IoT DATA PRIVACY AND SECURITY BASED ON BLOCKCHAIN TECHNOLOGY

2024
MASTER THESIS
COMPUTER ENGINEERING

Mohammed Talib RAHEEM

Thesis Advisor
Assist. Prof. Dr. İsa AVCI

IoT DATA PRIVACY AND SECURITY BASED ON BLOCKCHAIN TECHNOLOGY

Mohammed Talib RAHEEM

Thesis Advisor

Assist. Prof. Dr. İsa AVCI

T.C.

Karabuk University

Institute of Graduate Programs

Department of Computer Engineering

Prepared as

Master Thesis

KARABUK

February 2024

I certify that in my opinion the thesis submitted by Mohammed Talib RAHEEM titled "IoT DATA PRIVACY AND SECURITY BASED ON BLOCKCHAIN TECHNOLOGY" is fully adequate in scope and quality as a thesis for the degree of Master of Science.

Assist. Prof. Dr. İsa AVCI .....

Thesis Advisor, Department of Computer Engineering

This thesis is accepted by the examining committee with a unanimous vote in the Department of Computer Engineering as a Master of Science thesis February 5, 2024.

Examining Committee Members (Institutions)	Signature
Chairman : Assist. Prof. Dr. Nehad T.A. RAMAHA (KBU)	.....
Member : Assist. Prof. Dr. İsa AVCI (KBU)	.....
Member : Assist. Prof. Dr. Ali HAMİTOĞLU (İSÜ)	.....

The degree of Master of Science by the thesis submitted is approved by the Administrative Board of the Institute of Graduate Programs, Karabuk University.

Assoc. Prof. Dr. Zeynep ÖZCAN .....

Director of the Institute of Graduate Programs

"I declare that all the information within this thesis has been gathered and presented in accordance with academic regulations and ethical principles and I have according to the requirements of these regulations and principles cited all those which do not originate in this work as well."

Mohammed Talib RAHEEM

ABSTRACT

M. Sc. Thesis

IoT DATA PRIVACY AND SECURITY BASED ON BLOCKCHAIN TECHNOLOGY

Mohammed Talib RAHEEM

Karabuk University
Institute of Graduate Programs
The Department of Computer Engineering

Thesis Advisor:
Assist. Prof. Dr. İsa AVCI
February 2024, 55 pages

The integration of Deep Extreme Learning Machine (D.E.L.M.) and blockchain innovation speaks to a worldview move in tending to security and protection challenges inside the Internet of Things (IoT), especially in smart framework situations. This study, about proposes a blockchain-based smart framework that D.E.L.M. moves forward to reinforce security, maximize vitality proficiency, and offer individualized client encounters. The decentralized characteristic of blockchain guarantees data capacity that's safe to alter, thus diminishing the vulnerabilities connected to centralized confirmation frameworks. Factual measurements evaluate the system's execution amid the preparation and approval stages. The framework performs well, with few wrong expectations and tall exactness. This contributes to progressing the understanding of blockchain and D.E.L.M. synergies within the setting of keen frameworks, advertising an establishment for encouraging investigation and advancement inside IoT environments. As smart frameworks become progressively

predominant, the proposed framework lays the basis for a more secure, versatile, and privacy-conscious IoT scene.

Key Words : Internet of Things (IoT), Blockchain, Deep Extreme Learning Machine, Data Security, Data Protection, Decentralization.

Science Code : 92403

ÖZET

Yüksek Lisans Tezi

BLOK ZİNCİR TEKNOLOJİSİ TABANLI NESNELERİN İNTERNETİNDE VERİ GİZLİLİĞİ VE GÜVENLİĞİ

Mohammed Talib RAHEEM

Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı:
Dr. Öğr. Üyesi İsa AVCI
Şubat 2024, 55 sayfa

