MACHINE LEARNING AND BLOCKCHAIN

CHALLENGES, FUTURE TRENDS AND SUSTAINABLE TECHNOLOGIES

Editors:
Keshav Kaushik
Rewa Sharma
Ayodeji Olalekan Salau

Bentham Books

Machine Learning and Blockchain – Challenges, Future Trends and Sustainable Technologies

Edited by

Keshav Kaushik
Center for Cyber Security and Cryptology
Sharda School of Computer Science & Engineering
Sharda University, Greater Noida
India

Rewa Sharma
J.C Bose University of Science and Technology
YMCA, Faridabad, India

&

Ayodeji Olalekan Salau
Department of Electrical and Electronics
and Computer Engineering, Afe Babalola University
Ado Ekiti, Nigeria

Machine Learning and Blockchain – Challenges, Future Trends and Sustainable Technologies

Editors: Keshav Kaushik, Rewa Sharma and Ayodeji Olalekan Salau

ISBN (Online): 978-981-5324-21-1

ISBN (Print): 978-981-5324-22-8

ISBN (Paperback): 978-981-5324-23-5

First published in 2026.

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

PREFACE

Machine Learning and Blockchain-Challenges, Future Trends and Sustainable Technologies (MLB) by Bentham Science is a brainchild of Keshav Kaushik, Rewa Sharma, and Ayodeji Olalekan Salau. The goal of this book is to make it easier for academics and prospective readers to grasp blockchain technology and machine learning. They will be able to practice and gain expertise with ML techniques thanks to this book. The book will provide readers with a thorough grasp of the cutting-edge technologies around blockchain, artificial intelligence, and machine learning. These technologies have the ability to collect and process enormous amounts of data from the real world. The edited book will be set up with distinct chapters to provide readers with maximum readability, flexibility, and adaptability. We are very grateful to all of our co-authors for sharing their expertise and experience; they are all authorities in their fields. This book is an attempt to gather their thoughts and share them with the world in the format of chapters. This book offers insights into AI, FinTech, Deep Learning, Blockchain, Machine Learning, and Blockchain applications. Academicians, industry professionals, researchers, undergrads, and grads will all find the book useful. We acknowledge Bentham Science Publishers and all of the authors of this book for their cooperative efforts.

Keshav Kaushik
Center for Cyber Security and Cryptology
Sharda School of Computer Science & Engineering
Sharda University, Greater Noida
India

Rewa Sharma
J.C Bose University of Science and Technology
YMCA, Faridabad, India

&

Ayodeji Olalekan Salau
Department of Electrical and Electronics
and Computer Engineering, Afe Babalola University
Ado Ekiti, Nigeria

List of Contributors

Ambika R. Thakur	Department of Computer Science and Engineering, The NorthCap University, Gurugram, India
Abhijeet Kaiwade	Institute of Management and Research., Abhinav Education Society's Institute of Management and Research, Pune, India
Anupama Chadha	Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, India
Belsam Jeba Ananth M.	Department of Mechatronics Engineering, SRM Institute of Science and Technology, Kattankulathur, India
Binod Kumar	Department of Computer Applications, JSPM's Rajarshi Shahu College of Engineering, Pune, India
Balraj Kumar	School of Computer Application, Lovely Professional University, Phagwara, Punjab, India
Chetna Tiwari	Department of Computer Science and Engineering, The NorthCap University, Gurugram, India
Chetan Shelke	Alliance College of Engineering and Design, Alliance University, Bangalore, India
Dharamvir	Department of Computer Application, The Oxford College of Engineering, Bengaluru, India
Dheerdhwaj Barak	Department of Computer Science & Engineering, Vaish College of Engineering, Rohtak, India
G. Madhumita	Department of Management Studies, Vels Institute of Science Technology and Advanced Studies (VISTAS), Chennai, India
Garima Sharma	Department of Computer Science and Engineering, The NorthCap University, Gurugram, India
Gunjan Chhabra	Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India
Gaurav Kumar	School of Computer Application, Lovely Professional University, Phagwara, Punjab, India
Harish Kumar	Department of Computer Science, King Khalid University, Abha, Saudi Arabia
J. Jayaganesh	Department of Computer Science, Government Arts and Science College Perumbakkam, Chennai, India
K. Santhanalakshmi	Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, India
Kamreed Udham Singh	School of Computing, Graphic Era Hill University, Dehradun, India

CHAPTER 1

Blockchain: A Sustainable Technology

Renu Singh[1,*], **Ashlesha Gupta**[1] and **Poonam Mittal**[1]

[1] *Faculty of Informatics and Computing, J.C. Bose University of Science and Technology, YMCA, Faridabad, India*

Abstract: In recent years, blockchain has become one of the most booming technologies. It has completely revolutionized industries and academia by creating a transparent system of trading money. The blockchain industry has started to get significant investments from corporations and tech mega-corporations. In the upcoming years, its net worth is expected to increase more than three times. Blockchain Technology has grown in popularity because of its trust, transparency, and data security. As a result, everyone, either from academics or industry, wants to learn the Blockchain. This chapter provides a detailed overview of Blockchain Technology, which will help researchers and scholars quickly understand Blockchain. Firstly, we introduce blockchain along with its history and a thorough understanding of different types of networks. Then, the definition of Blockchain, fundamentals, categories of Blockchain structure, characteristics, architecture, workflow, components, version, Blockchain protocols, and finally, applications of Blockchain are discussed.

Keywords: Blockchain technology, Consensus, Cryptography, Distributed, Decentralized applications.

INTRODUCTION TO BLOCKCHAIN

Blockchain Technology (BT) can transform ongoing business methods. Blockchain Technology has now become very popular in both academics and industries. All the technologists, researchers, and research scholars are just picking up the books on blockchain and beginning to study them to master the concepts of Blockchain. Also, people from different backgrounds are very much interested in becoming professionals in blockchain application development. Until one picks up a good source, it becomes extremely difficult to clear the basic concepts of Blockchain Technology. So, to aid one in comprehensively gaining the concepts of Blockchain, we have written this chapter on Blockchain, a Sustainable Technology. This chapter is intended for all levels of software

[*] **Corresponding author Renu Singh:** Faculty of Informatics and Computing, J.C. Bose University of Science and Technology, YMCA, Faridabad, India; E-mail: renus2344@gmail.com

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

engineers, developers, researchers, scholars, and anyone from academia and industry who wants to learn Blockchain Technology in detail.

This chapter includes a very detailed discussion of Blockchain, including the history of Blockchain, Blockchain and its fundamentals, categories, characteristics, architecture, workflow of Blockchain process, components, version, blockchain protocols, and applications. Lastly, we end our chapter with the conclusion.

History of Blockchain

The Distributed ledger concept was introduced in 1976 [1]. After the evolution of cryptography, "Scott Stornetta" and "Stuart Haber" presented a paper titled [2], which provides the concept for time stamping the data in place of the medium. Another idea that plays a major role in Blockchain is "Electronic cash" or "Digital Currency," which was presented by David Chaum. He has also made a major contribution to e-cash schemes and double-spending detection.

Adam Back, in 1997, presented a concept known as "hashcash", which provides a means to control spam emails. Then Wei Dai created money known as "b-money", a peer-to-peer network.

Blockchain originated from Satoshi Nakamoto [3] and was created using Bitcoin paper [3]. This paper focuses mainly on electronic payment systems using cryptography. In this paper, Nakamoto presented a technique that prevents double-spending. The idea of a public ledger was introduced in this paper to track and confirm the transaction history of digital coins.

After some months, an open-source program for implementing Bitcoin was released. Beginning in 2009, Satoshi Nakamoto introduced the first bitcoin. The inventors of Bitcoin are unanimous, but Bitcoin still has a very large community that supports and addresses the different issues of the code.

While there are various cryptocurrencies like Dogecoin, Litecoin, *etc*, Bitcoin holds a maximum market share. The main feature of Bitcoin that attracts users is its capacity to maintain the anonymity of users and transparency. Afterward, the use of Bitcoin grew, and in 2013, investors started to invest heavily in contract-starting. Ethereum has become popular as it provides safety, speed, and a more efficient environment [4]. To understand the major contributions of Blockchain, a summary of its history is shown in Fig. (**1**).

Blockchain is a distributed form of the network. The other two ways in which nodes in the network can be arranged are centralized and distributed, as shown in

Fig. (**2**). To understand the difference between these three network types and distinguish why the distributed form of network is preferred for blockchain, here, we provide a detailed discussion of them.

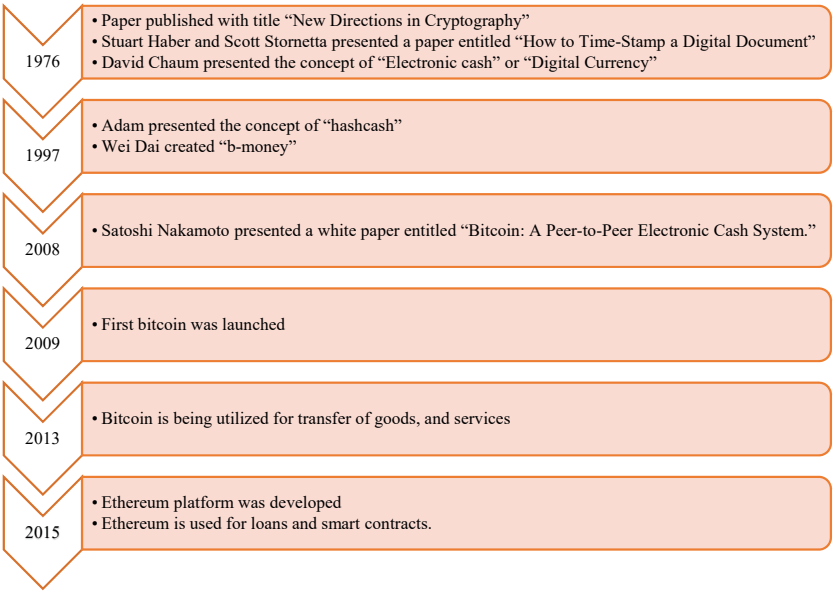

Fig. (1). History of blockchain.

