ADVANCES IN AI FOR FINANCIAL, CYBER, AND HEALTHCARE ANALYTICS

A MULTIDISCIPLINARY APPROACH

Editors:
Ashwani Kumar
Mohit Kumar
Avinash Kumar Sharma
Yojna Arora

Bentham Books

Advances in AI for Financial, Cyber, and Healthcare Analytics: A Multidisciplinary Approach

Edited By

Ashwani Kumar
School of Computer Science Engineering and Technology
Bennett University, Greater Noida, India

Mohit Kumar
Department of Computer Science and Engineering
Amity University Ranchi– 834001 Jharkhand
India

Avinash Kumar Sharma
School of Engineering and Technology
Sharda University, Greater Noida, India

&

Yojna Arora
School of Engineering and Technology
Sharda University, Greater Noida, India

Advances in AI for Financial, Cyber, and Healthcare Analytics: A Multidisciplinary Approach

Editors: Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora

ISBN (Online): 979-8-89881-054-2

ISBN (Print): 979-8-89881-055-9

ISBN (Paperback): 979-8-89881-056-6

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA. All Rights Reserved.

First published in 2025.

BENTHAM SCIENCE PUBLISHERS LTD.

End User License Agreement (for non-institutional, personal use)

This is an agreement between you and Bentham Science Publishers Ltd. Please read this License Agreement carefully before using the ebook/echapter/ejournal (**"Work"**). Your use of the Work constitutes your agreement to the terms and conditions set forth in this License Agreement. If you do not agree to these terms and conditions then you should not use the Work.

Bentham Science Publishers agrees to grant you a non-exclusive, non-transferable limited license to use the Work subject to and in accordance with the following terms and conditions. This License Agreement is for non-library, personal use only. For a library / institutional / multi user license in respect of the Work, please contact: permission@benthamscience.org.

Usage Rules:

1. All rights reserved: The Work is the subject of copyright and Bentham Science Publishers either owns the Work (and the copyright in it) or is licensed to distribute the Work. You shall not copy, reproduce, modify, remove, delete, augment, add to, publish, transmit, sell, resell, create derivative works from, or in any way exploit the Work or make the Work available for others to do any of the same, in any form or by any means, in whole or in part, in each case without the prior written permission of Bentham Science Publishers, unless stated otherwise in this License Agreement.
2. You may download a copy of the Work on one occasion to one personal computer (including tablet, laptop, desktop, or other such devices). You may make one back-up copy of the Work to avoid losing it.
3. The unauthorised use or distribution of copyrighted or other proprietary content is illegal and could subject you to liability for substantial money damages. You will be liable for any damage resulting from your misuse of the Work or any violation of this License Agreement, including any infringement by you of copyrights or proprietary rights.

Disclaimer:

Bentham Science Publishers does not guarantee that the information in the Work is error-free, or warrant that it will meet your requirements or that access to the Work will be uninterrupted or error-free. The Work is provided "as is" without warranty of any kind, either express or implied or statutory, including, without limitation, implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the results and performance of the Work is assumed by you. No responsibility is assumed by Bentham Science Publishers, its staff, editors and/or authors for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products instruction, advertisements or ideas contained in the Work.

Limitation of Liability:

In no event will Bentham Science Publishers, its staff, editors and/or authors, be liable for any damages, including, without limitation, special, incidental and/or consequential damages and/or damages for lost data and/or profits arising out of (whether directly or indirectly) the use or inability to use the Work. The entire liability of Bentham Science Publishers shall be limited to the amount actually paid by you for the Work.

General:

1. Any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims) will be governed by and construed in accordance with the laws of Singapore. Each party agrees that the courts of the state of Singapore shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims).
2. Your rights under this License Agreement will automatically terminate without notice and without the

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

CONTENTS

FOREWORD

In the past few years, the world of finance has experienced a seismic shift. Traditional financial analysis, relying heavily on historical data, human intuition, and static models, is now being supplemented, if not outright transformed, by the power of data science and machine learning. As financial markets continue to evolve in complexity and speed, the need for more sophisticated tools to analyze, predict, and optimize financial outcomes has never been greater. Against this background, machine learning for financial analytics emerges as a timely and necessary guide for professionals working within this new context. Financial data is best suited to machine learning techniques, as it possesses high volumes, variety, and velocity, characteristics that help identify patterns in large datasets, make predictions, and adapt to new information. From algorithmic trading to fraud detection, risk management to portfolio optimization, machine learning offers innovative solutions to some of the most pressing challenges in finance today. This book provides a comprehensive and approachable guide for those eager to harness the power of machine learning in the financial domain.

It also discusses how the techniques of machine learning could be used to provide new insights, improve forecasting, and optimize decisions in finance. The book easily navigates the challenges by giving the technical depth needed to understand the algorithms and the financial context necessary for their application. This is more than an academic resource; this is a practical guide to the future of finance. As we look forward, data-driven decision-making will continue to grow, and machine learning will be at the heart of this transformation. This book will provide you with the knowledge and tools needed to succeed in this fast-changing field if you are a financial analyst, a data scientist, an investor, or a student with an interest in the intersection of technology and finance. In the chapters that follow, you will embark on a journey that will reshape your understanding of both finance and machine learning.

Pradeep Kumar Gupta
Computer Science & Engineering and Information Technology
Jaypee University of Information Technology
Solan H.P, India

PREFACE

The intersection of machine learning (ML) and finance has emerged as a transformative force, reshaping the way financial professionals analyze markets, predict trends, and manage risks. As financial systems become increasingly complex and data-driven, traditional methods of analysis are no longer sufficient to handle the scale and intricacies of modern financial markets. Machine learning gives the ability to extract insights from vast datasets, identify patterns that may not be easily observed, and develop predictive models that inform decision-making for improved financial performance. This book will present an introduction to the application of machine learning techniques in financial analytics through an exploration of theoretical foundations and practical implementations in the subject area. We will examine core concepts of machine learning: supervised and unsupervised learning, as well as reinforcement learning. They will be applied in solutions to different financial problems, including the application of algorithmic trading, risk management, portfolio optimization, fraud detection, and market forecasting. As financial institutions and investment firms increasingly rely on data-driven insights to gain a competitive edge, the principles of machine learning have become essential for professionals looking to navigate the evolving landscape of financial analytics. This book aims to provide the reader with a broad view of how machine learning can be applied to solve real-world financial problems and the tools and techniques that need to be mastered to facilitate these solutions effectively.

In all chapters, we balance theory with practice by incorporating case studies, coding examples, and industry insights to guide the reader step by step in the process of designing, implementing, and evaluating machine learning models for financial analytics. Whether you are a financial analyst, data scientist, or a student eager to explore the vast potential of this exciting field, this book will serve as a valuable resource to help you build the knowledge and skills necessary to leverage machine learning in the financial sector. As the integration of technology and finance is becoming ever more intimate, machine learning is not only a tool but a paradigm for a new approach to financial analysis and decision-making. It is our hope that this book will inspire and equip you to engage with the dynamic field of financial analytics, unlocking new opportunities for innovation and growth.

Content and Organization

Chapter 1 explores how financial analytics is being revolutionized, transforming the ways institutions analyze data, manage risks, and make informed decisions. With the rapid growth in volume and complexity of financial data, machine learning enables organizations to uncover valuable insights and maintain a competitive edge. By leveraging advanced algorithms, financial firms can improve predictions, optimize investment strategies, and detect fraud more effectively. Nevertheless, challenges, such as ensuring data quality, dealing with non-stationary data, and enhancing model interpretability, must be addressed. Overcoming these obstacles is crucial to fully harnessing machine learning transformative potential in the financial sector and making it more transparent, adaptable, and reliable in dynamic environments.

Chapter 2 discusses that human activity recognition (HAR) helps in segregating and distinguishing human actions among data generated from numerous sensing modalities. In this review, an exploration of Deep Learning models for HAR is considered, focusing on advancements in CNN and LSTM architectures. Deep Learning models have considerably outperformed traditional machine learning approaches owing to their capacity for automatically extracting both spatial and temporal features. Furthermore, attention mechanisms, such as the self-attention and Squeeze and Excitation modules, have significantly enhanced model performance by focusing on relevant feature maps and recalibrating them adaptively. This review also highlights hybrid models that combine CNN and LSTM for more accurate HAR, especially when working with sensor-based datasets. Additionally, the incorporation of attention mechanisms not only boosts accuracy but also optimizes the complexity of the models. Key trends in attention-driven deep learning methods are examined, indicating their growing importance in real-world human activity recognition applications.