Derin Aşırı Öğrenme Makinesi (D.E.L.M.) ve blok zinciri teknolojisinin entegrasyonu, Nesnelerin İnterneti (IoT) içinde, özellikle de akıllı çerçeve durumlarında güvenlik ve koruma zorluklarına yönelmede bir bakış açısı geliştirilmesine fayda sağlamaktadır. Bu çalışma, D.E.L.M.'in güvenliği güçlendirmek, farkındalık seviyesini en üst düzeye çıkarmak ve bireyselleştirilmiş müşteri taleplerini karşılamak için ileriye taşıdığı blok zinciri tabanlı bir akıllı çerçeve önermektedir. Blok zincirinin merkezi olmayan özelliği, değiştirilmesi güvenli olan veri kapasitesini garanti etmektedir. Böylece merkezi onay çerçevelerine bağlı güvenlik açıklarını azaltılması sağlar. Gerçeklere dayalı ölçümler, hazırlık ve onay aşamaları sırasında sistemin çalışmasını denetler. Bu çerçeve, minimum sayıda hata ve yüksek doğruluk ile iyi performans gösterilmesini sağlar. Bu çalışma, IoT ortamlarında araştırma ve geliştirmeyi teşvik ederek daha doğru ve güvenli çerçeveler ortamında blok zinciri ve D.E.L.M. birlikte çalışmasına katkıda bulunur. Bu çerçeveler

giderek daha çok kullanılmaya başlandıkça, önerilen çerçeve daha güvenli, çok yönlü ve gizlilik bilincine sahip bir IoT sahnesinin temelini oluşmasına imkan sağlayacaktır.

Anahtar Kelimeler: Nesnelerin İnterneti (IoT), Blokzincir Teknolojisi, Veri Güvenlik, Veri Koruma, Merkezi Olmayan Yapı.

Bilim Kodu : 92403

ACKNOWLEDGMENT

First and foremost, I wish to express my heartfelt gratitude to Allah Almighty for his divine guidance and blessings throughout my educational journey. Additionally, I extend my thanks to Karbuk University for affording me this opportunity to undertake my graduate studies. A special acknowledgment goes to my supervisor, Assist. Prof. Dr. İsa AVCI, and the dedicated professionals at this renowned institution. I sincerely appreciate my husband, a steadfast pillar of support whose consistent encouragement and faith have been instrumental in my academic pursuits.

Lastly, I wish to convey my thanks and my enduring love for Turkey and my homeland, Iraq.

CONTENTS

Page

Page

LIST OF FIGURES

Page

Page

LIST OF TABLES

Page

ABBREVIATIONS

IoT : Internet of Things

COP : Connection-Oriented Protocol

DELM : Deep Extreme Learning Machine

POW : Prof of Work

Dapp : Decentralized Application

PART 1

INTRODUCTION

In today's period ruled by the Internet of Things (IoT), the mechanical scene has experienced noteworthy changes, affecting different logical and innovative areas [1]. The IoT acts as a catalyst for consistent communication and collaboration between machines, making an interconnected organizing of gadgets that creates a Connection-Oriented Protocol (COP) [2]. Remote sensor arrangements and gadgets shape the establishment of this network, empowering viable communication, data sharing, and complex examination. The Internet of Things may be a combination of numerous innovations counting computation, analytics, sensors, actuators, communication, and data [3]. As the IoT extends, overseeing gadget integration, arranging networks, and disseminating the nature of IoT parts gets progressively troublesome [4]. The need for central servers for verification is expanding. However, the unwavering quality and security of these servers are being addressed, taking off the IoT environment powerless to security and information security dangers. Working in the IoT environment is complicated by the expansion of associated gadgets, false confirmation, gadget spoofing, and uncertain information transmission [5]. In today's time ruled by the IoT, the innovative scene has experienced noteworthy changes, affecting different logical and mechanical areas [1]. The IoT acts as a catalyst for consistent communication and collaboration between machines, making an interconnected array of gadgets that create a COP [2]. Remote sensors organize gadgets and frame the establishment of this network, empowering viable communication, data sharing, and complex examination. The IoT could be a combination of different innovations counting computation, analytics, sensors, actuators, communication, and data [3]. Overseeing gadget integration, arranging linkages, and the scattered nature of IoT pieces become more troublesome as the IoT grows [4]. The require for central servers for verification develops; however, these servers' steadfastness and security are addressed, clearing out the Internet of Things biological system powerless to dangers to security and information security. Exploring the IoT biological system is made more troublesome

by the multiplication of organized gadgets, false authentications, gadget spoofing, and unsecured information transmission [5].

