other online resources. For researchers, promptly gathering, analyzing, and retaining technological proof often poses a challenge, delaying incident response and mitigation. This study introduces a novel approach to digital security inquiry, focusing on DDoS attacks against various computer systems. The proposed method makes use of recent leverages recent advances in transfer learning and DDoS threat detection to enhance the effectiveness and precision of queries. The proposed approach, which integrates cybersecurity, cutting-edge technologies, and mathematical principles, can enable businesses to effectively safeguard their critical assets and mitigate the impact of denial-of-service attacks. This paper provides a comprehensive explanation of the proposed technique, detailing its key components, implementation methods, and potential benefits for businesses susceptible to DDoS attacks. Through empirical evaluations and real-world experiences, the study also shows the practical effectiveness of the adopted strategies. Overall, the research adds to the expanding corpus of knowledge in digital forensics and cybersecurity by providing insightful analysis and useful suggestions for businesses looking to strengthen their defenses against DDoS attacks. Government, military, and industrial networks are particularly vulnerable to complex DDoS attacks, which can result in severe disruptions and data breaches. Because traditional signature-based detection methods rely on well-known patterns of criminal activity, they often struggle to handle the dynamic and complex nature of contemporary cyber threats. Attackers are continually devising new strategies; therefore, these traditional approaches are insufficient. Consequently, it is imperative to design and implement sophisticated anomaly detection techniques. These state-of-the-art methods focus on identifying anomalous patterns and behaviors in network traffic that deviate from the norm, thereby revealing dangers that signature-based systems may overlook. Artificial intelligence and machine learning enable anomaly detection systems to learn, adapt, and identify threats more successfully in real time. This improves the security posture of different network settings. This proactive strategy is essential for reducing the risks associated with the dynamic and increasingly sophisticated cyber threats of today. DDoS assaults employ the same attack approach as DoS attacks, with the exception that a sizable number of controlled zombie devices carry out the attack [1]. Dispersed Zombies flood the targeted device with requests, depleting its resources and finally bringing down the service. Research

indicates that, although more methods are being employed to maintain network security, DDoS attacks are becoming more advanced and destructive to networks over time [2]. The remaining sections of the document are arranged as follows: Section 2 covers related work, and Section 3 summarizes the transfer learning paradigm for identifying attacks. The Transfer Learning Approach *via* Spectral Transformation is explained in Section 4. The proposed architecture is shown in Section 5, and the experimental findings are explained in Section 6. Section 7 concludes the study and outlines potential directions for future research.

Related Work

There has been an increase in research efforts in the past several years to improve DDoS attack detection and mitigation in various scenarios. Due to the size of contemporary network infrastructures and the evolution of attack strategies, traditional approaches to DDoS attack detection, such as signature-based and anomaly-based methods, have proven to be inadequate. Signature-based detection techniques recognize bad traffic by comparing it to established patterns or signatures of DDoS attacks. These techniques work well against well-known attack vectors, but they are less successful in identifying new or zero-day assaults since they lack recognizable signatures. Even though anomaly-based techniques can identify assaults that have never been observed before, they frequently have a high false-positive rate and are not very scalable. Researchers have resorted to machine learning methods, especially deep learning, for DDoS attack detection as a result of these constraints. Transfer learning techniques enable models to leverage data from related tasks or domains, which may help overcome this restriction. By leveraging such knowledge, models that have fewer information points for an activity might perform better. The objective of this method is to transfer data from a larger source domain to a smaller destination domain. The literature describes several approaches to learning transfer, such as feature-based, model-based, and instance-based methods. Threats are frequently detected using anomaly detection [3, 4], as it searches for peculiar patterns that deviate from normal behavior. However, this method relies heavily on features derived from expert knowledge, which might result in a high rate of false positives. A rapidly developing field in machine learning, called transfer learning, makes it easier to create reliable models that can take on new tasks with minimal effort. Many successful applications have been made of it in domains such as natural language processing and visual identification. Transfer learning can be used to improve DDoS detection algorithms. Despite the lack of thorough formalization in findings, the researchers proposed that transfer learning could improve the identification of unknown malware across different environments [5]. In one study, instance-based transfer learning was applied to network intrusion detection; nevertheless, a significant amount of labeled data from the target domain was

CHAPTER 13

Rising Concerns: Cybercrime & Financial Fraud in the Indian Context

Preethi Nanjundan[1,*], Blesson Varghese James[2], Arushi Sharma[2] and **Aryan Gupta[2]**