Chapter 3 provides the classification of acute leukemia and myeloid neoplasm using ResNet leverages deep learning for accurate diagnosis of hematological disorders. ResNet (Residual Network), a convolutional neural network architecture, is used to process microscopic blood smear images and classify cell abnormalities effectively. By utilizing residual connections, ResNet overcomes the vanishing gradient problem, enabling deep networks to learn complex features. This approach automates and improves diagnostic accuracy, reducing dependency on manual interpretation. The method is particularly effective for distinguishing between various subtypes of leukemia and myeloid neoplasms, aiding in early detection and personalized treatment strategies. Experimental results typically demonstrate high accuracy, showcasing the potential of ResNet in medical image analysis.

Chapter 4 examines the moral ramifications of AI decision-making in fields ranging from criminal justice and employment to healthcare and finance. There are numerous advantages to incorporating AI technologies into routine tasks, including improved accuracy and efficiency as well as data-driven insights. Algorithmic bias, which can result in discriminatory actions against minority groups, is one of the main issues discussed in this chapter. Since users and other affected parties frequently lack the knowledge necessary to refute the reasoning behind automated judgments, responsibility and trust have become increasingly prominent. Furthermore, where AI is at the crossroads of numerous human rights concerns, for instance, invasion of privacy and potential debasement of civil liberties, society faces direct challenges.

Chapter 5 deals with anticipating cyber threats using AI predictive learning as a proactive cybersecurity strategy. AI analyzes data, detects patterns, and raises alerts for emerging risks. Known attacks are handled with signature-based identification, while real-time monitoring, data preprocessing, and continuous learning improve threat detection. Machine Learning algorithms, anomaly detection, and behavioral analysis strengthen the system's predictive ability. This approach adapts to changing threats, safeguarding sensitive information and public trust while reducing risks. This concept aligns with "machine learning for financial analytics," as both fields use data-driven models for prediction. In finance, ML analyzes market trends and detects anomalies to predict risks. Similarly, AI in cybersecurity uses pattern recognition to predict and counter threats. Both fields depend on real-time data analysis, pattern detection, and continuous adaptation.

Chapter 6 explores IoT as a technique for smart home authentication. IoT refers to a network of physical objects, also known as "things," that are embedded with electronics, software, and other technologies that enable them to communicate and exchange data with one another and with other connected devices and systems over a network, such as the Internet [1]. In recent years, the Internet of Things has emerged as one of the most significant technological advancements. Due to its increasing popularity, IoT has become increasingly prominent in ordinary day-to-day activities and applications.

Chapter 7 discusses channel response measurements and analyzes the human body as a medium for biometric applications. Today, digital systems control every facet of human life, allowing more individuals to get the services they need through a variety of channels. Personal identification of smart devices based on biometric recognition, which uses an individual's unique biological characteristics to verify their identity, has become a viable option in recent years.

Chapter 8 deals with artificial intelligence (AI), which improves cybersecurity by offering advanced tools to detect and mitigate threats with efficiency. AI-enabled security systems analyse large volumes of data in real-time and recognize suspicious patterns. Machine learning-based models enable proactive threat detection by continuously learning from historical attack patterns. The proposed work contributes to understanding the role of AI in safeguarding digital ecosystems. The key contribution is its focus on AI's role in securing IoT environments, and scalable solutions to security. This chapter not only advances theoretical knowledge but also offers valuable insights into integrating AI with existing security frameworks. Ultimately, it serves as a roadmap for using AI in the building of defences against emerging cyber threats.

Ashwani Kumar
School of Computer Science Engineering and Technology
Bennett University, Greater Noida, India

Mohit Kumar
Department of Computer Science and Engineering
Amity University Ranchi– 834001
Jharkhand
India

Avinash Kumar Sharma
School of Engineering and Technology
Sharda University, Greater Noida
India

&

Yojna Arora
School of Engineering and Technology
Sharda University, Greater Noida
India

List of Contributors

Ajeet Kumar Sharma	Department of CSE, Sharda University, Greater Noida, India
A. Aminu	Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India
Arun Prakash Agarwal	School of Computer Science Engineering & Technology, Bennett University, Greater Noida, Uttar Pradesh, India
Arvind Kumar	Department of CSE, NSUT, Delhi 110031, India
Akshat Gautam	Department of CSE, Sharda University, Greater Noida, India
B.S. Kiruthika Devi	School of Computing, Sathyabama Institute of Science and Technology, Chennai, India
Esha Singh	Department of CSE, Sharda University, Greater Noida, India
Gaurav Kumar	Department of Computer Science and Application, School of Computer Science and Engineering, IILM University, Greater Noida, India
Gowroju Swathi	Department of Computer Science and Engineering (AI and ML), Sreyas Institute of Engineering and Technology, Nagole, Hyderabad, India
G. Jyothi	Department of Computer Science and Engineering (DS), Sreyas Institute of Engineering and Technology, Nagole, India
G. J. Lakshmi	Department of ECE, Aditya University, Surampalem, India
Jyoti Gautam	Department of CSE, NSUT, Delhi 110031, India
Kumar G. Arun	Department of Electronics & Communication Engg., JSS Academy of Technical Education, Noida, Uttar Pradesh, India
Kirti Sharma	Department of CSE, NSUT, Delhi 110031, India
Komal Shakya	Department of CSE, Sharda University, Greater Noida, India
Mahadev Ajagalla	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India
Mahesh K. Singh	Department of ECE, Aditya University, Surampalem, India
M. S. Priya	Department of ECE, Aditya University, Surampalem, India
Rosey Chauhan	Department Of Computer Science and Engineering, Sharda University, Greater Noida, India
Rajneesh Kumar Singh	Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India
Raj Shekhar	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India
Sarvesh Maurya	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India
S. Pratap Singh	Thapar Institute of Engineering and Technology, Patiala, Punjab, India
Srivash A.	Department Of Computer Science and Engineering, Sharda University, Greater Noida, India

Shikha Chadha	Department Of Computer Science and Engineering, Sharda University, Greater Noida, India
Shobha Bhatt	Department of CSE, NSUT, Delhi 110031, India
Sanjeev Kumar	Department of ECE, Aditya University, Surampalem, India
V. Satyanarayana	Department of ECE, Aditya University, Surampalem, India

CHAPTER 1

Introduction to Financial Analytics and Machine Learning

Raj Shekhar[1,*], **Sarvesh Maurya**[1] and **Mahadev Ajagalla**[1]

[1] *School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India*

Abstract: This chapter will introduce financial analytics very holistically and then dive into how machine learning transformed the finance industry. The discussion shall start with the underlying principles of financial analytics; it involves rigorous analytical expositions of financial data to deduce insights that promote decision-making, enhance performance, and avoid risks. Areas such as performance analysis, risk management, forecasting, fraud detection, and optimization will be featured within this light theme of data-driven decision-making in contemporary finance. The role of machine learning is then discussed within the chapter. The author states that the impact machine learning has on predictive analytics, algorithmic trading, fraud detection, portfolio optimization, and scoring credit has increased lately. Much more accurate and almost instantaneous decision-making with financial applications is enabled by machine learning when processing large, complex datasets. A challenge to financial data, the chapter goes on to discuss issues it poses in terms of quality, non-stationarity, imbalanced datasets, and interpretability of model outcomes. While such challenges are plentiful, there are many opportunities as well inside this landscape, from alternative sources of data to real-time analytics, automation, and even RegTech solutions. The chapter concludes by stating that it is only when the following challenges are addressed that machine learning will truly be leveraged in finance for both scalable insight and cooperative intelligence.

Keywords: Financial analytics, Machine learning, Principal component analysis.

INTRODUCTION

Financial analytics refers to the entirety of finance data analysis with the aim of creating meaningful insights into decision-making, the improvement of financial performance, and risk control. This is a systematic process that involves the examination of several financial metrics-based assessments of the financial health of an organization, such as revenue, expenditures, profit margins, and investment returns. Financial analytics leads to corporations' use of historical data in

[*] **Corresponding author Raj Shekhar:** School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India; E-mail: raj.shekhar@bennett.edu.in

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

determining and predicting business trends and future outcomes. It supports crucial areas such as budgeting, forecasting, and resource allocation by helping organizations make decisions based on data towards improving profitability and increasing efficiency. Another important role played by financial analytics [1 - 4] is its implication in risk management, which yields the identification of potential financial risks associated with the organization's actions and finding ways to minimize these risks. This analytical process equips businesses with tools and insights to adapt to the changing market conditions and to make informed investment choices that guarantee their long-term financial sustainability. Key areas in financial analytics include:

Performance Analysis

Performance analysis is a critical function of financial analytics: assessing what companies, or their portfolios and assets, have performed over time and thereby helps evaluate the efficiency of operations, profitability, and overall financial health of a company. Basic metrics applied in performance evaluation are Return on Investment, ROI, which provides the profit obtained from an investment relative to its cost and therefore allows the investor to make decisions on the efficiency of an investment relative to others and their profitability; Earnings Before Interest and Taxes, EBIT, which indicates a company's operational earnings beyond the influence of financial structure for comparisons within an industry; and profit margins, gross, operating, and net, which measure the extent of revenues retained as profits at different stages in operations. Higher margins mean effective control over costs and prices. Moreover, metrics such as Return on Equity (ROE) measure the return yielded on the shareholders' equity, thus making it a richer analysis. Collectively formed in that organizations use these metrics to analyze their financial position, make better decisions regarding investment choices, and find areas that present opportunities for improvement.