The way we lock in with the advanced world has changed significantly as a result of the IoT quick extension, introduced in a time of unparalleled association. Advanced innovation must be coordinated in this ever-changing environment to handle the developing security and adjustment issues. The integration of blockchain innovation with Deep Extreme Learning Machine (D.E.L.M.) in the IoT design is one such imaginative union, particularly when it comes to shrewd frameworks. The presentation acts as a beginning point for an intensive investigation of how the combination of D.E.L.M. and blockchain innovation might alter the essential nature of IoT environments. It gives peruses a street outline for exploring these technologies' complexities, expecting their progressive impacts, and increasing in value their multifaceted impact on the security, adaptability, and user-centered components of shrewd frameworks.

1.1. MOTIVATION

The reason for this inquiry is to start an imaginative worldview move within the field of support methodologies, moving from conventional centralized models to decentralized approaches. The proposed strategy leverages dispersed ledger-based innovations, with specific accentuation on the blockchain, to address the squeezing security and security challenges of the IoT [6]. The inspiration for this alteration stems from the inborn vulnerabilities in centralized information administration frameworks, which pose critical dangers to data security and protection within the complex interconnected environment of the IoT [7]. Centralized information administration frameworks have been recognized as a source of vulnerabilities that uncover basic vulnerabilities within the security and protection of IoT biological systems. The proposed arrangement advocates the appropriation of a decentralized structure empowered by blockchain technology. Expressly, the exciting properties of blockchain are accepted to assist in disseminating belief among organized members, dispensing with the requirement for a central specialist to supervise the verification preparation [8]. Decentralized approaches based on blockchain offer other ways to

diminish the dangers related to centralized upkeep. The proposed worldview points to moving forward the security and security of IoT situations by conveying belief and confirmation instruments over the arrange. The takeoff from conventional strategies reflects a commitment to the assembly of the advancing challenges postured by the multiplication of connected devices. In outline, this ponder contends for a noteworthy worldview move in upkeep techniques in favor of a decentralized approach upheld by blockchain innovation. The proposed system addresses the inadequacies of centralized frameworks, particularly in terms of security and privacy in IoT. This work aligns with our broader objective of adjusting to the energetic scene of associated advances and building a more versatile and secure establishment for the IoT.

1.2. PROBLEMS OF STATEMENTS

This examination centers on the complex intuition between the IoT and fabricating. It addresses critical issues such as colossal information administration, data framework disturbance, and the expanding complexity of worldwide mechanical systems. We are working on it [9]. This article recognizes the inborn security dangers related to the coordination of blockchain innovation into his IoT arrangement and highlights critical vulnerabilities and related challenges confronted by data framework planners [10]. This paper centers on keeping up information security, judgment, privacy, and security and portrays the complexities emerging from the advanced change of mechanical commerce forms [11]. This thinks about and covers an extent of challenges confronted by the interface between the IoT and the fabricating division, from overseeing expansive datasets to the disturbance of data frameworks and the expanding complexity of worldwide mechanical systems [9]. The talk centered on recognizing the security dangers related to the integration of blockchain innovation into IoT systems, with specific emphasis on revealing basic security vulnerabilities and the challenges confronted by data framework designers [10]. The most significant concern is the assurance of information, including security, astuteness, secrecy, and protection, and the article depicts the complex challenges emerging from the progressing computerized change of mechanical forms [11]. In rundown, this comprehensive investigation addresses different challenges at the crossing point of IoT and fabricating. It addresses issues such as huge information administration, data

framework disturbance, and advancing complexity inside worldwide mechanical systems [9]. The integration of blockchain innovation is being considered with a solid mindfulness of security dangers, highlighting the troublesome challenges confronted by data framework modelers [10]. This paper reliably emphasizes the need to ensure information security, keenness, secrecy, and security within the transformative setting of computerized mechanical forms [11].

1.3. AIM OF STUDY

The objective of this investigation is to use blockchain innovation to supply a decentralized arrangement to address the security and security challenges related to the IoT. This examination centers on the mechanical division and highlights potential information debasement and security concerns in complex IoT systems. This considers points to look at how blockchain's decentralized approach can make strides in information administration, data processing, and the, in general, secure design of IoT within the setting of cutting-edge fabricating. The central center of this investigation is to use the capabilities of blockchain innovation to propose a decentralized arrangement to address the security and protection challenges of the IoT.