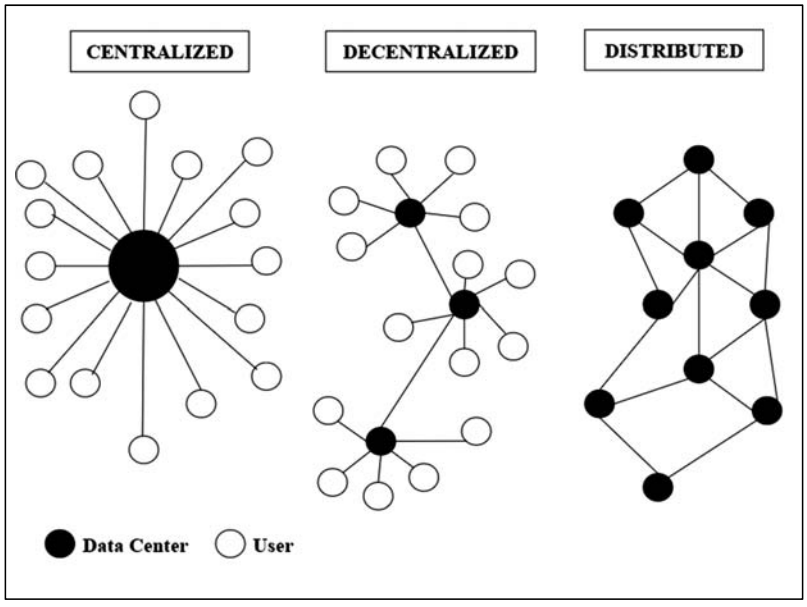

Fig. (2). Types of network.

CHAPTER 2

Mapping of Blockchain Technology with the Indian Fintech Sector for Securing Financial Operations

Khushwant Singh[1,*], Mohit Yadav[2], Yudhvir Singh[1] and **Dheerdhwaj Barak[3]**

[1] *Department of Computer Science & Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, India*

[2] *Department of Mathematics, University Institute of Sciences, Chandigarh University, Mohali, India*

[3] *Department of Computer Science & Engineering, Vaish College of Engineering, Rohtak, India*

Abstract: The term "Fintech" (Financial Technology) refers to software and other spearheading technologies adopted by different organizations to automate and enhance financial services. It refers to the technology that improves the backend system at traditional financial institutions. In FY22, $8.53 billion was invested in India's Fintech industry. It has been anticipated that the FinTech industry will generate around $200 billion in revenue by the year 2030 and overall throughput will be $1 trillion. Fintech is expanding quickly, yet there are several problems in the current fintech market including interacting with legacy systems like banks, data and payment security, compliance, lack of end-user awareness, retaining users, and user experience. Due to the development of fintech, more data is now accessible in digital formats, which facilitates analysis and the generation of insights but also increases the risk of security breaches. Blockchain is disruptive technology using which one can securely move money from one account to another without using a bank or any financial organization The term "distributed ledger technology" is often used interchangeably with "blockchain technology" in the financial services corporation. Each transaction has a trustworthy record, thus there is no chance of changing to earlier ones. In essence, blockchain technology can completely ensure the accuracy of every transaction. In this study, the problems facing India's fintech industry are described in detail, and possible solutions employing blockchain distributed ledger technology are suggested. Additionally, it finds blockchain technology has the ability to enhance the security and competence of financial operations in the Indian fintech sector, there are challenges such as regulatory uncertainty and scalability that require to be addressed. The paper concludes with recommendations for the upcoming development and adoption of blockchain technology in the Indian fintech sector.

* **Corresponding author Khushwant Singh:** Department of Computer Science & Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, India; E-mail: erkhushwantsingh@gmail.com

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

Keywords: Blockchain, Cryptocurrency, DeFi, FinTech India, FinTech, Security.

INTRODUCTION

Fintech is a word used to explain companies that incorporate technology to boost or automate financial services and processes [1]. The combination of "financial" and "technology" forms the term and refers to a rapidly growing sector that caters to the needs of both businesses and consumers [2, 3]. Fintech includes a broad variety of uses, like mobile banking, cryptocurrency, insurance, and investment apps [4, 5]. It encompasses a variety of financial transactions that are often done without human intervention, such as money transfers, smartphone check deposits, credit applications, raising capital for startups, and investment management [6 - 8]. According to a report titled "The winds of change: Trends shaping India's Fintech Sector," released in September 2022, the global financial services sector has been greatly impacted by fintech in the past decade [9 - 11]. However, in the first half of 2022, fintech investment growth slowed down due to increased regulation, shifting customer preferences, uncertain global events, and ongoing geopolitical unrest [10 - 12]. In spite of the obstacles, the global fintech industry experienced significant growth in 2021, although the pandemic caused some disruptions [13 - 15]. Supernova cryptocurrencies such as Bitcoin and Ethereum have clinched prominence and brought blockchain technology into the spotlight [16 - 18]. The extensive implementation of blockchain has caught the attention of the finance and corresponding industry, resulting in the development of new cryptocurrencies such as ZCash, NameCoin, PrimeCoin, and LightCoin) [19 - 21]. This has consequences for the appearance of a novel way of financing innovative ventures and products, known as Initial Coin Offerings (ICO) [22 - 25]. In current times, there has been rising attention to the utilization of blockchain beyond cryptocurrencies, driven by the distinctive characteristics of distributed ledger technologies (DLT) such as cryptographic security, immutability, decentralization, and transparency [26 - 29]. These features present exciting possibilities for a variety of industries. The fintech industry, including major financial organizations, insurance companies, and exchange corporations, has recently turned its focus toward blockchain technology [30 - 32]. The term "distributed ledger technology" is often used instead of simply "blockchain" as it highlights the security, immutability, reliability, and auditability that the technology provides [33 - 35]. Additionally, the utilization of efficient contracts in financial operations is a significant advantage of DLT. As a consequence of circulated ledger technology, blockchain uses a one-way cryptographic hash function to maintain a secure, replicated, and distributed ledger of transactions that cannot be altered or disputed [36 - 39]. This consensus-verified, unchanging record of transactions among peers results in a single, agreed-upon version of the truth within the system [40 - 42]. Due to the temper-proof nature of DLT, it is

difficult for anyone to alter records, which boosts trust between parties [43 - 46]. By using a DLT platform, fintech companies can improve their bank-to-bank (B2B) transactions and reach agreements faster compared to traditional centralized systems, which may take one to several days to process [47, 48]. DLT's ability to securely record digital representations of fiat currency, securities, and physical goods opens numerous opportunities for fintech to build smart contracts and provide secure and innovative financial services. This allows for seamless trading and settlement of securities without manual intervention [49, 50].

Various blockchain platforms and technologies can be utilized in the Indian FinTech sector. Ethereum is a decentralized stage that permits the formation of smart contracts and decentralized applications (DApps) using blockchain technology. It is widely used in the FinTech space due to its open-source nature, strong set of tools, and frameworks for developing blockchain-based FinTech solutions. Hyperledger Fabric, on the other hand, is a key blockchain proposal that is planned for enterprise employment cases. Its modular architecture enables customizations and integrations with existing enterprise systems, making it ideal for FinTech utilization that needs safe and proficient processing of financial transactions and data. Ripple is a payment procedure and cryptocurrency that enables faster, cheaper, and more reliable cross-border payments. It uses a consensus algorithm called the Ripple Protocol Consensus Algorithm (RPCA) to authenticate transactions on its distributed ledger. Other blockchain technologies and protocols, such as Corda, Quorum, and Stellar, are also being developed and adopted in the Indian FinTech space. The choice of platform and technology relies on the particular needs and use case of the FinTech solution, as well as factors such as security, scalability, and regulatory compliance.

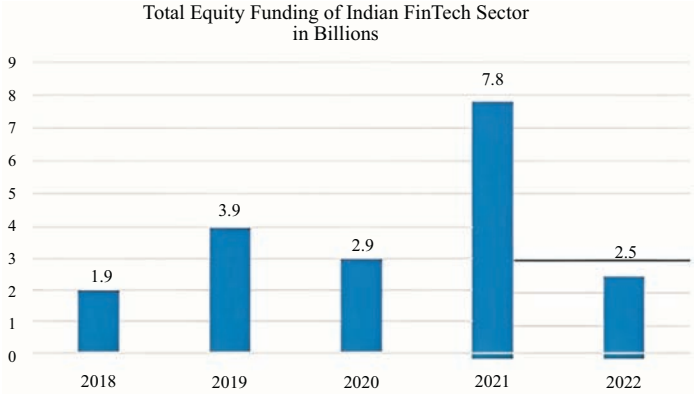

Fig. (1). FinTech adoption in India.