Risk Management

Financial operations risk management involves the systematic identification, quantification, and mitigation of risks that might adversely affect a firm's financial stability and performance. There exist different types of risks, which include credit risk, market risk, and operational risk, all of which require specific strategies to be in place to manage these risks effectively. Credit risk is believed to be the risk generated by the probability of defaulting of a borrower in the discharge of his duties. In relation to the handling of this risk, financial institutions consider creditworthiness and operate within appropriate lending limits. Market risk arises as a result of losses to finance resulting from changes in other market variables like interest rates, exchange rates, or stock prices and is generally addressed using hedging and diversification. It relates to risks from internal failures-which include system and human failures-and external events, which are managed through robust internal controls, audit, and contingency planning. Machine learning and advanced analytics continue to assume critical roles in risk management through their enablers, including voluminous data analysis, the identification of emerging risks in real time, and dynamic adjustments of strategies to quickly minimize losses. Through these quantitative models combined with human expertise, a firm will be able to assess how exposed they are to risk and, therefore, put in place specific controls to protect their financial interests.

Forecasting and Prediction

Forecasting and prediction [5, 6] are essential components of financial analytics that leverage historical data to anticipate future financial outcomes, enabling organizations to make informed decisions and optimize resource allocation. By analyzing past trends, financial analysts can predict stock prices, market trends, and consumer behaviours, which are crucial for strategic planning. For instance, in stock price prediction, various statistical and machine learning techniques are employed to analyze historical data and macroeconomic indicators, aiding investors in making buy, hold, or sell decisions. Additionally, forecasting plays a vital role in budgeting and cash flow management, as organizations use historical financial data to create realistic budgets and predict future cash inflows and outflows, ensuring sufficient liquidity for operations. Revenue prediction, similarly, involves analyzing sales data and market conditions to estimate future revenue streams, helping businesses set targets and identify growth opportunities. Techniques such as time series analysis, regression analysis, and machine learning models enhance the accuracy of these forecasts by identifying patterns and relationships in data. Overall, effective forecasting and prediction empower organizations to navigate financial complexities, allocate resources wisely, and position themselves for success in a dynamic market environment.

Optimization

Optimization is a crucial aspect of financial analytics that aims to identify the most efficient ways to allocate resources, maximizing returns while minimizing risks and costs. One primary application is portfolio optimization, where financial analysts utilize Modern Portfolio Theory (MPT) to select the ideal combination of assets, diversifying investments across various classes like stocks, bonds, and real estate to achieve an optimal risk-return balance. Additionally, investment balancing involves continuously monitoring and adjusting portfolios to maintain desired risk levels, ensuring that changing market conditions and asset

CHAPTER 2

Attention Inspired Human Activity Recognition Models Using Deep Learning: A Review

A. Aminu[1], **Rajneesh Kumar Singh**[1,*], **Gaurav Kumar**[2], **Arun Prakash Agarwal**[3] and **S. Pratap Singh**[4]

[1] *Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India*

[2] *Department of Computer Science and Application, School of Computer Science and Engineering, IILM University, Greater Noida, India*

[3] *School of Computer Science Engineering & Technology, Bennett University, Greater Noida, Uttar Pradesh, India*

[4] *Thapar Institute of Engineering and Technology, Patiala, Punjab, India*

Abstract: Human Activity Recognition (HAR) plays a critical role in segregating and distinguishing human actions among data generated from videos and other numerous sensing modalities, such as accelerometer, gyroscope, GPS, and magnetometer. HAR is considered a rapidly growing field that has revolutionized numerous areas, such as healthcare, manufacturing, security, smart homes, *etc*. Manual extraction of features in traditional machine learning approaches makes it difficult to handle the spatial and temporal complexities of real-world datasets, thereby necessitating the need for Deep Learning algorithms that offer automatic feature extraction to effectively capture both the spatial and temporal data. This chapter provides a review of Deep Learning models for HAR, focusing on advancements in CNN and LSTM and their variant architectures that play a significant role in handling complex and multivariate datasets gathered from wearable devices and smartphones. Furthermore, attention mechanisms, such as the self-attention and squeeze and excitation modules, have significantly enhanced model performance by focusing on relevant feature maps and recalibrating them adaptively. These mechanisms do not only improve the accuracy but also the interpretability of the model by concentrating on the important aspects of the data in consideration. This chapter also highlights hybrid models that combine CNN and LSTM and their variants for more accurate HAR, especially when working with sensor-based datasets. Additionally, it also examines that incorporation of attention mechanisms not only boosts accuracy but also optimizes the complexity of the models. Key trends in attention-driven deep learning methods are examined, indicating their growing importance in real-world human activity recognition applications.

[*] **Corresponding author Rajneesh Kumar Singh:** Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India; Tel: +91 82853 97615; E-mail: rajneesh.kumar@sharda.edu.in

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

Keywords: Artificial intelligence (AI), Deep learning (ML), Human activity, Wearable sensor.

INTRODUCTION

Many algorithms within the field of artificial intelligence have been developed to effectively categorize and classify human actions. Several Deep Learning models have been widely used to achieve better accuracy in comparison to other traditional approaches based on Machine Learning. Moreover, the attention mechanism by Deep Learning approaches significantly boosts the performance of a model [1].

Singh *et al*. [2] introduced an effective and highly regarded technique of incorporating a self-attention mechanism that effectively extracts and analyzes the sequential patterns from time series data using some stacked layers of the LSTM model. The major advantage of attention-based models is to enhance the model's accuracy and complexity by concentrating on identifying the most relevant features from the dataset under consideration. This study provides a review of deep learning models for human activity while incorporating attention mechanisms. It explores recent advances in deep learning models for human activity recognition, as well as the approaches proposed for the hybrid amalgamation of several deep and machine-learning algorithms. Moreover, it discusses published articles within the domain, focusing on their key findings. In addition to that, a summary of the deep learning models that incorporate attention mechanisms is also presented.

Human Activity

Human activity includes any motions, signs, and physical acts that necessitate using energy, such as walking, running, jogging, eating, drinking, *etc* [3]. In a broader term, human activity can be categorized into simple and complex activities. Simple human actions take posture and body movement into consideration while performing different tasks. Such activities include running, jogging, walking, *etc*, while the other category (complex) includes carrying out simpler ones in conjunction with other activities. These include subjects brushing their teeth and, at the same time, performing a simple activity like standing or sitting. By utilizing deep learning techniques on sensor data collected from different sensing modalities, various human activities, ranging from simple to complex, will be classified into sub-categories, such as ambulation-related, general hand-oriented, and hand-oriented activities related to eating, as illustrated in Fig. (**1**). Sensor-based systems can be further classified into ambient, device-bound (object-tagged), and wearable [4].

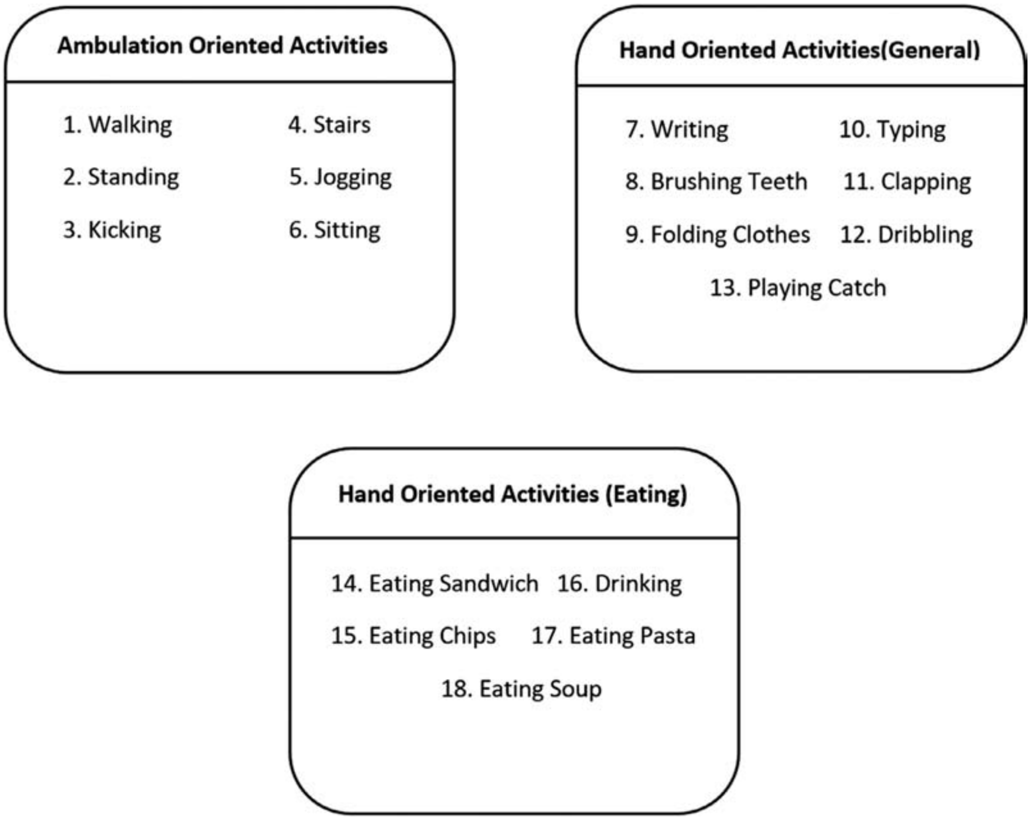

Fig. (1). Categories of human activities [3].