This considers centers, particularly on the mechanical division, and addresses conceivable information annihilation and security issues inside the complex structure of the IoT. This ponders points to investigate how blockchain-specific decentralized procedures can contribute to improving data administration, data handling, and then, in general, secure systems of IoT within the setting of cutting-edge fabricating operations.

1.4. OUTLINE OF THESIS

The structure of this work is orderly, beginning with a diagram of the IoT scene and highlighting its transformative effect in different areas. The, by and large, targets of the investigation are defined at that point, with a primary thought of the impediments inborn in centralized approaches to securing the Internet of Things. The article, at that

point, addresses the complexities that producers confront when joining IoT advances, highlighting the need for solid information administration. The examination will advance and grow into the region of security challenges related to the integration of blockchain innovation into the IoT framework. At last, this ponder investigates the cooperative energy between blockchain innovation and cryptography to imagine a vigorous defense component against protection concerns inside mechanical systems. This conclusion highlights the requirement for a comprehensive protection security system that incorporates agreement calculations, get-to-control strategies, and cryptography. This work is created by giving a comprehensive outline of the IoT environment and outlining its far-reaching changes over diverse segments.

To begin with, this portion sets the organization for a comprehensive examination of the inquiry about destinations, characterized by an essential evaluation of the inadequacies inborn in centralized strategies for securing the Internet of Things. The story, at that point, moves to the challenges confronted by fabricating IoT execution, with a specific center on the basics of viable information administration. This section serves as a premise for a more profound understanding of the security angles that emerge from coordination blockchain innovation into the structure of his IoT foundation. Exploring the security concerns related to the meeting of blockchain and IoT will be a crucial point of our work. The ensuing inquiry will address the advantageous relationship between blockchain innovation and cryptography, envisioning synergistic unions that will fortify protections against security concerns inside broader mechanical working systems.

In summary, this paper highlights the requirement for a comprehensive system committed to ensuring protection in IoT situations. This incorporates not as it was joining blockchain and cryptography, but moreover, consolidating agreement calculations and getting to control strategies. The conclusion highlights the requirement for a multi-layered approach and recognizes the complex transaction of different components to construct strong security against information assurance dangers in mechanical systems. This nuanced and organized consideration contributes to the broader talk on securing IoT situations and gives experiences and proposals for a comprehensive protection assurance system.

PART 2

LITERATURE REVIEW

Investigate joining blockchain into IoT frameworks is characterized by scholarly endeavors aimed at accomplishing differing objectives and the advancement of inventive methodologies to address advancing challenges. It takes put in an energetic and advancing setting. Later, I inquired about securing an assortment of points, counting security dangers related to the utilization of rambles and Unmanned Ethereal Vehicles (UAVs), setting up secure communications systems for the IoT, and moving forward with information assurance. Framework judgment and responsibility by coordinating blockchain innovation into IoT environments. This written audit gives a comprehensive diagram of these modern commitments. It gives insight into the bits of knowledge, applications, and arrangements rising at the crossing point of blockchain and the IoT.

In later inquiries about endeavors, spoken to by the considers [12] and [13], researchers have put forward imaginative propositions for joining blockchain into supply chain administration frameworks, particularly within the setting of fabricating. The center of these recommendations is to make strides in reliability, security, and straightforwardness within the supply chain. One striking proposal that arose from this exertion was the backing of utilizing blockchain innovation to decentralize IoT frameworks, which could be an effective technique to address security issues. These security challenges are efficiently categorized into four layers: recognition layer, arrange layer, preparing layer, and application layer. Joining blockchain into supply chain administration frameworks is picking up consideration as a compelling implies of upgrading belief, security, and straightforwardness, particularly in energetic fabricating situations [12,13]. This nuanced approach reflects a profound understanding of the complexity of security concerns within the IoT biological system. It highlights the requirement for targeted arrangements at different levels of framework