CHAPTER 3

Blockchain Technology and Smart Contracts for Financial Transactions in Virtual Environments

Pooja Sharma[1], Sangeet Vashishtha[1,*], Neeraj Saxena[2] and **Shruti Saxena[2]**

[1] *IIMT University, Meerut, India*

[2] *Sandip University, Nashik, India*

Abstract: Blockchain technology and smart contracts have revolutionized the way financial transactions are conducted in virtual environments. This review paper provides a comprehensive overview of the role of blockchain technology and smart contracts in shaping the future of virtual financial transactions. We explore the fundamentals of blockchain technology, its applications in the financial industry, and the pivotal role that smart contracts play in automating and securing virtual financial transactions. Furthermore, we discuss the benefits, challenges, and prospects of these innovations within the virtual financial landscape.

Keywords: Artificial intelligence, Blockchain technology, Cross-border payments, Cryptocurrency, Digital identity, Financial transactions, Kyc, Machine learning, Smart contracts, Virtual finance.

INTRODUCTION

In recent years, the convergence of financial transactions and virtual environments has given rise to transformative technologies that promise to redefine the way we conduct and secure digital transactions. At the forefront of this paradigm shift is blockchain technology, a decentralized and tamper-resistant ledger system originally designed to underpin cryptocurrencies like Bitcoin. However [1], its applications extend far beyond digital currencies, finding innovative use cases across various industries. One of the most noteworthy applications within the financial realm is the integration of blockchain technology with smart contracts [15].

Blockchain technology is a relatively recent innovation, which emerged within the last decade. Despite its short history, blockchains have garnered significant interest across diverse domains, including computer science, cryptography,

* **Corresponding author Sangeet Vashishtha:** IIMT University, Meerut, India; E-mail: sangeet83@gmail.com

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

finance, economics, civil law, healthcare, rights management, real estate, auctions, gambling, and various industries where challenges such as reliability, accountability, trust, and transparency are crucial [2 - 16]. Many assert that blockchains have the potential to revolutionize asset management to a degree comparable to the transformative impact the Internet had on communication.

Specifically, within the realm of Intelligent Environments and the burgeoning domain of the Internet of Things (IoT), blockchains have the potential to be a transformative force [3 - 8].

By leveraging smart contracts, blockchains introduce a groundbreaking element—provable trust—in the interactions among sensors, actuators, and processors owned by diverse entities spanning different jurisdictions and administrative domains. This breakthrough implies that blockchains have the capacity to bring a heightened level of reliability, transparency, and trust to both existing and future designs of intelligent environments [21].

AI can significantly enhance the functionality of smart contracts, especially through predictive analytics and fraud detection. Here's how these technologies could add value:

Predictive Analytics

Smart contracts are self-executing agreements that automatically enforce the terms written into their code. By integrating AI-driven predictive analytics, smart contracts can make more informed, proactive decisions, adding layers of intelligence beyond simple automation. Here's how:

Risk Assessment and Decision Making: Predictive models can assess the likelihood of certain outcomes (*e.g.*, default risk in insurance or credit). For instance, in insurance claims, smart contracts can use predictive analytics to determine whether a claim is likely to be fraudulent or predict the future behavior of a policyholder based on historical data.

Market Predictions for Dynamic Pricing: In use cases like decentralized finance (DeFi) or supply chain contracts, smart contracts can adjust terms dynamically based on AI's market trend predictions. For instance, in supply chains, AI could predict price fluctuations for goods or services, automatically adjusting contract terms to match market conditions.

Predicting Contract Triggers: AI could foresee when certain events (*e.g.*, financial triggers or performance milestones) are likely to happen, ensuring the

contract's clauses are executed at the optimal time or recommending renegotiations before breaches occur.

Personalization of Smart Contracts: Predictive analytics can also help tailor smart contract terms to individual participants by analyzing data such as past behavior, transaction history, or market conditions. For example, in the insurance industry, contracts can adjust premiums dynamically based on real-time data on a user's behavior [22 - 23].

Fraud Detection

Fraud detection is another area where AI can make smart contracts significantly more secure and reliable. By integrating machine learning models and pattern recognition algorithms, smart contracts can detect anomalies and mitigate fraud risks in several ways:

Real-Time Anomaly Detection: Machine learning models can analyze real-time transaction data to spot irregularities or suspicious patterns. If a fraudulent action or transaction attempt is detected, the smart contract could trigger specific clauses (*e.g.*, freeze funds, alert parties) to mitigate risks.

Behavioral Analysis: AI can track and analyze user behavior over time to establish a baseline of normal activity. When behavior deviates significantly from this baseline, AI could flag these transactions for further investigation before the contract is executed.

Anti-Money Laundering (AML) and KYC Compliance: AI can enhance smart contracts by screening transaction data and identifying suspicious behavior that could indicate money laundering. Smart contracts could be embedded with algorithms that enforce regulatory compliance by identifying high-risk users based on KYC (Know Your Customer) and AML policies.

Dynamic Contract Adjustments: If a smart contract detects potential fraud risks, it could dynamically adapt its terms. For instance, in peer-to-peer lending, if a borrower's creditworthiness deteriorates (detected by AI), the smart contract could adjust loan repayment schedules or interest rates to compensate for increased risk.

Automated Audits and Reporting

AI can continuously audit the execution of smart contracts, verifying compliance with contract terms and flagging any discrepancies. Predictive models can forecast potential contract breaches or regulatory non-compliance, allowing for preemptive action. This would be particularly valuable in industries such as

CHAPTER 4

Blockchain: Use of Smart Contracts in Finance

Ambika R. Thakur[1], Chetna Tiwari[1], Kartikey Vats[1] and **Garima Sharma[1,*]**

[1] *Department of Computer Science and Engineering, The NorthCap University, Gurugram, India*

Abstract: Through its decentralized architecture, blockchain technology has become a transforming paradigm in the banking sector, revolutionizing established procedures. This study analyzes the dynamic convergence of blockchain and finance, with an emphasis on smart contracts' essential role in altering financial transactions. It adds to the expanding knowledge of the practical uses and possibilities of this technology in the banking industry by investigating the uses, problems, and prospects of smart contracts within the financial environment. This research study digs into the many uses, effects, problems, and prospects of smart contracts in the banking industry. This chapter attempts to give a full knowledge of how smart contracts are revolutionizing financial processes and determining the future of the financial sector through theoretical studies.

Keywords: Applications, Blockchain, Decentralization, Efficiency, Finance sector, Improvements, Security, Smart contracts, Transparency.

INTRODUCTION

Blockchain technology was originally made public in 2008 when Satoshi Nakamoto released the Bitcoin software [1]. Blockchain is a system that enables many parties to have a secure, transparent, and immutable record of transactions. It was originally intended to be the core technology for the cryptocurrency Bitcoin, but its uses go well beyond that [1]. The blockchain networks can be broadly categorized into four categories, namely: (1) Public, (2) Private, (3) Hybrid, (4) Consortium. Table **1** provides a summary of the characteristics of all four blockchain networks.

This chapter delves into smart contracts, which are automated programs encoded with the terms of an agreement. These contracts, which operate on blockchain systems, automatically enforce terms when predefined criteria are satisfied, removing the need for an intermediary. By leveraging blockchain's decentralized

* **Corresponding author Garima Sharma:** Department of Computer Science and Engineering, The NorthCap University, Gurugram, India; E-mail: garimasharma@ncuindia.edu

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

nature, platforms like Ethereum ensure transparency and resistance to tampering during contract execution [2, 3]. Originally conceptualized by computer scientist Nick Szabo in the 1990s, smart contracts found practical applications with the emergence of blockchain technology, particularly on platforms such as Ethereum [3]. Fig. (**1**) illustrates the usage statistics of smart contracts in financial organizations like banks, insurance companies, and investment businesses.

Table 1. Various blockchain and their features.

Various Blockchain	Features
Public Blockchain	- Decentralized - Open to anyone - Transparent and verifiable - High security through consensus mechanisms
Private Blockchain	- Restricted access - Controlled by a single organization or consortium - Faster transaction processing - Enhanced privacy and confidentiality
Consortium Blockchain	- Shared among a group of organizations Blockchain - Permissioned access - Collaborative decision-making - Balances decentralization and control
Hybrid Blockchain	- Combination of public and private/consortium aspects - Offers flexibility based on use case requirements - Suitable for various industries and applications

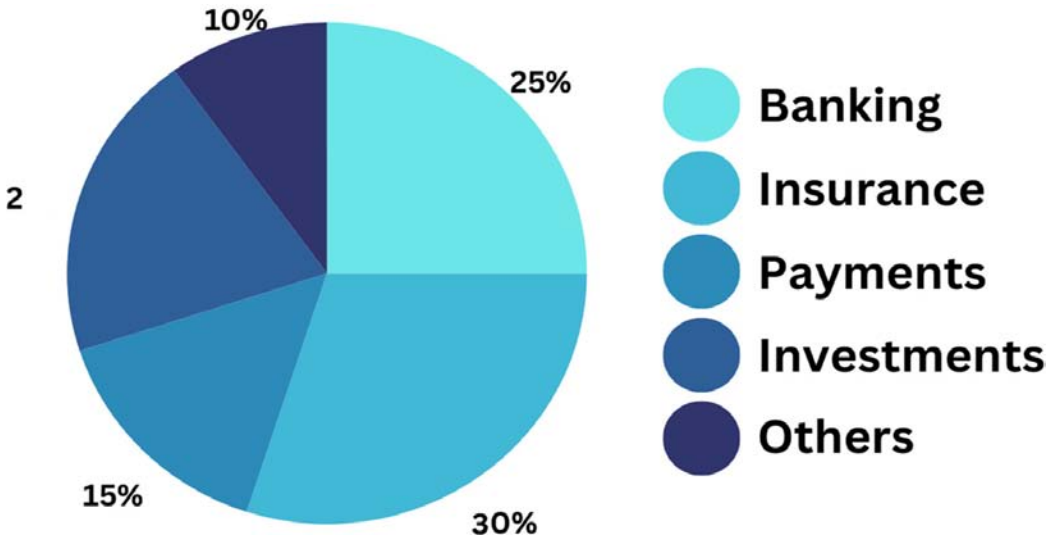

Fig. (1). Use of smart contracts in various financial sectors.