Generally, two approaches are broadly categorized for human activity recognition systems in terms of data gathering and accumulation, namely vision-based and sensor-based, as shown in Fig. (**2**).

Vision-based systems employ optical sensors or video surveillance cameras to detect and interpret different activities of individuals being studied. A significant challenge of these systems is the privacy of the subjects, as it may not be feasible to install cameras in every location due to ethical regulations [5]. Moreover, vision-based Human Activity Recognition (HAR) relies heavily on graphical activities, which necessitate substantial computing power. Vision-based HAR is classified into two modules: motion-based approach and video-based systems. The motion-based approach utilizes a wearable marker Motion Capture (MoCap) system, which is known for its accuracy in tracking complex human movements. However, this method has drawbacks, such as the requirement for multiple camera setups and the need for sensors to be affixed to the body. On the other hand, video-based systems utilize depth video cameras and do not require

CHAPTER 3

Classification of Acute Leukemia and Myeloid Neoplasm Using ResNet

Gowroju Swathi[1,*] and **G. Jyothi**[2]

[1] *Department of Computer Science and Engineering (AI and ML), Sreyas Institute of Engineering and Technology, Nagole, Hyderabad, India*

[2] *Department of Computer Science and Engineering (DS), Sreyas Institute of Engineering and Technology, Nagole, Hyderabad, India*

Abstract: An extensive comparison of cutting-edge image processing and machine learning methods for leukemia identification and classification is presented in this chapter. The proposed approach incorporates a thorough, extensive analytical approach that includes morphological operations, watershed segmentation, Wiener filtering, K-means clustering, and Gaussian filtration. By fine-tuning microscopic medical images, these preprocessing techniques enable accurate feature extraction and categorization. Using a multi-class Support Vector Machine (SVM) model, a total of 20 sub-features, including morphological, visual, and statistical characteristics, are retrieved and categorized. The proposed approach effectively classifies Acute Lymphoblastic Leukemia (ALL), Acute Myeloid Leukemia (AML), Chronic Lymphocytic Leukemia (CLL), Chronic Myeloid Leukemia (CML), and normal cells with a detection accuracy of 97.06% when tested on a dataset of 250 samples. To demonstrate the efficacy of the proposed approach, it is compared to state-of-the-art methods. The current method achieves 91.2% accuracy for ALL. By providing a scalable, effective, and precise method for leukemia identification and categorization, this study discusses advanced computer-aided diagnostic tools. The findings highlight how machine learning and image processing technology may enhance medical diagnostics by helping medical practitioners identify leukemia subtypes early and accurately.

Keywords: Classification, Deep learning, Leukemia, Lymphocytes, Neoplasm, Segmentation, White blood cells.

INTRODUCTION

White blood cells (WBC), known as “blasts,” which are immature and irregularly shaped, are produced abnormally during the course of leukemia, a type of malignancy. White blood cells in a blood smear are often examined under a

[*] **Corresponding author Swathi Gowroju:** Department of CSE(AI&ML), Sreyas Institute of Engineering and Technology, Nagole, Hyderabad, India; E-mail: swathigowroju@sreyas.ac.in

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

microscope to aid in diagnosis [1 - 6]. The proportion of RBC to WBC in an adult remains at 1000:1, and any figure above this mark indicates the presence ofleukemia in the patient. Hematologists use microscopic morphological and histological differences in blood smear cells to determine the kind and diagnosis of leukemia. Acute and chronic types of leukemia are the two major categories. The severe condition known as acute leukemia is characterized by a sharp rise in the proportion of abnormal cells in the patient's blood [7]. A biopsy test reveals high amounts of cells together with low concentrations of healthy white blood cells. Conversely, chronic leukemia typically progresses gradually [8]. Leukemic cells remain functional and carry out their natural tasks in the early stages, but as the disease progresses, the cells suffer substantial impairment. The patients experience symptoms such as weariness and nausea, and the primary diagnosis is made as a result of abnormal blood test findings. Inevitably, leukemia cells will outweigh healthy blood cells [9] and compromise systemic function if untreated. People with acute leukemia [10] have weariness, easy bruising, and frequent infections as symptoms.

Based on thorough scientific data, the World Health Organization (WHO) offers a categorization system for cancers. This system encompasses cancers that impact several organ systems and is a worldwide reference for clinical diagnosis, research, cancer registries, and public health monitoring. The most recent version, the fifth edition, advances the work that started more than 60 years ago by gathering all human tumors into a single relational database. This unique paradigm applies taxonomic principles along with key requirements, such as process transparency, bibliographic rigor, and bias avoidance, to classify tumors hierarchically across all organ systems and volumes (blue books).

An editorial board that oversees the creation of the 5th edition is made up of highly qualified individuals appointed for their leadership and current expertise pertinent to a particular volume, along with standing members who oversee the entire series and are participants from major medical and scientific organizations worldwide. The editorial board then chooses writers using a well-informed bibliometric method, placing a focus on trans-disciplinary knowledge and a wide geographic representation. To establish conceptual coherence and content harmonization, interdisciplinary writer/editor groups (a total of 420 participants) intentionally shared overlaps in the coverage of disease categories. Prior to 2001, numerous different and frequently disputed approaches were chosen to classify lymphomas, leukemia, and chronic myeloid diseases. Pathologists took the lead in classifying lymphoma using single skilled or neighborhood classifications, including those put forth by Rappaport, Lennert (Kiel), Lukes and Collins, and others. The Working Formulation, initially developed to standardize classification terminology, eventually evolved into its own classification system.

Hematologists have played a major role in the categorization of leukemias and myeloid diseases, with notable contributions from organizations like the Polycythemia Vera Study Group and the French-American-British (FAB) Cooperative Group. Leukemias and chronic myeloid diseases were also included in Rappaport's 1966 fascicle for the Military Institute of Pathology, which reflected early attempts to classify these ailments in a systematic manner. The criteria used to classify these tumors varied and were based on various combinations of clinical characteristics, cell morphology, cytochemical analyses and, in some cases, restricted immune phenotyping, frequently with little to no consideration of prognostic importance. Despite these drawbacks, the multiple classifications offered crucial diagnostic criteria for a range of hematologic neoplasms, enabling continued research and improvement. However, none of these categorizations represented a global consensus or included significant involvement from haematology experts.

Our goal is to develop a model to predict leukemia cells from cell images. We will approach this problem using two different methods:

Method 1: Build a basic Convolutional Neural Network (CNN) model using Keras.

Method 2: Use a pre-trained model to extract features from the images, then train traditional machine learning models on the extracted tabular features to solve the classification task.

LITERATURE SURVEY

Depending on the cell types involved, leukemia is further divided into subtypes. This additional classification indicates whether it is lymphoid or myeloid in origin. Lymphoid leukemia cells collect and result in lymph node enlargement, and immature white blood cells from the myeloid lineage proliferate out of control in Myeloid Leukemia (ML), especially Acute Myeloid Leukemia (AML). Leukemic cells can sometimes accumulate into solid masses known as myeloid sarcomas, also called chloromas. The four main types of leukemia are Acute Lymphocytic Leukemia (ALL), Persistent Lymphoid or Lymphoblastic Leukemia (PLL), Acute Myeloid Leukemia (AML), and Chronic Myeloid Leukemia (CML). The most frequent form of leukemia [14], known as ALL, accounts for about 12% of all instances of the disease, and its prevalence among children between the ages of 1 and 12 is 80%. Rapidly progressing ALL is distinguished by an abundance of embryonic leukocyte cells in the blood.

The examination of the ALL cells reveals that they contain a single nucleus and single nucleolus, as illustrated in Fig. (**1**). These cells are spherical and of uniform

CHAPTER 4

Ethical Implication of AI Decision-Making in Various Sectors.