[1] *Department of Data Science, CHRIST University, Lavasa Campus, Pune, India*

[2] *Department of Commerce, CHRIST University, Lavasa Campus, Pune, India*

Abstract: This chapter examines the prevalence and impact of cybercrime in India, focusing on various cyber threats and their consequences on individuals, businesses, and society. Drawing on data collected from a diverse sample of participants aged 15 to 67, the study reveals alarming statistics: over 70% of respondents reporting exposure to cybercrime. The most prevalent forms of cybercrime include online payment fraud, identity theft, phishing, and malware attacks. The chapter also explores the emotional and psychological impact of cybercrime, highlighting its profound effects on victim trust and mental well-being. In response to cyber threats, the study finds that individuals often bolster their security measures or decrease their online activity, reflecting a heightened vulnerability and distrust in digital platforms. Regression analysis reveals correlations between age groups and cybercrime victimization, emphasizing the need for targeted interventions and digital literacy initiatives. The findings underscore the urgent need for comprehensive cybersecurity measures, user education, and support structures to mitigate the impact of cybercrime and foster a safer online environment for all.

Keywords: Cybercrime, Cybersecurity, Digital literacy, Financial fraud, Identity theft, Malware attacks, Online payment scam, Phishing, Psychological impact, Regression analysis, Trust in online platforms.

INTRODUCTION

Cybercrime poses a significant and rapidly evolving threat in a globalized world, particularly in emerging economies. Defined as illegal activity utilizing the internet and information technology, cybercrime manifests in various forms, impacting businesses through unauthorized access and manipulation. The negative consequences necessitate a rigorous managerial approach for identification, recovery, and detection [1]. While cybercrime often seeks financial gain, motives

[*]**Corresponding author Preethi Nanjundan:** Department of Data Science, CHRIST University, Lavasa Campus, Pune, India; E-mail: preethi.n@christuniversity.in

Suneeta Satpathy, Sachi Nandan Mohanty & Subhendu Kumar Pani (Eds.)

can also be political or personal, with perpetrators ranging from highly skilled organized groups to inexperienced individuals. Emerging countries face heightened vulnerability due to intrinsic weaknesses in their security systems, making them susceptible to silent, "stalking"-like cyberattacks with potentially devastating economic and business consequences. Therefore, addressing and mitigating cybercrime demands ongoing attention and comprehensive strategies. Modern technology provides highly advanced tracking means that are seemingly untraceable and undetectable. Metaphorically, cyberattacks are based on two particular cracks in the security system, and their approach is identified with silent stalking (tracking). This criminal activity has highly harmful consequences for economic and business targets. This has increased the prevalence of online financial fraud victimization. A growing wave of cybercrime has negatively impacted the goodwill and economic growth of financial institutions, both directly through the loss of trust in digital infrastructure and indirectly through fraud and extortion in both developing and developed countries [2].

Fraudsters are continually evolving their approaches to exploit the vulnerabilities of current prevention measures, with many targeting the financial sector. These crimes include credit card fraud, healthcare and automobile insurance fraud, money laundering, securities and commodities fraud, and insider trading [3]. Phishing is one of the various social engineering tactics used by cybercriminals to deceive technical users into disclosing sensitive or financial information through malicious websites that appear legitimate. Malware is malicious software designed to disrupt computer system(s) and is heavily used by cybercriminals to solicit monetary funds fraudulently. Furthermore, malware and phishing are social engineering tactics commonly used by cybercriminals to defraud unsuspecting users. Moreover, malware and phishing are social engineering tactics widely used by cybercriminals to defraud unsuspecting users.

The COVID-19 pandemic has dramatically shifted societal norms, driving a mass transition towards online work, shopping, and social interactions. This digital migration has not gone unnoticed by cybercriminals, who have capitalized on the increased reliance on online services to develop innovative and diverse attack methods. As individuals and institutions transition from physical spaces to the digital realm, their vulnerability to cybercrime increases, potentially leading to service disruptions, financial losses, data breaches, and widespread anxiety. This chapter delves into the interplay between pandemic-driven behavioral shifts, the evolving landscape of cybercrime, and the resulting consequences for individuals and institutions [4]. COVID-19 had a significant impact on every sector. The rapid digitization of the banking sector has significantly impacted its stability and risk profile, driven by technological advancements and the increasing threat of cyberattacks [5, 6]. Exploiting the anonymity and interconnectedness of online

systems, cybercriminals pose a growing challenge, yet the link between sustainability and stability under such threats remains understudied and debated [7]. Researching cybercrime and its impact is crucial for the banking industry, particularly considering the rising prevalence of insider-driven attacks [8]. These attacks have witnessed a staggering 160% increase between 2019 and 2020 [9].