After discussing smart contracts, this chapter talks about the relationship between smart contracts and cryptocurrencies [5]. Smart contracts and cryptocurrencies are inextricably linked because smart contracts frequently run on blockchain systems that enable cryptocurrencies. To run on the blockchain, smart contracts demand computing resources. Native platform cryptocurrencies, such as Ether (ETH) in the case of Ethereum, are used to pay for the computational effort and storage required for smart contract execution [6]. This is frequently referred to as "gas" on the Ethereum network [6]. The term "gas" refers to the computing labor necessary to conduct operations or run programs (smart contracts) on the Ethereum blockchain [6]. According to 2023 data, the top 5 cryptocurrencies are (1) Bitcoin, (2) Ethereum, (3) Binance, (4) XRP, and (5) Solana as shown in Fig. (**2**) [7].

Fig. (2). Cryptocurrencies according to 2023 data.

Through its decentralized ledger, blockchain offers a platform for safe and transparent transactions [4]. On this blockchain, cryptocurrency's function, and smart contracts, which are programmable scripts, perform activities based on predetermined circumstances inside this decentralized and secure ecosystem [4]. The convergence of blockchain, cryptocurrencies, and smart contracts has resulted in novel applications and use cases that are transforming different sectors, notably banking [5].

The crux of this chapter discusses the application of smart contracts in the finance sector. The primary motivation of this study is rooted in the profound

CHAPTER 5

Blockchain in Agricultural Information Systems and Networks: Foundation and Future Potentialities - A Scientific Review

P. K. Paul[1,*], M. Kayyali[2], Nilanjan Das[3] and **Ritam Chatterjee[1]**

[1] *Department of Computer & Information Science, Raiganj University, Raiganj, India*

[2] *Department of Quality Assurance and Accreditation Directorate, Al Maaref University of Applied Sciences, Sarmada, Syria*

[3] *Siliguri Institute of Technology, Siliguri, India*

Abstract: Smart Agriculture, also known as Digital Agriculture, has emerged as an essential paradigm in today's agricultural landscape. The rapid development of this field is fueled by the growth and application of Agricultural Informatics, which significantly enhances various agricultural practices. These practices span from crop and seed cultivation to plant and vegetable farming, livestock management, and post-harvest activities.

Advanced Agricultural Information Systems (AIsS) deploy effective methodologies and cutting-edge technologies to optimize cultivation processes, aiming to improve productivity and efficiency. These Agroinformatics technologies are specifically designed to support more commercially intensive agricultural operations and streamline the management of large-scale systems. Agro Information Systems incorporate diverse components of Information Technology (IT), such as databases, networks, web technologies, software solutions, and multimedia systems, all of which contribute to a more connected and data-driven agricultural environment.

With the rapid evolution of IT, new technologies such as cloud computing, data analytics, big data, the Internet of Things (IoT), and Blockchain are becoming increasingly vital in modern agriculture. Among these, Blockchain technology is revolutionizing agriculture by enabling faster, more secure, and highly efficient systems for agricultural development. Blockchain applications in agriculture ensure transparency, traceability, and security in various processes, from farm-to-fork supply chains to smart contract-based transactions.

In this context, the integration of Blockchain and Machine Learning (ML) technologies plays a pivotal role in shaping Agriculture 4.0. By combining Blockchain's secure and decentralized nature with ML's predictive analytics and data-driven decision-making

* **Corresponding author P. K. Paul:** Department of Computer & Information Science, Raiganj University, Raiganj, India; E-mail: pkpaul.infotech@gmail.com

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

capabilities, these technologies offer unprecedented opportunities for improving farming practices. This paper explores the current applications of Blockchain and Machine Learning in agriculture, focusing on their potential and prospects in transforming the industry. Furthermore, it delves into how blockchain and Machine learning-based agrosystems can foster sustainable agricultural practices, supporting the future of farming by enhancing productivity, reducing waste, and promoting environmental stewardship.

Keywords: Agro ICT, Agriculture 4.0, Agro informatics, Digital agriculture, ML, Machine learning applications, Sustainable development.

INTRODUCTION

Agricultural development through the use of technology and appropriate techniques is crucial for the advancement of the sector. The application of Information and Communication Technology (ICT) and Information Technology (IT) has given rise to fields like Agricultural Information Technology (AIT), Agricultural Information Systems (AIS), and Agricultural Information Sciences (AISc), among others. Blockchain technology plays a significant role in the realm of computing and information technology, offering a wide range of potential applications for the future.

Blockchain functions as both a technology and a system within Information Technology, designed to maintain encrypted records of data. It is also used in the creation and management of distributed databases, which are critical for facilitating data transactions and various types of contracts. As a distributed database, Blockchain aims to maintain accurate and independent records, often referred to as digital ledgers. These systems are decentralized, ensuring accessibility across multiple platforms. In addition, Blockchain serves as a platform for digital monetary services, facilitating transactions involving digital currencies, such as Bitcoin. Both tangible and intangible assets can be recorded within a specific network or blockchain framework [2, 3, 27].

Blockchain has emerged as a highly sought-after tool for improving financial management. An effective Blockchain system relies on various processes that ensure efficient business transaction management. The rapid expansion of Blockchain applications across diverse industries has led to its recognition as a formal academic discipline, with many universities around the world offering courses related to it.

Since Blockchain enables the effective management of financial transactions without the need to share personal data with third parties, it adheres to strong encryption standards, reducing the risk of data breaches. Despite ongoing

concerns about large-scale data breaches and cyber-attacks, Blockchain's fraud-resistant features have revolutionized business practices, making them more secure and transparent. In comparison to traditional business processes, Blockchain offers greater efficiency and effectiveness, making it applicable across various sectors.

Machine learning algorithms, which are widely used across different industries, can also play a crucial role in enhancing agricultural productivity. When integrated with Blockchain technology, machine learning contributes to the development of smart agriculture, improving agricultural informatics practices. As a result, agro-ICT systems that focus on quality, quantity, and productivity are increasingly being adopted in both developed and developing countries. The combined power of Blockchain and machine learning can also be applied in underdeveloped regions to significantly boost agro-product production [6, 7, 10].

WORK OBJECTIVE AND AIM

This work, *'Blockchain in Agricultural Information Systems and Networks: Foundation and Future Potentialities - A Scientific Review,'* is a scientific review with the following objectives:

- To provide updates about the fundamentals of Agricultural Information Systems (AIS), including its features and related subjects.
- To gather information about allied technologies of agricultural information systems, especially their enhancement using Blockchain Technologies.
- To examine the basic features, foundation, and general applications of blockchain and machine learning technologies.
- To explore the fundamental and emerging applications of agricultural information systems using blockchain.
- To understand the fundamental concept of Agriculture 4.0, its features, and possible impact in the context of machine learning-supported blockchain technologies.
- To identify the latest issues and challenges in agricultural robots, emphasizing agro informatics development.

METHODS

The work titled *"Blockchain in Agricultural Information Systems and Networks: Foundation and Future Potentialities - A Scientific Review"* is a scientific review focusing on the role of Blockchain in agricultural information systems, particularly in the context of agricultural robots. This review involves the study of

CHAPTER 6

Deep Learning-based Intrusion Detection System for IoT-based Blockchain System

J. Jayaganesh[1,*], Sreenivas Mekala[2], M. Kalyan Chakravarthi[3], R. Sundarrajan[4], Belsam Jeba Ananth M.[5], Mohit Tiwari[6] and **Manika Manwal[7]**

[1] *Department of Computer Science, Government Arts and Science College Perumbakkam, Chennai, India*

[2] *Department of Information Technology, Sreenidhi Institute of Science & Technology, Hyderabad, India*

[3] *School of Electronic Engineering, Vellore Institute of Technology, Andhra Pradesh, Amaravathi, India*

[4] *Department of Information Techology, Kalasalingam Academy of Research and Education (Deemed to be University), Virudhunagar, India*

[5] *Department of Mechatronics Engineering, SRM Institute of Science and Technology, Kattankulathur, India*

[6] *Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, Delhi, India*

[7] *Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India*

Abstract: Security and privacy concerns, which are made worse by the growing number of Internet-connected devices, are the primary obstacles to the Internet of Things (IoT) widespread implementation. Everyone is now very concerned about Internet of Things security, including businesses, governments, and consumers. Even though no system can ever be completely protected from attacks, effective system defense depends on real-time threat detection. There is a dearth of studies on intrusion detection systems that work well in IoT-based blockchain systems. In this study, we present a novel approach to intrusion detection in the Internet of Things-based blockchain systems by employing the DL (Deep Learning) subfield of machine learning to identify security abnormalities. This detection platform provides security as a service and allows interoperability with numerous network communication protocols utilized by the Internet of Things. We go into great details about the suggested system's architecture and intrusion detection method. Real network traces are evaluated along with simulated data to illustrate the scalability of the proposed intrusion detection system to prove its viability. Our results confirm that the proposed intrusion detection system can correctly detect real intrusions.