Srivash A.[1], **Shikha Chadha**[1,*], **Rosey Chauhan**[1] and **Kumar G. Arun**[2]

[1] *Department Of Computer Science and Engineering, Sharda University, Greater Noida, India*

[2] *Department of Electronics & Communication Engg., JSS Academy of Technical Education, Noida, Uttar Pradesh, India*

Abstract: This chapter will explore the ethical implications of AI decision-making in domains from healthcare and finance to criminal justice and employment. Integrating AI technologies into daily operations has many benefits, increasing accuracy and efficiency and yielding data-driven insights. Some problems brought forth by this report include algorithmic bias that can lead to discriminatory action against minority groups. The greater concern that is surfacing today involves accountability and trust since the users and affected parties often lack a clear understanding in order to argue against the rationale of the automated decisions. Furthermore, where AI is at the crossroads of numerous human rights concerns, for instance, invasion of privacy and potential debasement of civil liberties, society faces direct challenges. AI models with comprehensive and well-curated datasets demonstrate diagnostic accuracy rates above 90%, whereas poor-quality data-derived models were incapable of performing adequately. Suggestions for developing ethical frameworks with fairness, accountability, and transparency in AI systems are included in the paper's conclusion.

Keywords: Artificial intelligence, Automated decision-making, Ethics, Sector analysis, Stakeholder engagement.

INTRODUCTION

This paper considers the ethical implications of artificial intelligence in decision-making across multi-industrial sectors like health, finance, criminal justice, and employment. As AI technologies become an integral part of everyday operations, the benefits are numerous such as improved efficiency, accuracy enhancement, and data-driven insights. But they have raised profound ethical concerns prompting further efforts to promote more responsible use. Another key issue

[*] **Corresponding author Shikha Chadha:** Department Of Computer Science and Engineering, Sharda University, Greater Noida, India; E-mail: Shikha.verma@sharda.ac.in

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

identified is algorithmic bias, which may lead to discrimination against marginalized groups. A lack of transparency over how AI makes decisions raises concerns related to accountability and trust due to the fact that most users and affected people cannot understand or counter the logic behind automated decisions [1]. Lastly, the intersection of AI with human rights, regarding problems from the erosion of civil liberties to the violation of privacy issues, places immediate pressure on society.

Through particular case studies of each type of application, this paper depicts what real-world implications might be for moral failures in the deployment of AI. Regarding the health sector, medical records and patient data create problems with confidentiality and informed consent. The whole area of predictive policing in criminal justice is problematic because it only feeds the already extant systemic biases present in society. Algorithmic biases may manifest some tendencies towards inequality and unfair hiring practices in finance in the use of AI in credit scoring and employment, respectively.

The paper concludes with actionable recommendations for creating ethical frameworks that prioritize fairness, accountability, and transparency in AI systems. Some of the strategies covered include ideas around bias mitigation techniques, stakeholder engagement, and regular audits to advance responsible AI practices. The essence of this research rests on a greater need for collaborative approaches to developing ethics into AI, wherein the potential is tapped to safeguard human rights while promoting social equity.

The integration of artificial intelligence into society makes the ethical use of such technologies important. Quite a few key ethical principles guide the development and deployment of AI systems to ensure that they benefit individuals and society and minimize harm [2].

Fairness and Non-Discrimination

AI systems need to deal with all people fairly, with no discrimination based on race, gender, ethnicity, or any other trait. Indeed, the principle ensures the use of unbiased data and algorithms for the avoidance of discriminative outcomes. The developers shall test and validate their systems for bias actively during the development lifecycle.

Transparency and Explainability

AI decision-making processes should be understandable to the users and stakeholders. Explainability is the ability to establish the justification for the decision reached by the AI. This is essential in achieving trust and accountability to open up avenues through which the decisions made by an AI could be questioned or challenged.

Accountability

The responsibility and liability of the results produced by the AI systems must be clearly defined. Organizations need to establish mechanisms to determine who is liable when an AI system does harm or reaches a wrong judgment. This includes both ethical and legal responsibility for developers, organizations and end-users [3].

Privacy and Data Protection

Huge volumes of such datasets usually contain sensitive personal data; hence, in general, ethical AI tends to emphasize protecting users' privacy and personal data. The data should be used that is gathered and stored, and in line with the laws and regulations on privacy.

Safety and Security

Therefore, safety and security should be considered while designing AI systems to minimize risks not only to the users but also to society. It goes without saying that AI systems should be resilient to adversarial attacks and function reliably under various conditions. Moreso, safety protocols should be defined to establish limits on potential harm.

Human-Centric Design

AI should complement human decision-making and extend human capabilities rather than replace them. Systems should be designed from the perspective of human values and needs, with emphasis on user interests and the interests of society at large. The process of design, as well as evaluation, should include user feedback.

Sustainability

In addition, AI development should consider environmental and social sustainability. The ecological impact of the technologies of AI is to be assessed, and deployment is to be facilitated, not contributing to societal inequalities and environment [4].

CHAPTER 5

Anticipating and Handling Cyber Threats through Predictive Capabilities of Artificial Intelligence

Kirti Sharma[1,*], **Shobha Bhatt**[1], **Jyoti Gautam**[1] and **Arvind Kumar**[1]

[1] *Department of CSE, NSUT, Delhi 110031, India*

Abstract: Anticipating cyber threats using Artificial Intelligence's (AI) predictive learning is a proactive and innovative strategy for protecting system against major attacks. By using algorithms and data analysis techniques to detect and handle possible threats, the Artificial Intelligence merger renders security. Artificial Intelligence systems can manage cyber risks by recognizing patterns and raising alerts for unidentified dangers. Known attacks can be tackled using signature-based identification, which is a reliable approach for managing them. Real-time monitoring, data collection, preprocessing, and model training techniques are the features that have been incorporated into the suggested framework. Threat prediction skills are enhanced by Machine Learning algorithms, anomaly detection, and behavioral analysis.

Furthermore, by combining threat intelligence with continuous learning, Artificial Intelligence systems are sanctioned to adapt dynamically to the futuristic and evolving landscape of cyber threats. It guarantees a robust shield for private information, proactively identifying vulnerabilities and mitigating risks while simultaneously reinforcing public confidence in the reliability and security of digital systems. These advanced capabilities enable early detection of potential threats and proactive responses to safeguard private and sensitive data effectively. The use of Artificial Intelligence in cyber security goes beyond traditional reactive measures by providing real-time insights and automated solutions that aim to mitigate both known and unknown emerging threats. This adaptive and innovative strategy provides cyber defenses, providing enhanced resilience and security for the digital space. It ensures strong protection for people and institutions to address rising threats with proactive approaches and new technological solutions.

Keywords: Artificial intelligence (AI), Quantum computing, Machine learning, Reinforcement learning.

[*] **Corresponding author Kirti Sharma:** Department of CSE, NSUT, Delhi 110031, India;
E-mail: kirti.sharma.phd24@nsut.ac.in

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

INTRODUCTION

The integration of Artificial Intelligence (AI) enhances threat anticipation and defense by leveraging advanced techniques such as machine learning algorithms and data analysis to address potential risks proactively. AI helps protect sensitive information in an environment where data is increasingly exposed to unauthorized access, anonymous exploitation, and cyberattacks. By predicting and mitigating potential threats before they materialize, AI contributes to a more secure digital landscape [1 - 6].. The act of shielding the information instead of resolving them later makes the AI merger more essential to execute. This proactive strategy aids in detecting weaknesses and creating effective countermeasures. By analyzing patterns [7], AI-driven systems can provide early warnings of possible intrusion attempts to unknown attacks. For known threats, the approach may include signature-based detection and predefined response protocols.

Mechanism Of Achieving Predictive Capabilities

Predictive capabilities are achieved through ML algorithms that analyze past data to to identify patterns, analyze normal user actions, integrate external threat intelligence for updated insights, and use anomaly detection techniques to uncover unusual activities. The following are some mechanisms to achieve predictive capabilities:

Machine Learning Algorithms

The core of the predictive capabilities lies in the ML algorithms employed. These algorithms investigate trends in historical data associated with both benign and malicious activities. As the model processes more data, it improves its accuracy in recognizing potential threats.

Anomaly Detection Techniques

Techniques like outlier detection and statistical analysis help in recognizing odd trends that diverge from normal behavior, indicating possible intrusion attempts or breaches.

Behavioral Analysis

Analyzing user and entity behavior provides insights into typical activities. The AI system can recognize deviations from these established behaviors, enabling the early detection of potential threats.

Threat Intelligence

Incorporating external threat intelligence feeds enhances the AI system's ability to predict threats by incorporating information about known vulnerabilities, attack vectors, and threat actor behaviors.

Continuous Monitoring

A continuous monitoring approach ensures that the AI system remains vigilant, providing real-time analysis and updates as new data is collected.