Financial institutions face significant losses, uncertainty, and funding restrictions due to cyberattacks [10]. A single insider-led cybercrime can trigger substantial economic losses, intellectual property theft, and erode customer trust [11]. The repercussions extend beyond individual institutions, impacting the entire financial ecosystem and stakeholders like customers, regulators, and employees [12] (Ferracane, 2019). Therefore, preventing and mitigating insider fraud is paramount [13, 14]. Cybercrime can be controlled using digital technology, and computer networks will also require a variety of new networks, including those between police and other agencies within the government, between police and private institutions, and across national borders [15]. Issues of effectiveness and relevance of national fraud strategies, the absence of incentives and identifiable benefits, and the continuous influence of competing agendas on three police priorities continue to marginalize fraud as a mainstream police function, limiting the level of resources committed to what remains a rising area of criminality [16]. Techniques like Anomaly detection have been intensively studied by researchers over the last few decades for this purpose, with many employing statistical, artificial intelligence, and machine learning models. Supervised learning algorithms have been the most widely studied models in research until recently. However, supervised learning models are associated with numerous challenges, which can be addressed by semi-supervised and unsupervised learning models proposed in recent literature. This chapter will focus on the economic, social, and psychological consequences for individuals, businesses, and society. It will quantify the financial losses, reputational damage, and emotional distress caused by cybercrime.

LITERATURE REVIEW

Introduction to Cybercrime in the Banking Sector

Here is an explanation that aligns with the research issue and the aim outlined in the introduction. Prior studies will be evaluated to establish a well-founded thesis for a thorough literature review, which aims to replace the existing knowledge base. Stress the broad range of computer crimes from which the bank industry stands to lose, including unauthorized intrusion, credit/ debit card fraud, money laundering, employee embezzlement, pharming, phishing, malware, hacking, virus, spam, and advanced fee fraud.

SUBJECT INDEX

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Suneeta Satpathy

Dr. Suneeta Satpathy is an Associate Professor at the Center for Cyber Security, SOA University, Bhubaneswar, with a Ph.D. in Computer Science from Utkal University (2015) supported by the Directorate of Forensic Sciences, MHA scholarship. Her research focuses on Computer Forensics, Cyber Security, Data Fusion, Data Mining, Big Data Analysis, and Decision Mining. She has edited books with Springer, Wiley, CRC AAP, and NOVA Publications, published widely in reputed international journals and conferences, and guided numerous graduate and postgraduate students. Actively engaged in professional service, she is a reviewer or editorial board member for leading journals such as Robotics and Autonomous Systems (Elsevier), Computational and Structural Biotechnology Journal (Elsevier), and Journal of Big Data (Springer). She is also an active member of CSI, ISTE, OITS, IE, Nikhil Bharat Shiksha Parisad, and IEEE.

Sachi Nandan Mohanty

Dr. Sachi Nandan Mohanty, ranked among the Top 2% World Scientists by Stanford University and Elsevier (2023–2025), completed his postdoctoral research at IIT Kanpur and Ph.D. at IIT Kharagpur with an MHRD fellowship. He has published over 240 research papers and authored/edited 42 books with leading publishers including Springer, Wiley, CRC Press, and IEEE-Wiley. His research covers Data Mining, Big Data Analytics, Cognitive Science, Fuzzy Decision Making, Brain–Computer Interface, and Computational Intelligence. Recipient of multiple awards including the Best Ph.D. Thesis Award (2015) from the Computer Society of India and four Best Paper Awards, he has guided nine Ph.D. scholars and 23 postgraduates. A Fellow of IEI and IETE, Senior Member of IEEE, and Ambassador of EAI, he also serves as Editor-in-Chief of EAI Transactions on Intelligent Systems and Machine Learning Applications.

Subhendu Kumar Pani

Dr. Subhendu Kumar Pani is a Professor at Krupajal Engineering College, Biju Patnaik University of Technology, Odisha, and serves as Editor-in-Chief of multiple international book series with Routledge (Taylor & Francis), CRC Press, Wiley, Bentham Science, and NOVA Publishers. He has also been a guest editor for journals such as the MDPI Journal of Sensors. His multidisciplinary research spans Artificial Intelligence, Health Informatics, IoT, Collective Computational Intelligence, Robotics, Social Computing, Web Intelligence, Web Services, and Data Mining, with over 300 research publications, including 40+ books and 80+ Scopus-indexed works. Actively engaged in global academia, he has organized numerous conferences, contributed to over 150 international program committees, and served on several editorial boards. Recognized with five prestigious research awards, Dr. Pani earned his Ph.D. in Computer Science from Utkal University (2013) and M.Tech. from KIIT University (2007). He is a Fellow of the Scientific Society of Advanced Research and Social Change and a life member of IE, ISTE, ISCA, OBA, OMS, SMIACSIT, SMUACEE, and CSI.