engineering. The complete report highlights the progressive potential of blockchain within the field of IoT applications. We position blockchain as an imaginative innovation that can give decentralized and secure information trade administrations and robust solutions to complex security challenges in IoT frameworks. Of specific note is that this innovation can address information assurance issues and address the developing sensitivities encompassing information security within the fabricating segment. This survey diagrams how blockchain presents straightforwardness and responsibility while adjusting to administrative commitments concerning security in IoT-based fabricating data frameworks. Al-Turjman et al. [14] distinguish security and protection issues in shrewd city applications, emphasizing the requirement for future investigation. Karati and Biswas [15] propose a cryptographic convention for information secrecy and genuineness challenges in IoT-based swarm discernment, joining identity-based encryption for anonymity. Blockchain, renowned for securing Bitcoin, is utilized for improved IoT security and security [16, 17], utilizing Prof of Work (PoW) agreements and cryptographic methods. Axon [18] presents a privacy-conscious blockchain PKI to address security escape clauses in ordinary PKI plans. Hardjono and Pentland [19] propose ChainAnchor, a permissioned blockchain framework utilizing zero-knowledge proofs for personality and control. Shen et al. [20] display a security SVM preparing a scheme for encrypted IoT data utilizing blockchain and homomorphic encryption. Container et al. [21] present EdgeChain, an edge IoT system based on blockchain and shrewd contracts that connects cloud assets with IoT gadgets. Hong et al. [22] propose a narrow-band IoT engineering based on blockchain for information character confirmation, investigating intermediary re-encryption as a privacy-enhancing component. Su et al. [23] propose a PAUG plot for cloud ciphertext data upgrade authorization. Koe and Lin [24] display an offline intermediary re-encryption conspire for client personality and category protection. Pise and Uke [25] propose an intermediary re-encryption strategy for secure information sharing on enormous information stages. Baboolal et al. [26] utilize intermediary reencryption to secure ramble video protection. Hong and Sun [27] present an ABPRE conspire for IoT, combining attribute-based encryption and key cover. The integration of proxy encryption into ring signature plans is proposed as an improvement, combining the qualities of both instruments and applying blockchain innovation for enhanced privacy assurance in IoT [28]. The multifaceted commitments of blockchain

innovation to IoT grandstand its potential in tending to security, protection, and responsibility concerns. Blockchain is developing as a key enabler as scholastics in this field keep coming up with unused thoughts. It provides decentralized solutions to improve frameworks, communication, and information astuteness over a range of IoT applications. The inquiry included in this outline of the writing extends from ensuring nourishment supply chains and keen frameworks to advertising solid communication systems for IoST. All of them assist our information on and utilization of blockchain within the quickly changing field of IoT innovation. It is envisaged that more inquiries about and improvements will progress on current approaches, address unused issues, and open up unused roads for the smooth integration of blockchain innovation in the interior IoT biological systems [29–50].

Table 2.1. Comparative work with Previous work.

Study	Focus Area	Blockchain Application	Security Measures	Privacy Solutions
[12]	Manufacturing, Supply Chain Management	Integration for transparency, security, reliability	Decentralization to address security challenges	Privacy concerns addressed through blockchain integration
[13]	Manufacturing, Supply Chain Management	Integration for transparency, security, reliability	Decentralization to address security challenges	Privacy concerns addressed through blockchain integration
[14] ([9])	Smart City Applications	Identifying security and privacy issues	N/A	N/A
[15] ([10])	IoT-based Crowd Perception	Cryptographic protocol for data confidentiality, authenticity	Identity-based encryption for anonymity	N/A
[16] ([11], [12])	General IoT Security	Leveraging blockchain for enhanced IoT security and privacy	Proof of Work (PoW) consensus, cryptographic methods	N/A
[17] ([13])	General IoT Security	Leveraging blockchain for enhanced IoT security and privacy	Proof of Work (PoW) consensus, cryptographic methods	N/A
[18] ([14])	Privacy-conscious Blockchain PKI	Addressing security loopholes in conventional PKI designs	N/A	N/A
[19] ([15])	ChainAnchor - Permissioned Blockchain System	Using zero-knowledge proofs for identity and access control	N/A	N/A
[20] ([16])	Privacy Protection SVM Training Scheme	Using blockchain and homomorphic encryption for IoT data	N/A	Privacy protection through encrypted IoT data
[21] ([17])	EdgeChain - Edge IoT Framework	Based on blockchain and smart contracts, linking cloud resources with IoT devices	N/A	N/A
[22] ([18])	Narrow-Band IoT Architecture	Based on blockchain for data identity verification	Proxy re-encryption for privacy enhancement	N/A