Workflow for Anticipating Cyber Threats Using AI

To anticipate the cyber threats using AI, the proposed approach is hypothesized. Fig. (**1**) gives a systematic workflow of the proposed technique. The workflow starts with collecting data, preprocessing data, then selecting of model, detecting anomalies and concluding with the prediction of threats.

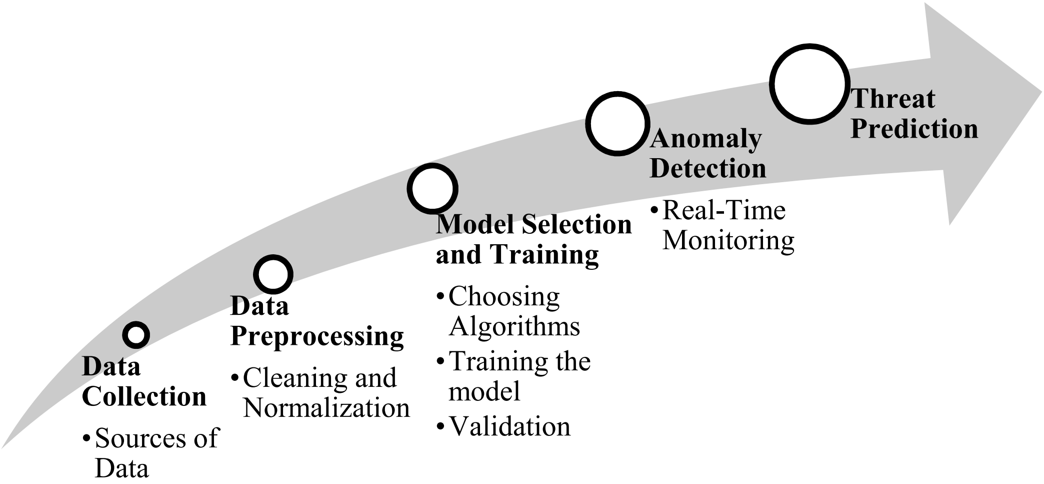

Fig. (1). Workflow for anticipating cyber threats using AI.

Data Collection

Sources of Data

i. Collect information from a range of sources, such as past incident reports, network logs, endpoint data, and analytics on user activity.
ii. Use data to gain comprehensive insights.

CHAPTER 6

Secure Interaction-based Identification System: A Technique for Smart Home Authentication

Mahesh K. Singh[1,*], **G. J. Lakshmi**[1], **V. Satyanarayana**[1] and **Sanjeev Kumar**[1]

[1] *Department of ECE, Aditya University, Surampalem, India*

Abstract: Applications that make use of the Internet of Things (IoT), such as the smart home (S-home), are growing in popularity as more and more smart gadgets are becoming available and affordable. However, existing authentication solutions may not be adequate for protecting IoT settings due to the peculiarities of these contexts, such as the utilization of devices with limited resources. This has led to the development of a variety of different authentication techniques that are specifically designed for the environment of the Internet of Things. An exhaustive overview of the current authentication techniques is given in this work. This chapter presents noteworthy contributions, which are outlined as follows: It begins by introducing a general model that was created using an S-Home use-case scenario. In order to identify potential entry points for an attack, it then conducts a threat assessment using the model as a basis. The study can be considered successful if it defines a workable set of security requirements for creating S-home authentication solutions. Third, based on the needs, a comparison of the current authentication methods is conducted, and recommendations are provided for achieving effective and efficient authentication in IoT settings. IoT computing provides additional benefits to users through the use of internet-connected smart appliances, objects, and gadgets. It is vital to process the data generated by intelligent IoT devices securely.

Keywords: Authentication, IoT, Internet of things, S-home, Security.

INTRODUCTİON

The IoT is a network of physical objects, also known as “things,” that are embedded with electronics, software, and other technologies that enable them to communicate and exchange data with one another and with other connected devices and systems over a network, such as the Internet [1]. In recent years, the Internet of Things has emerged as one of the most significant technological advancements. Due to its increasing popularity, it has become increasingly prominent in ordinary, day-to-day activities and applications [2]. It is now feasible

[*] **Corresponding author Mahesh K. Singh:** Department of ECE, Aditya University, Surampalem, India; E-mail: mahesh.092002.ece@gmail.com

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

for everyone, at any time, from any location, to have connectivity for anything, and it is projected that these connections will expand and form a totally advanced and dynamic IoT network. The technology of the Internet of Things can also be utilized to construct a new concept and a vast developmental space for smart homes, with the objectives of boosting both intelligence and comfort, as well as the overall quality of life [3].

The IoT is currently viewed as a mature technology within the consumer electronics sector, and the "smart home" has been praised as one of the market segments with the greatest potential for IoT deployment [4]. The purpose of the smart home, also known as S-Home, is to improve the quality of life of the occupants by automating a number of household tasks. These responsibilities include energy management, security surveillance, and health care services [5]. Smartphones are more than just phones in today's world; they contain a vast array of programs that may be utilized for a variety of reasons, including education, health care, and entertainment [6]. The ever-increasing popularity of mobile devices and the extension of their capabilities have led to increased demand for increasingly complex and widespread mobile applications in people's daily lives. The underlying premise is to connect internet-enabled devices to everyday objects [7]. This allows objects to continue transmitting data to the web and makes them globally accessible [8].

Due to the fact that everyone has access to a smartphone in the modern world, regardless of where they live (rural areas, cities, *etc*.) [9], we intend to construct Smart Home Technology using smartphones so that it can provide us with convenience and comfort, satisfy our needs, and enhance the overall quality of our life. A "Smart Home" is a private residence with internet-connected equipment and systems like lighting and heating. "Smart homes" use "home automation" or *demotics* (from the Latin word for home, "*Domus*"), which enables homeowners to control smart gadgets in their houses, thereby enhancing their safety, comfort, convenience, and energy efficiency [10]. This is often performed by installing a smart home application on the homeowner's smartphone or another networked device. Authentication refers to the process of validating the identification of a person, software process, or device [11].

A smart home is comprised of a wide variety of elements, such as equipment connected to the Internet of Things (IoT), software for automation, people, voice assistants, and companion applications. These entities interact with one another in the same physical environment, which may result in outcomes that are undesirable or even dangerous. These kinds of outcomes are referred to as interaction hazards associated with the Internet of Things. The scope of work conducted on interaction hazards is limited to the consideration of automation applications.

Other control channels for the Internet of Things, such as voice commands, companion apps, and physical actions, have been disregarded. An expanding number of IoT platforms are being utilised by smart homes, which is becoming an increasingly prevalent practice. It is possible for these platforms to issue directives that are in direct opposition to one another because each has a limited view of the status of the gadgets that are utilised within the home.

There has been significantly less study conducted on the handling of interaction hazards compared to the detection of interaction hazards. In prior studies, generic handling policies were utilised; however, it is highly unlikely that these policies will meet the requirements of all houses. IoTMediator is a solution that provides precise risk recognition and threat-tailored treatment in houses that are equipped with many control channels and a large number of platforms. It has been proved that IoTMediator performs far better than earlier work that has been considered to be state-of-the-art. This was demonstrated by our evaluation of two residences that are situated in the real world [12, 13].

The latest versions of smart home technologies provide unprecedented levels of usability and productivity improvements. The following are examples of smart home technologies:

- If a home system monitor senses an electrical surge, it will shut off the home's appliances. If the water supply monitor detects a malfunction, it will shut off the water to avoid the basement from flooding.
- Kitchen appliances, such as smart refrigerators, can monitor when food should be discarded and provide reminders. Smart locks and garage door openers provide users with greater control by allowing them to regulate when visitors are admitted. In the future, smart locks may one day be able to sense when people are near and unlock the door as soon as the person gets close enough [14].
- Smart thermostats, such as the one developed by Nest Labs, Inc. thermostats, are the only ones on the market with built-in Wi-Fi, allowing users to remotely configure, monitor, and control the temperature in their homes [15].
- Connected timers can be used to water both indoor and outdoor plants, including lawns and gardens. Additionally, with the assistance of connected feeders and other gadgets, pet care can be simplified [16].