[*] **Corresponding author J. Jayaganesh:** Department of Computer Science, Government Arts and Science College Perumbakkam, Chennai, India; E-mail: everjays@gmail.com

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

Keywords: Smart contracts, Blockchain, Deep learning, IoT, Intrusion detection.

INTRODUCTION

A network of common physical things that can be linked to the Internet and utilized to transmit data and combine it with other network resources is known as the Internet of Things, or IoT [1]. These items are either sensors or networked digital gadgets that can exchange data *via* the World Wide Web after being collected. New applications and services are produced as a result of these interactions among people, processes, sensors, and connectivity. In the Internet of Things, these electronic gadgets or sensors are called "things." IoT networks are essentially formed by connecting IoT devices that are within a user's range, usually within ten meters. These networks feature an unstable topology that is subject to alter over time [2]. IoT technology is being utilized more and more in a variety of fields, including business-augmented services, health care, national security, and, on a smaller scale, smart home environments. IoT networks are getting more and more popular, which makes them more vulnerable to security breaches. Attacks on cyberspace are turning into one of the biggest risks to IoT security [3]. Blockchain technology is driven mostly by the need for decentralization. Blockchain's open and accessible record ensures that a single node breakdown has no impact on the entire network. Blockchain transformed the transactional networking structure from a constellation to a point-to-point (P2P) design. This changed architecture enables 2 entities to connect openly through the use of encrypted and safety depending on coding and algorithmic safety. Therefore, it is crucial to secure IoT-based blockchain systems and build intrusion-resistant IoT networks to protect sensitive data.

Research Objective

The objectives of this research are as follows:

- To have a thorough understanding of IoT and its constituent parts.
- To research anomaly detection approaches and construct an intrusion detection model for Internet of Things networks based on deep learning.
- To assess the model and offer suggestions for improving its development.

Scope and Limitations of Study

To facilitate safe data transfer among Internet of Things devices that are located close to one another, this study aims to develop an intelligent, portable intrusion detection system. The goal of this system is to examine textual or numerical real-world data that is contained in network packets. At present, this technology is not designed to handle encrypted or raw/unformatted data. Moreover, this intrusion

detection system can only identify anomalies at the transport layer. As such, it will be difficult to find more sophisticated or physical attacks that could use this method to alter or tamper with the hardware of Internet of Things devices. Despite being designed to be portable, the recommended intrusion detection system is meant to be a logical control that is, software rather than a physical control for Internet of Things networks.

LITERATURE REVIEW

Internet of Things Definition

All current gadgets that can generate data and send it *via* the Internet are collectively referred to as the IoT. According to a recent study, the total number of internet-connected devices is predicted to surpass 6.4 billion by 2016 and reach 20.8 billion by 2020 [4]. The iPhone, iPad, iWatch, Smart TVs, and many other gadgets are on this list.

IoT Security Issues and Existing Intrusion Detection Methods

The characteristics of hacker groups involved in cybercrime are covered by some researchers [5]. They define cybercrime, discuss its potential, meaning, and the theoretical and practical difficulties in dealing with these cyber offenders, and come to the conclusion that state actors' cybercrime and protest-oriented cybercrime are more structured and specialized than regular forms of protest. They contend that although cybercriminals operate in loose networks, even in cases where their attacks span national borders, they are still physically close to one another. Research efforts are focused on mitigating security risks associated with IoT network protocols, such as the Constrained Application Protocol (CoAP) [6], which holds great potential for the ambitious vision of a Smart City Environment. They recommend a modular rule-based intrusion detection framework, but their results highlight the advantages of a hybrid approach that blends anomaly- and rule-based intrusion detection. Furthermore, the IDS system they had in place was limited to mitigating routing assaults. Using behavioral modeling, Arrington *et al*. suggest identifying anomalies connected to non-playing characters (NPCs), or people acting out various roles within or around a smart home, as a means of detecting intrusions in smart homes [7]. The proposed work claims to create cost-effective, easily verifiable autonomous monitoring for intrusion detection, but it does not specify which hardware implementation or IA was utilized.

CHAPTER 7

E-analysis and Notarization of Social Media based on Blockchain Technology

K. Santhanalakshmi[1,*], G. Madhumita[2], Martin Selvakumar Mohanan[3], Sathish Kumar R.[4], Belsam Jeba Ananth M.[5], Subhrajit Chanda[6] and **Gunjan Chhabra[7]**

[1] *Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, India*

[2] *Department of Management Studies, Vels Institute of Science Technology and Advanced Studies (VISTAS) Chennai, India*

[3] *Department of Organization & Human Resource Management, Great Lakes Institute of Management, Chennai, India*

[4] *Department of Artificial Intelligence and Machine Learning, Faculty of Engineering and Technology, Jain University (Deemed-to-be-University), Bengaluru, India*

[5] *Department of Mechatronics Engineering, SRM Institute of Science and Technology, Kattankulathur, India*

[6] *Jindal Global Law School, OP Jindal Global University, Sonipat, India*

[7] *Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India*

Abstract: Social media has completely changed how people communicate on a worldwide scale by offering a robust platform for idea sharing, contract negotiations, and the submission of fresh business concepts. However, a number of problems, such as inaccurate information, inadequate content screening, copyright infringement, hacking, identity theft, and fake news, limit the use of social media. This paper presents a proof-of-credibility (PoC) and notarization service-based blockchain strategy for identifying fake news and preventing its spread through social media. Social media platforms are using machine learning methods as part of their marketing strategies. On social media, however, deliberately created screenshots and bogus news are constantly created and shared. Blockchain technology is a good platform for notarizing online activity because it can store data in a safe, unchangeable manner. The Proof-of-Concept methodology was tested on two datasets of notable tweets gathered from various news sources on Twitter. We propose a framework for the authenticated archiving of social media content using blockchain technology. A text message scenario is given as a proof-of-concept based on the suggested strategy, and the results demonstrate how well the suggested approach works in identifying rumors and halting their spread.

[*] **Corresponding author K. Santhanalakshmi:** Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, India; E-mail: santhank@srmist.edu.in

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

Keywords: Blockchain, E-analysis, Fake news, Machine learning, Notarization, PoC, Social media.

INTRODUCTION

Social media refers to internet sites that let users create social networks or engage with others who have similar interests, pastimes, life experiences, or connections [1]. It is now very difficult to share essential materials on social media sites like Facebook, Twitter, and Instagram if you do not first evaluate its credibility. The spread of incorrect information and fake news on social media platforms poses a severe threat to academics and Social Network Service Providers (SNPs) [2]. Furthermore, because people are more prone to disseminate fake information across their social networks farther, faster, and deeper than real information, on social media, this false information spreads like wildfire [3]. Furthermore, it is challenging to prosecute criminals due to the absence of credible digital evidence.

This study provides a revolutionary technique to notarize social media content using blockchain technology, together with Proof of Credibility (PoC) that can detect false information spread throughout social networks and validate shared information [4].

Businesses use machine learning findings to better understand customer perspectives and to enhance their marketing tactics. Machine learning instruments can help electronic advertisers more effectively indicate and understand data, which is an advantage. By maintaining apprised of consumer tastes and providing the required information, one may forecast the actions of online customers. The generation and dissemination of information could be altered by developing blockchain-based solutions [5]. When creating a trusted social system, blockchain technology can offer transactions that are transparent, verifiable, trustworthy, immutable, and dependable [6].

A blockchain is an ever-expanding collection of blocks that include transaction data, a timestamp, and a cryptographic hash of the previous block [7]. Data integrity is immediately guaranteed by blockchain technology once transaction data is recorded there. Blockchain is the perfect platform for notarization services because of this feature. Ensuring that input data are not changed before being incorporated into a block is an important but difficult issue. Then, if you want to notarize user-provided content that is unchangeable, an official social media service provider can be of great assistance. Specifically, official service providers can submit a document or photo with a digital signature in response to requests from users on social media accounts. The document's validity can be confirmed through the use of a public key infrastructure (PKI) protocol.

Any document that lacks an authentic signature from the official service provider shall be regarded as fraudulent according to the PKI standard. Furthermore, it is anticipated that the malevolent actions of spreading false information would significantly reduce because any attempt at shifting public opinion using fake news will be permanently stored in the blockchain.

We look into the idea of applying blockchain theory to the creation of a unique Proof of Credibility (PoC) protocol that may be used to identify false information spread *via* social networks and validate shared information. 1003 notable tweets pertaining to the famous hashtag #ISIS and 802 remarkable tweets pertaining to the well-known hashtag #Halamadrid, collected from multiple news outlets on Twitter, are used to evaluate the proposed technique. The results demonstrated that a standard blockchain consensus could be established to verify the accuracy of information and stop misinformation from spreading on social media. Proof of Concept (PoC) will be the first blockchain solution to address the issue of false information and fake news on social media.

Objective of Study

- To look into the potential of applying blockchain theory to the creation of a revolutionary Proof of Credibility (PoC) protocol that can be used to identify false information on social media networks and validate material that has been posted.
- To examine how social media posts can be notarized using blockchain technology.
- To get over the primary problems with censorship, fake news, and privacy on social media.