RELATED WORK

A study conducted in 2000 proposed a method for the real-time detection and recognition of a person's face. This method can be used in place of the manual technique, which is time-consuming, difficult to maintain, and prone to manual errors [17]. A 2012 article examined a number of security vulnerabilities with the

CHAPTER 7

Channel Response Measurements and Analysis of the Human Body for Biometric Resolutions

Mahesh K. Singh[1,*], **B.S. Kiruthika Devi**[2], **M. S. Priya**[1], **V. Satyanarayana**[1] and **Sanjeev Kumar**[1]

[1] *Department of ECE, Aditya University, Surampalem, India*

[2] *School of Computing, Sathyabama Institute of Science and Technology, Chennai, India*

Abstract: The infrastructure and technologies of computer security have undergone several improvements and modifications. There is a growing trend toward building an identity based on a combination of three factors: what you know, what you have, and who you are in the present (biometrics). Knowledge-based and token-based authentication systems have been deemed inadequate; however, new technology from the East has overcome these issues (biometrics). There is a chance that you will lose access to your resources if you forget your password. Biometrics is the science of identifying a person without disclosing private information. Biometrics is an authentication mechanism that uses a person's unique biological characteristics. This article examines the history and evolution of the many biometric identification modalities and the distinguishing characteristics that each of them possesses. The ability to recognize faces is one of the most fundamental ways in which humans have linked as individuals. Facial recognition is a sort of visual processing that works with human data. As there were no mirrors available to ancient humans, facial descriptions were typically established through the gaze of another person or, at best, through the description of the person's reflection in clear water. This was the normal practice for an extended period of time.

Keywords: Biometrics, Channel response, Distinctiveness, Minutiae features, Verification.

INTRODUCTION

Today, digital systems control every facet of human life, allowing more individuals to get the services they need through a variety of channels. Personal identification of smart devices based on biometric recognition, which uses an individual's unique biological characteristics to verify their identity, has become a viable option in recent years [1, 2]. When opposed to more archaic approaches

[*] **Corresponding author Mahesh K. Singh:** Department of ECE, Aditya University, Surampalem, India; E-mail: mahesh.092002.ece@gmail.com

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

like password-based user identification processes or ID cards, which are prone to forgery and loss, biometric systems have clear advantages in terms of usability, portability, and accuracy. Damage to or disclosure of inherent biometric information renders recovery impossible and may even lead to misidentification. The use of many biometrics at once, or in addition to other security measures like an electronic signature or a personal identification number, can result in a much higher level of safety [3, 4].

This process can be used to verify the user's identity on a portable device by physically touching it, an action that is easy and intuitive for users of all ages. One can use this method to verify the authenticity of their own devices [5]. Direct connections utilizing the user's keys to establish Bluetooth or Wi-Fi networks between IoT devices can also execute the authentication operation in parallel with the pairing process. The pairing procedure is quite similar to setting up a Bluetooth or Wi-Fi network, making it an achievable target [6, 7].

Our initial step was to create an experimental setup in which we could measure BCR reliably without altering any underlying biometric traits, and for this, we relied on the theory behind capacitive coupling-based electrical signal transmission in the body. The electric signals released by the GE (Ground Electrode) of the receiver that produce oscillations in the electric field formed between the GE and the SE (Signal Electrode) of the transmitter can be used to analyze the body channel's parameters. [8, 9]. In contrast to biometric authentication, which differentiates itself by focusing on the live person, forensics does not require the identification of a person in real time shown in Fig. (**1**).

The term “distinctiveness” describes how significantly an individual's biometric pattern deviates from the norm of the community as a whole. The clarity of the labelling improves as the degree of difference increases. Having a one-of-a-kind personality is a key component in reaching the pinnacle of uniqueness. If a biometric pattern has a low degree of uniqueness, it is likely to be shared by most people [10, 11]. The following is a case in point: The differences between the iris and retinal geometry are greater than those between the hand and finger geometry. The implementation helps determine the appropriate level of uniqueness and resilience [12, 13].

RELATED WORK

Thanks to his development of the Bertillon body measurement system, Alphonse Bertillon is often credited as the man who initiated the field of modern biometrics [14]. A biometric identity system was first mentioned in the 1800s in Paris, France, despite references to biometrics going back to the Babylonian Empire in the 500s B.C. This biometrics report is more recent than accounts that came before it in 500 B.C. [15]. In order to better categorize and evaluate criminals, Alphonse Bertillon developed a method that relied on precise body measurements [16]. Average classification accuracy was roughly 95.8%, with no obviously biased topic misidentifications using the kernel-based support vector machine. Receiver operating characteristic curve analysis further demonstrates that the suggested classifiers are robust against decision limits over a wide range of threshold settings [17]. Beginning in 1991, groundbreaking research into face detection opened the door to the possibility of real-time facial recognition. Turk and Pentland found that residual error might be utilized for face recognition while working with eigenface approaches. This development paved the way for the creation of robust, in-process automatic facial recognition [18].

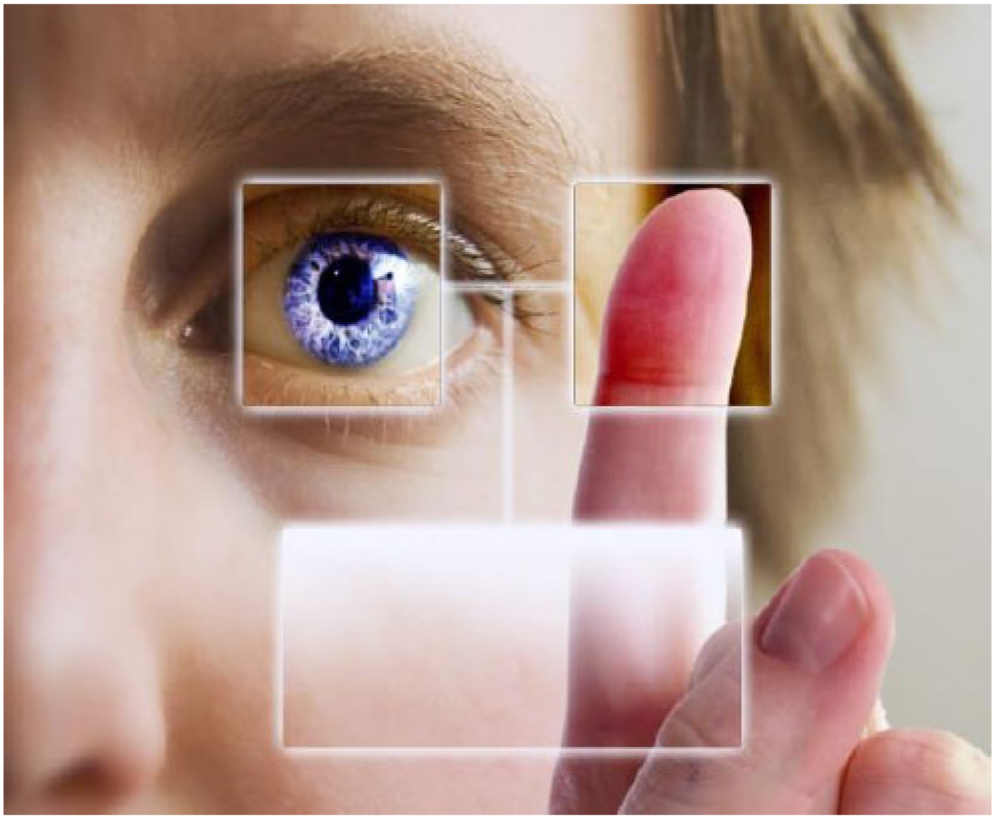

Fig. (1). Biometric resolutions of the human body [1].

In 1992, the United States government officially launched the Biometric Consortium. The first conference of the Biometric Consortium took place in October 1992, with the help of the National Security Agency [19]. The Consortium received its charter in 1995 from the Security Policy Board, which

CHAPTER 8

Applicability of AI in Cyber Security

Akshat Gautam[1,*], **Esha Singh**[1], **Komal Shakya**[1] and **Ajeet Kumar Sharma**[1]

[1] *Department of CSE, Sharda University, Greater Noida, India*

Abstract: Connectivity, data proliferation, and technology have gained great advantages in this age of digitization. However, these advantages bring significant cybersecurity challenges. Especially with the advancement of malware, phishing attacks, and ransomware, advances like these are making it challenging to stay ahead in traditional security practices.

The advanced complexity in cyber security arises from these developments, like cloud computing, the Internet of Things, and mobile technologies. Organizations now have to shield not only their traditional networks but also environments based on the cloud, endpoints, and third-party integrations. The more interconnected devices and systems grow, the harder they are to secure from Distributed Denial of Service attacks and data breaches, for instance. An important challenge would be the time it takes to detect and respond to cyber incidents. Traditional security systems rely on static rules or signature-based methods, which make them ineffective at changing attack tactics. Artificial Intelligence has emerged as one of the significant transformative elements within the realm of cybersecurity, offering improved methodologies for the detection, prevention, and alleviation of cyber threats. With the complexity and intricacy of cyberattacks on the rise, AI-driven systems offer a much more advanced system than conventional security approaches. Further, artificial intelligence can predict potential weaknesses and automate redundant security functions so that cybersecurity experts can focus on strategic matters. This chapter analyses the increasing role of artificial intelligence in the cyber defense strategy and its potential use in different sectors of security.

Keywords: Artificial intelligence, Cyber security, Cyber attack, Network security.