LITERATURE REVIEW

Notarization

Notarization usually involves a variety of procedures to assure the parties to a transaction (such as business formation, patent applications, and intellectual estate protection) that the documents certifying the transaction are legitimate [8]. Every one of those processes involves a number of parties, from the party seeking notarization to the central authority, which essentially verifies the accuracy and validity of the required documents and the signatures placed on them. To put it simply, by monitoring the procedure, the central organization assures the legitimacy of the transaction.

Let us examine the situation from the standpoints of the IT administrator, the notary public, and the person who granted the power of attorney. Thanks to

CHAPTER 8

Development of Smart City using Blockchain and Artificial Intelligence

Chetan Shelke[1,*], Preeti Gupta[2], Binod Kumar[3], Abhijeet Kaiwade[4], Belsam Jeba Ananth M.[5], Sumeet Gupta[6] and **Satvik Vats[7]**

[1] *Alliance College of Engineering and Design, Alliance University, Bangalore, India*

[2] *Department of Computer Science and Engineering, Jain University (Deemed-to-be-University), Bangalore, India*

[3] *Department of Computer Applications, JSPM's Rajarshi Shahu College of Engineering, Pune, India*

[4] *Institute of Management and Research., Abhinav Education Society's Institute of Management and Research, Pune, India*

[5] *Department of Mechatronics Engineering, SRM Institute of Science and Technology, Kattankulathur, India*

[6] *Global Economics and Finance Cluster, School of Business, University of Petroleum and Energy Studies, Dehradun, India*

[7] *Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India*

Abstract: The rapid uptake of blockchain and artificial intelligence (AI) technologies like machine learning (ML) in particular has brought about a paradigm change that is elevating the digital ecosystem for smart cities. The development of new technology can be used to create intelligent societies within smart cities in this era of rapid digital communication. Uses of blockchain technology and ML technologies are proliferating, guaranteeing solutions for issues in a multitude of sectors, such as financial services, cryptocurrency, threat intelligence, social and public services, and the Internet of Things. These "smart cities" are constructed using various technologies, including artificial intelligence and blockchain. As a result, the way these technologies are applied in smart cities both present and future will alter not only the character of governance and human interaction but also the way business is done. The research suggests doing an experimental study to find out how blockchain technology and artificial intelligence are affecting the creation of smart cities. It tries to set the scene for queries like how traditional business models are getting ready for this disruption, what obstacles they might encounter, and what effects both technologies might have on the organization's growth. Blockchain technology and artificial intelligence have a lot

* **Corresponding author Chetan Shelke:** Alliance College of Engineering and Design, Alliance University, Bangalore, India; E-mail: binod.istar.1970@gmail.com

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

of potential to help create smart cities. The results of the research will provide corporations with the rationale to start concentrating on these technologies and putting early adoption strategies into place, which will eventually cause them to change their smart city business models advance.

Keywords: Artificial intelligence, Blockchain, Development, Electronic commerce, Smart city.

INTRODUCTION

Smart cities are high-tech urban areas with intelligent subsystems linking individuals and institutions. These cities have the capacity to provide quick access to high-quality public services, hence improving the quality of life for all stakeholders, by using big data collections. Information and communication technology foster economic progress. In addition to enhancing city administration, they may have had the greatest impact on promoting social interaction and the sharing concept [1].

By 2030, 66% of people on Earth will reside in big cities, according to UN estimates [2]. This means that in order to maintain social sustainability, we must address a number of challenges. Additionally, this type of city structure presents social and environmental challenges. Municipalities are using up about half of the world's resources. It creates problems when distributing these resources using current technology in a uniform manner [3]. Thus, ICT (information and communication technology) might be very important to the idea of smart cities.

As the world grows more interconnected, the fourth industrial revolution—fueled by inventions like the internet is speeding up. In order to perform transactions securely and quickly, new sectors are emerging as a result, such as smart cities, which combine internet connectivity, blockchain technology, and online payment [4]. Moreover, Schwab and Davis [5] assert that data is the driving force behind the fourth industrial revolution. As a result, data-intensive methods like cloud computing, artificial intelligence, machine learning (ML), and the Internet of Things (IoT) will become more valuable and widely used. The purpose of this research is to demonstrate how blockchain technology and artificial intelligence can be used to further the development of smart cities (Fig. **1**).

Pervasive sensors are transforming urban transportation, improving security, and making it easier to collect enormous amounts of data that artificial intelligence (AI) computers can analyze. They enable the city to monitor and react to resident mobility, as well as to communicate with its own infrastructure. The conditions of the city can therefore be optimized. ML is built to gather, analyze, and interpret data accurately and efficiently while requiring no human intervention. ML is still

a away from becoming self-sufficient, but it may learn and develop by collecting and evaluating new data that must be supplied and stored correctly. Because of its distributed registry architecture, which allows data to be stored concurrently on all network nodes, blockchain technology is advantageous in this respect. Complete decentralization of data is made possible by this, improving the efficiency and "democratic" nature of data access.

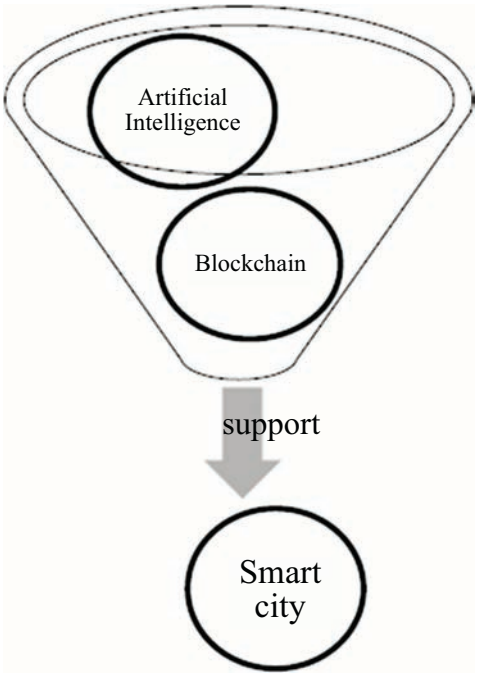

Fig. (1). AI and blockchain as elements supporting the creation of smart cities.

However, since these smart cities are constructed on consolidated facilities, attacks that take benefit of a single point of failure can target them. For instance, even though it might not be as convenient, a bank has the authority to charge astronomically high fees for each transaction. In addition, the bank may not always be online or might have a breach, providing dishonest attackers with access to customer data, as the recent Capital One data leak demonstrates [6]. Moreover, the increased demand for personal data, such as credit card numbers, passport details, and medical histories, on the dark web exposes citizens of smart cities to needless risk [7].

Blockchain technology was inspired by Satoshi Nakamoto's Bitcoin paper, and it is necessary to solve these and other problems that smart cities have [8]. Blockchains can perform peer-to-peer atomic transactions that eliminate

CHAPTER 9

Blockchain, Big Data, and Deep Learning-based Fraud Detection System for Credit Card Fraud

Nur Mohammad Ali Chisty[1,*], Shweta Gakhreja[2], Yogita Satish Garwal[2], Belsam Jeba Ananth M.[3], Tripti Tiwari[4], Dharamvir[5] and **Kamreed Udham Singh[6]**

[1] *Cyber Crime Wing, Anti-Terrorism Unit, Bangladesh Police, Dhaka, Bangladesh*

[2] *Manipal University Jaipur, Jaipur, India*

[3] *Department of Mechatronics Engineering, SRM Institute of Science and Technology, Kattankulathur, India*

[4] *Department of Management Studies, Bharati Vidyapeeth (Deemed to be University) Institute of Management and Research, Delhi, India*

[5] *Department of Computer Application, The Oxford College of Engineering, Bengaluru, India*

[6] *School of Computing, Graphic Era Hill University, Dehradun, India*

Abstract: Companies in the financial industry are among those who are implementing their operations online as a result of the internet's rapid growth in usage. Because of the enormous economic damages that arise from financial fraud, it is becoming an important concern as financial frauds are becoming more common and sophisticated globally. An economic fraud detection system (FDS) must be able to identify risks such as unusual assaults and unauthorized entry. The last few decades have seen a widespread application of data mining and machine learning (ML) methods to address this problem. These techniques still require improvement, though, to handle big data quickly and recognize unidentified trends in attacks. The importance of data safety and evaluation systems for big data has changed recently due to the enormous volume of data and its continuous growth. Big data is defined as information that is difficult to handle, store, and evaluate using standard software tools and databases. Big databases exhibit considerable quantity, speed, and diversity, necessitating the development of novel methods for handling them. Thus, employing blockchain and a deep learning-based (DL) approach for FDS is suggested in this work for credit card frauds. The objective of this framework is to improve the accuracy of identification in the context of big data in a private-permissioned blockchain network, while also improving the existing detection methods. A present DL algorithm called the Auto-encoder algorithm

[*] **Corresponding author Nur Mohammad Ali Chisty:** Cyber Crime Wing, Anti-Terrorism Unit, Bangladesh Police, Dhaka, Bangladesh; E-mail: nmachisty@gmail.com

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

and a few other ML algorithms are contrasted with the outcomes of the suggested framework's evaluation using a real database of credit card frauds. According to the study findings, the LSTM performed flawlessly, achieving 99.9% accuracy in roughly a minute.

Keywords: Big data, Blockchain, Credit card frauds, Deep learning, Fraud detection system.