INTRODUCTION

Artificial Intelligence is changing the modern cyber security landscape to a great extent, as it improves threat detection and mitigation through increased efficiency in an accurate manner and speed. Cyber security systems become more responsive

[*] **Corresponding author Akshat Gautam:** Department of CSE, Sharda University, Greater Noida, India;
E-mail: ronitakki3@gmail.com

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

and proactive against threats by leveraging machine learning, deep learning, and other AI techniques. The core work of AI includes automation of threat detection based on pattern and behavior learning of anomalies. Machine learning models can be trained on vast datasets so that they can spot suspicious activities and even deviations from the usual behavior [1]. Thus, a threat can be noticed and addressed much sooner than in the case of rule-based systems since the latter often do not possess such subtlety. AI also allows scalability for threat analysis due to the tremendous amount of data that would be involved with potential threats. This, in turn, reduces the burden on security teams, allowing them to focus on more complex issues and even predict potential cybersecurity threats before they emerge. This basis is laid on predictive analytics models that analyze historical data, laying out patterns that will lead to a security incident. Such models would outline vulnerabilities, predict the probability of an attack on a particular input, and provide methods for preventive measures. To enable real-time autonomous responses, AI must be properly utilized to detect the nature of threats and take appropriate actions, such as isolating infected systems, blocking malicious traffic, and applying patches to vulnerable areas. This autonomous response can significantly reduce the damage caused by malware attacks, especially when human intervention is delayed or insufficient.

Artificial intelligence is increasingly being used to help cyber defense systems adapt and evolve based on new information. It is challenging for traditional security tools to compete with the rapid evolution of threats in the cyber world, while AI systems are continually learning from new data and updating their models based on the new information; hence, these are very effective against APT. Cybercrime today uses automation, AI, and machine learning for optimal effectiveness and distribution of attacks [1]. Human factors are among the biggest challenges in cyber security as social engineering attacks exploit vulnerability by humans rather than technology. One of the reasons that most of these attacks is because of poor security practices, such as weak passwords and access controls and failure to update software.

The global nature of cyber threats indeed creates a challenge in terms of legal and regulatory frameworks, different from one country to another, respective to cyber security regulation. Moreover, the anonymity of the internet actually opens the opportunity for attackers to work from jurisdictions beyond law enforcement's reach. Indeed, achieving a good balance between robust security and budgetary constraints is a significant challenge, especially for SMEs.

The Role of AI in Addressing Cyber Threats

The current digital world needs real-time threats detection and ensures the safety and integrity of the systems. Because the nature and intensity of attacks are much more than conventional security solutions can capture, the detection and response to threats remain much delayed. Artificial Intelligence has indeed emerged as the game-changer that enables threat detection in real-time with a speed and accuracy one has never seen before.

This way, AI systems can scan humongous volumes of network traffic, user activity, and system behavior in real time because of the machine learning algorithms that identify anomalies when they occur. Due to comparisons in patterns of normal behavior, AI can rapidly spot anomalies that may be symptomatic of a cyberattack or unique login attempts, transfers of data, and application activities that sometimes surpass normal levels. Given such information, organizations can easily identify and neutralize potential threats before such threats become significant security breaches.

This is possible only if AI processes huge volumes of data, which might identify the subtle signs of an attack. Modern attacks are in the nature of APTs or zero-day exploits and are so designed to evade traditional security measures and go unnoticed for long periods. AI-based systems can track such subtle and hidden threats because such systems feed on new data continuously, adjusting models accordingly. Fig. (**1**) shows the flow chart attackers perform the attack.

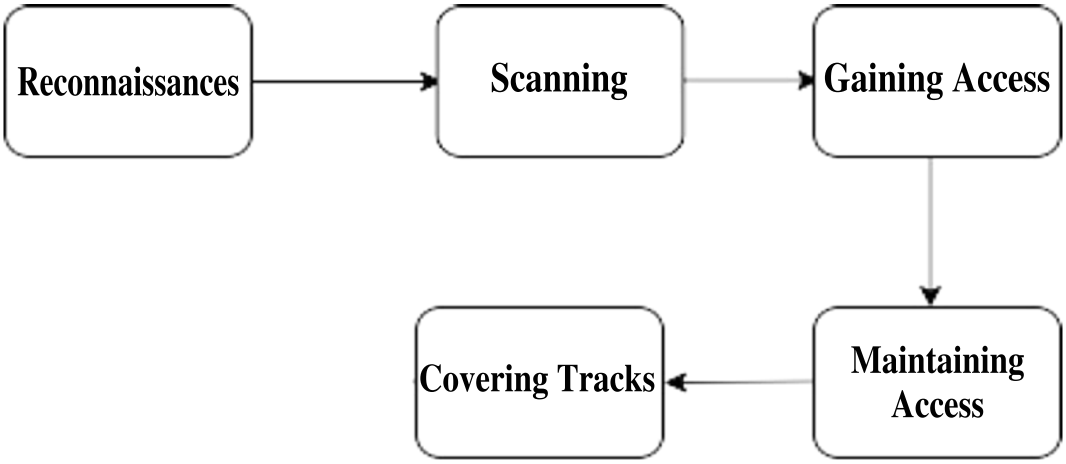

Fig. (1). Phases of attack.

For the systems to detect suspicious activities, they would start the response mechanisms automatically. This includes some network isolation, blocking some

SUBJECT INDEX

Ashwani Kumar, Mohit Kumar, Avinash Kumar Sharma & Yojna Arora (Eds.)

Ashwani Kumar

Dr. Ashwani Kumar is an Associate Professor at the School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India. He completed his Ph.D. in Computer Science and Engineering from Jaypee University of Information Technology, Himachal Pradesh, in 2017, following his M.Tech in 2011 and B.Tech in 2009. With over 13 years of teaching and research experience, he has published more than 50 research papers in journals indexed in SCI, SCOPUS, and Web of Science. His work appears in reputed publishers such as Wiley, Springer, Elsevier, and IEEE. Dr. Kumar serves as a reviewer for several international journals and is on editorial boards of multiple SCOPUS/WoS-indexed journals. He was honored with the Bentham Brand Ambassador Award in 2019–2020 and has chaired sessions at international conferences. His research interests include image security, multimedia applications, watermarking, cryptography, and network security. He is also a lifetime member of professional bodies like IEEE, ISTE, IACSIT, and IAENG.

Mohit Kumar

Dr. Mohit Kumar is an Associate Professor in the Department of Computer Science and Engineering at Amity University, Jharkhand. He holds a Ph.D. in Computer Science and Engineering from Jaipur National University and has over 13 years of experience in academia and research. He has authored and co-authored papers in reputed journals such as IEEE Transactions on Industrial Informatics, IEEE Transactions on Network Science and Engineering, Scientific Reports (Nature), MDPI Sensors, Symmetry, and HCIS Springer, with a cumulative impact factor exceeding 50. Dr. Kumar has served as a reviewer for high-impact journals and has participated in various international conferences as a session chair and technical program committee (TPC) member. He has been granted three patents and has authored one book, with another under development for Springer. His key research areas include wireless sensor networks, IoT, data science, machine learning, and deep learning. He has also consulted on government-funded research projects.

Avinash Kumar Sharma

Dr. Avinash Kumar Sharma is an Associate Professor in the Department of Computer Science & Engineering at Sharda University, Greater Noida, India. He holds a B.Tech from UPTU, an M.Tech from UTU Dehradun, and a Ph.D. in Computer Science from Veer Madho Singh Bhandari Uttarakhand Technical University. His research focused on cloud computing, particularly infrastructure optimization. With more than 18 years of experience in teaching, research, and academic administration, Dr. Sharma has published over 60 research articles and holds seven Indian patents, including two design patents. He has edited books with IGI Global and Wiley and authored a book with BPB Publications. He has mentored winners in national innovation competitions such as the Smart India Hackathon and has served in leadership roles such as NBA Coordinator, Program Coordinator, and R&D collaboration lead. His research interests include cloud computing, artificial intelligence, smart agriculture, and image processing.

Yojna Arora

Dr. Yojna Arora is an Associate Professor in the Department of Computer Science and Engineering at Sharda University, Greater Noida, India. She earned her B.Tech in Information Technology from Kurukshetra University, M.Tech in Computer Science from Amity University, and a Ph.D. in Computer Science with a specialization in Big Data Analytics. With over 12 years of academic and research experience, she has authored over 50 research papers, presented 25 conference papers, published 2 books, 10 book chapters, and 5 magazine articles. She holds 2 granted patents and 1 published patent in emerging domains like AI and data science. Her research interests include big data analytics, data mining, cloud computing, and network security. She has mentored Ph.D. scholars, postgraduate dissertations, and undergraduate projects. Dr. Arora is affiliated with professional bodies such as IET, IAENG, the Internet Society, and CSI. She also contributes as a reviewer and editorial board member for several international journals.