INTRODUCTION

The variety of bank operations using credit cards has increased dramatically in the past few decades, as has the incidence of fraud and card burglary. According to the 2018 Organization for Financial Analysts Settlements Fraud Poll [1,] there has been a rise in transactions scams. As per the research, a record-breaking seventy-eight percent of every company experienced fraudulent payments last year, totaling seven hundred treasury and finance experts. Finance organizations have dropped billions of dollars because of credit card fraud since the emergence of electronic payments [2]. As a result of this problem, financial companies and banks encounter the difficulty of developing efficient and assertive fraud detection systems (FDS).

Illegal economic operations are highly complex and difficult to detect. With the advancement of contemporary innovations, especially inside the economic industry, fraud is on the rise. There are many kinds of fraud in finance structures, including internet banking deception, credit card deception, fake loans, documentation deception, Phishing, fraud, and fake logins, among many others. Fraud charges cost economic institutions millions of dollars each year, negatively impacting the institution's economic position and client trust [3].

Worldwide economic organizations and corporations are suffering huge damages as a result of several economic frauds. Daily, there are reports of credit card information being hacked. An illegal activity employing debit and credit card information without the consent of the true client is ringing a warning for financial institutions, clients, and authorities all over the globe [4].

Monetary fraud has become an enormous issue. Unapproved access and unique assaults are detected by employing an approach to identify banking fraud. Banking organizations should regularly improve their processes to identify fraud. In recent years, machine learning (ML) and data mining techniques have become widely utilized to address this issue [5]. Nowadays, ML is frequently employed in financial services and industries for a variety of uses, including portfolio administration, dealings, risk evaluation, avoidance, and fraud detection. In the financial sector, for instance, ML is employed to create Chatbots, which are

artificial intelligence programs that communicate with clients and react to their inquiries [6]. Decision Dealing Support Devices, also known as Computational Dealing, are employed in dealing with making highly rapid choices. Furthermore, among the main applications of ML in the financial services sector is fraud detection. Identifying illicit behavior became less difficult with the assistance of ML methods. Built on the transaction history, ML demonstrated novel approaches for analyzing client behavior and determining whether or not there is fraud [7].

Nevertheless, these methods must be enhanced in the areas of computing expenses, memory expenses, and handling big data, which is becoming an aspect of modern economic deals. Economic fraud detection is a difficult issue because of 4 essential causes: (1) fraudulent conduct is continually transforming, (2) there is no process for monitoring data on a fraudulent deal, (3) present identification methods (such as ML methods) have specific constraints, and (4) economic fraud databases are extremely biased, making it difficult to train methods [8]. Previous research has explored the potential of blockchain-based technologies and smart contracts in cooperative and distributed DL. Maintaining confidentiality is crucial for a secure collaborative environment. The objective of this study is to suggest a FDS centered on a deep learning (DL) method. This system is designed to detect skeptical financial transactions and notify suitable officials so that suitable measures can be taken. As an outcome, the suggested approach could be a helpful instrument for the banking industry in reducing possible losses.

LITERATURE REVIEW

DL is outlined in a study[9] as an excellent option for dealing with scams in banking transactions by causing the most effective utilization of financial institutions' big data. DL is a catch-all term for ML that employs an advanced multiple-layer artificial neural network (ANN). It is a physiologically encouraged system of human cells made up of multifaceted hidden layers of nonlinear computational units, with every neuron capable of sending data to another neuron within the hidden layers [10]. The research conducted by some authors [11] presents a blockchain-based progressive outlier clustering method that is both mathematically efficient and successful in terms of functionality. Blockchain innovation is being employed to improve system safety, while DL methods are employed for prediction purposes.

They constructed an approach for detecting fraudulent use of credit cards depending on data gathered from purchases made with credit cards. The findings demonstrated the significance of categorizing characteristics such as kinds of goods, purchases kinds, and places, among others, in detecting the fraudulent use of credit cards. The application of a Logistic Regression (LR) method for

CHAPTER 10

IoT-driven Blockchain System for Prediction of Heart Disease Using Smart Healthcare Monitoring Deep Learning Model

Mrunal K. Pathak[1,*], Shaik Balkhis Banu[2], Anupama Chadha[3], Gaurav Kumar[4], Shashi Kant Mishra[5], Tarun Jaiswal[6] and **Vikrant Sharma[7]**

[1] *Department of Information Technology, AISSMS Institute of Information Technology, Savitribai Phule Pune University, Pune, India*

[2] *Department of Physiotherapy, Fatima College of Health Sciences, Al Ain, UAE*

[3] *Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, India*

[4] *School of Computer Application, Lovely Professional University, Phagwara, Punjab, India*

[5] *Guru Nanak Institute of Technology, Hyderabad, India*

[6] *National Institute of Technology, Raipur, India*

[7] *Department of Computer Science and Engineering, Graphic Era Hill University; Adjunct Professor, Graphic Era Deemed to be University, Dehradun, India*

Abstract: The Internet of Things (IoT) is utilized to enhance conventional healthcare organizations in a variety of ways, such as monitoring patient habits. Sensor data from the IoTs is critical for medical facilities. Due to confidentiality and safety concerns, data should be safeguarded from unwanted alterations. On the contrary, Blockchain innovation offers a variety of ways to protect data from alterations. Deep learning (DL), as a subsection of machine learning (ML), has the revolutionary possibility to reliably analyze enormous amounts of data at very fast rates, provide insightful conclusions, and effectively resolve complex problems. Preventive treatment and prompt intervention for individuals at risk depend heavily on rapid and precise disease prediction. The capacity to handle consecutive time-series data with recurrent neural network variations of DL depends on developing prediction systems with improved accuracy, which is crucial given the increased usage of electronic clinical documents. Prediction analysis is used for the electronic clinical data kept in the cloud regarding patient records by the proposed framework, which acquires data from IoT gadgets. With an accuracy of 98.8 percent, specificity of 98.8 percent, precision of 98.9 percent, and F-value of 98.8 percent, the bidirectional long short-term memory-based intelligence medical network for monitoring and precisely predicting heart disease threat outperforms the current Intelligent cardiovascular illnesses prediction structures.

[*] **Corresponding author Mrunal K. Pathak:** Department of Information Technology, AISSMS Institute of Information Technology, Savitribai Phule Pune University, Pune, India;
E-mail: mrunal.pathak@aissmsioit.org

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

Keywords: Blockchain, Deep learning, Internet of things, Heart disease, Prediction.

INTRODUCTION

The advancement of science and technology has coincided with the emergence of humankind. Innovations in the fields of medical services, agriculture, transport, and logistics, among others, have been made possible by the progress made in information and communication technology (ICT). The IoT Internet of Things is a significant factor behind the technological growth of ICT and is guiding future industries toward automated and decentralized intelligence [1]. The Internet of Things is constantly changing, influencing every aspect of our lives and acting like a living thing. The IoT links individuals, information, things/objects, and processes—from robots in industries to domestic gadgets. In the meantime, cloud computation offers flexible service-on-demand with nearly limitless processing and storage capacity. Parts of cloud computing and the IoTs support one another even if they have evolved independently and uniquely [2]. The two innovations eventually developed together in the last few years, and the resultant convergence was dubbed the Cloud-IoT model [3, 4]. This presented enormous opportunities for launching brand-new, cutting-edge services .

Since information technology uses started to distantly gather, route, and manage the condition of patients, wellness-based uses were driving advances in science and technology. As a result, IoT is driving and revolutionizing current advancements in healthcare by using wearable technology and sensor systems to collect patient physiological information [5]. The Cloud-IoT leverages the vast capacity of the Cloud to store and handle massive amounts of patient medical files, comprising sensing statistics from healthcare IoT for investigation in the medical industry.

Analytics follows the methodical, statistical, and qualitative examination of medical data for effective decision-making, while prediction analyses come from enhanced statistics aiming to evoke the prediction of prospective incidents utilizing accessible statistics [6]. Among other critical responsibilities in healthcare, statistics is used for medical decision assistance, prediction risk evaluation, and distant health monitoring. A large portion of healthcare involves risk prediction and reduction using historical and present patient statistics. The combination of humongous datasets from different resources encompassing electronic clinical data (ECD), healthcare imaging, testing outcomes, and administration data warranting rapid judgments is effectively handled by medical statistics [7]. Clinicians frequently have to make highly unpredictable decisions, but because of advancements in prediction analysis, such decisions will be better

enlightened than ever. With the use of these state-of-the-art prediction analysis techniques, one may prevent hospital readmissions, minimize overhead costs, avoid complications, enhance long-term disease care, and detect problems early on. Microservices have prompted a shift from centralized to decentralized frameworks among developers and scholars. The benefits of blockchain innovation are discussed, as well as its possible uses in healthcare institutions.

Healthcare prediction analysis uses a range of methods, from sophisticated machine learning (ML) and artificial intelligence (AI) methods to traditional linear frameworks [8]. A branch of machine learning called deep learning (DL) is strong and dependable enough to manage and acquire knowledge from massive amounts of complicated medical data autonomously. It also provides useful knowledge and solutions to challenging situations. Its use in a broad range of healthcare settings has outperformed the outcomes of conventional systems. In particular, the recurrent neural network (RNN) [9] has gained popularity in the investigation of temporal occurrences and time-sequential activities and is capable of handling the ongoing connections of input statistics. The current period is driven by Industry 4.0, which involves implementing high-touch technologies and developing blockchains for real-time utilization of patient clinical data employing deep learning (DL).

Hence this aims to investigate the heart disease prediction rate using the DL algorithm. In this study, a fuzzy information system (FIS) is used for initial classification activity. Bidirectional long short-term memory (Bi-LSTM) is precisely employed to predict the risk of heart disease.

LITERATURE REVIEW

Incorporating blockchain and cloud technology creates a multitier structure for incorporating IoT into healthcare systems. Various techniques have been proposed recently for the prediction of heart disease. An accuracy of 85.4 percent is shown by deploying multiple ensemble classifiers to improve the accuracy of cardiovascular disease risk prediction [10]. A study proposed a fog strategy for handling healthcare data that combines blockchain and the cloud [11]. The primary purpose of the approach is to offer patients the ability to manage their personal information. Fog nodes are deliberately located near detectors to create a distributed blockchain with an authorization tier for data access by users. This article presents an instance analysis that evaluates the efficacy, openness, and availability of the proposed design in several settings, such as resident medical services.

CHAPTER 11

Adoption of Machine Learning Techniques in Smart Applications based on Blockchain Technology

K.M. Rashmi[1,*], Balraj Kumar[2], K.T. Thilagham[3], Harish Kumar[4], S. Aswath[5], Mohit Tiwari[6] and **Rahul Chauhan[7]**

[1] *Department of Electronics and Communication Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, Karnataka, India*

[2] *School of Computer Application, Lovely Professional University, Phagwara, Punjab, India*

[3] *Department of Metallurgical Engineering, Government College of Engineering Salem, Salem, India*

[4] *Department of Computer Science, King Khalid University, Abha, Saudi Arabia*

[5] *Department of Electronics & Communication Engineering, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai, India*

[6] *Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, Delhi, India*

[7] *Department of Computer Science, Graphic Era Hill University, Graphic Era Deemed to be University, Dehradun, Uttarakhand-248007, India*

Abstract: The Internet of Things (IoT) has advanced toward smart houses as a result of the widespread detection and supply administration brought about by the advancement of technological advances in the field of sensing devices advancements. Many IoT gadgets in smart houses are represented by gateway links, the safety of which is dependent on the centralized framework. The blockchain structure is thought of as a smart house gateway to handle safety concerns in this system by fending off potential threats and utilizing the machine learning algorithm Deep Reinforcement Learning (DRL). The safety and dependability of the suggested blockchain-oriented smart house strategy were thoroughly assessed in terms of reach, confidentiality, and authenticity. In the data storage and transfer of blocks, blockchain is used to circumvent conventional centralized design. The capacity of networked users to authenticate is caused by the data authenticity within and outside of the smart house. The system that is being exhibited is built on the Ethereum blockchain, and its safety, responsiveness, and accuracy are measured. The results of the study demonstrate that the suggested fix outperforms more current, published works. The most successful parts of the suggested method to enhance structure performance oriented on appropriate values and integrate

[*] **Corresponding author K.M. Rashmi:** Department of Electronics and Communication Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, Karnataka India; E-mail: rashmi.km@manipal.edu

Keshav Kaushik, Rewa Sharma & Ayodeji Olalekan Salau (Eds.)

with blockchain in terms of smart house safety oriented on smart gadgets to prevent sharing and confidentiality hackers are found in DRL, a machine learning-based method. This chapter tested the suggested approach using two different kinds of databases and then contrasted it to other state-of-the-art systems. In the subsequent phase, when there are sixteen percent disparities in terms of enhancing the accuracy of smart houses, a DRL with an accuracy of 96.7 percent operates better and produces more powerful results compared to Artificial Neural Networks with an accuracy of 80.05%.

Keywords: Deep reinforcement learning, Blockchain, Machine learning, Smart home, Smart applications.

INTRODUCTION

Over the last few years, data has emerged as a crucial resource of expertise and, *via* smart applications, it has opened up novel avenues for solving issues in real-world industries including finance, bioinformatics, farming, and wireless communications [1, 2]. People can accomplish the intended activity more quickly due to these data-driven applications that integrate relevant information into user expertise [3]. It makes information functional, enhances client communications, personalizes the client's expertise, boosts functional effectiveness, and opens up novel commercial opportunities [4]. A person's life can be made simple by a variety of smart applications, like smart houses, hospitals, cities, *etc*. With the ability to control smart houses and improve human lifestyles, contemporary society is thought to include smart innovations. The gadgets, namely smart devices, can be linked to share data with other gadgets in the house through an Internet of Things (IoT)-based framework [5]. From five hundred million smart house to 700 million gadgets in 2018–2022, the mean annual expansion of smart houses and their technology was over 30 percent [6].

The vast volume of data produced by these apps presents challenges for keeping databases, as well as safety concerns with its communication. A distributed database system called blockchain can be utilized to address these problems [7]. Blockchain, which has a dispersed database system, has been employed to address these problems. It was created in 2008 by Satoshi Nakamoto and comprised a collection of networked devices that work together as a time-stamped, tamper-proof ledger [8]. It is made up of a series of blocks joined by basics in cryptography. The 3 pillars of blockchain are immutability, decentralization, and openness. These three features made it possible for a broad spectrum of uses, such as the presence of electronic currency (currency that doesn't exist physically) and analyses of its appropriateness for smart applications [9]. Even though blockchain guarantees confidentiality and safety, different weaknesses also began surfacing once it was implemented.

Since conventional techniques rely on signatures to identify trends, a strong Intrusion Detection System (IDS) is necessary to address the previously stated problem. However, one of the newer technologies known as machine learning (ML) can be utilized to analyze data traffic and find breach and attack trends [10]. Therefore, creating successful and rapid methods to examine this enormous volume of data is essential for managing blockchain-based smart applications [11]. As a result, ML is widely used in modern society and is used on twelve occasions a day without the user even realizing it. ML allows machines to process information, operate, and research without human oversight [12]. Deep Reinforcement Learning (DRL) is a new technology that may be applied to interruption areas and assault trends in the stream of data assessment [13]. Depending on several uses, like data exchange in the smart house, this paper shows the integration of blockchain and DRL in smart houses.

LITERATURE REVIEW

To safeguard the smart house against threads, a study introduced a blockchain-based safe system that makes use of IoT detection devices [14]. This system's execution demonstrates safe communication amongst the Internet of Things gadgets in a dispersed setting.

The incorporation of blockchain technology and IoT with a smart area concept is presented [15], providing clients with a connection to the electricity grid. The created technology establishes a link between the client and the blockchain within the electricity grid network. The one who accesses the solar panel setup may entertain the system and purchase and trade the power through blockchain.

The application of smart house technologies in household settings is expanding as a result of recent advancements. With the use of gadgets and management systems, it is possible to effortlessly regulate the living space [16].

The smart house connection was introduced [17] using safety flaws. Because of a lack of client data, employing an ISP to manage gadgets and verify certificates is feasible but insufficient for safety.

Blockchain technology and ML were integrated into the smart grid's renewable power supply, as demonstrated in a study [18]. Hyperledger Calliper is the applicable blockchain system, which is chosen depending on speed, delay, and resource utilization. The power crowdsourced structure can benefit from this approach.

SUBJECT INDEX

S

T

U

V

W

Keshav Kaushik

Keshav Kaushik is an Associate Professor at the Center for Cyber Security and Cryptology, Sharda School of Computer Science & Engineering, Sharda University, Greater Noida, India. A leading expert in cybersecurity, AI-driven security systems, and digital forensics, he has authored over 200 publications, including SCI/SCIE and Scopus-indexed articles, and holds 15 patents. Recognized among the World's Top 2% Scientists by Stanford University and Elsevier (2024), he is a Guest Editor for the IEEE Journal of Biomedical and Health Informatics and serves as Associate Editor for journals including Scientific Reports (Springer Nature), Journal of Cybersecurity and Privacy (MDPI), and several others. He is a Senior Member of IEEE, Vice Chairperson of the ACM Meerut Chapter, and an active contributor to national cybersecurity training initiatives. His work bridges academic rigor, technological innovation, and policy relevance in the global cybersecurity landscape.

Rewa Sharma

Rewa Sharma is a dedicated academician and researcher with over 15 years of experience in teaching and research in the field of Computer Science and Engineering. She holds a Ph.D and M.Tech in Computer Science from Banasthali University and currently serves as an Assistant Professor at J.C. Bose University of Science and Technology, YMCA, Faridabad. Her areas of expertise include Wireless Networks, Internet of Things (IoT), Blockchain, and Machine Learning. She has contributed significantly to academia through numerous publications in reputed UGC, Scopus, and SCIE-indexed journals and conferences. Her expertise blends deep technical knowledge with strong academic leadership and mentoring skills.

Ayodeji Olalekan Salau

Ayodeji Olalekan Salau is a Professor in the Department of Electrical/Electronics and Computer Engineering at Afe Babalola University, Nigeria. He holds a B.Eng. from the Federal University of Technology, Minna, and M.Sc. and Ph.D. degrees from Obafemi Awolowo University, Ile-Ife. A registered professional engineer with COREN and a member of IEEE and IAENG, he has authored three academic books and over 320 research articles across leading international journals, conferences, and book series. His research focuses on computer vision, image and signal processing, artificial intelligence, and power systems engineering.

Dr. Salau has received numerous distinctions, including the Best Paper Award in Cogent Engineering (2019), the International Best Researcher Award (IISTAC, 2022), and recognition as one of the World's Top 2% Scientists in Artificial Intelligence by Elsevier/Stanford University. In 2025, he was named 2nd Best AI Researcher in Higher Education in Nigeria by NAAIP/NUC/TETFund and received the Best Researcher Award at the International UILA Awards during ICDAM-2025, London.