[23] ([19])	PAUG Scheme for Cloud Ciphertext Data Update Authorization	Proposal for secure cloud data update authorization	N/A	N/A
[24] ([20])	Offline Proxy Reencryption Scheme	Protecting user identity and category privacy in big data platforms	Offline proxy encryption for privacy protection	N/A
[25] ([21])	Proxy Reencryption for Secure Data Sharing on Big Data Platforms	Proposal for secure data sharing on big data platforms	Proxy encryption for secure data sharing	N/A
[26] ([22])	Proxy Reencryption for Drone Video Privacy	Protecting drone video privacy through proxy encryption	Proxy re-encryption for privacy protection	N/A
[27] ([23])	ABPRE Scheme for IoT	Combining attribute-based encryption and key insulation	N/A	N/A
[28] ([24])	Integration of Proxy Reencryption into Ring Signature Schemes	Enhanced privacy protection using both mechanisms and blockchain	N/A	N/A

Blockchain, with its unique structure and usefulness, is based on several principal concepts that frame its hypothetical establishment. Blockchain innovation was initially conceived as the primary system for cryptocurrencies such as Bitcoin, but it has advanced into a flexible apparatus with applications in an assortment of financial segments. This ponder addresses the hypothetical establishments of blockchain, covering its essential components, cryptographic basics, agreement handle, and the fundamental decentralization that characterizes its quintessence, as portrayed in reference [51].

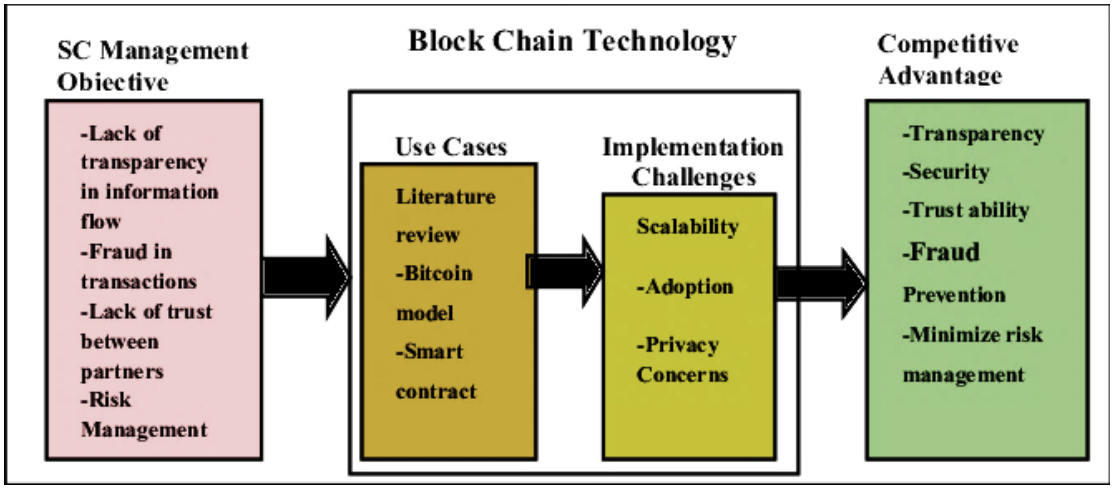

Figure 2.1. Blockchain with structure and usefulness.

At the center of blockchain's hypothetical establishment are crucial components that lay the establishment for its unique structure and operational flow. Initially planned to bolster computerized monetary standards, especially Bitcoin, blockchain has advanced past its unique reason into a flexible innovation that can be connected to an assortment of financial segments.

2.1. DECENTRALIZATION AND DISTRIBUTED LEDGER TECHNOLOGY

At the heart of blockchain innovation is the basic guideline of decentralization as a transformative drive that reshapes conventional ideal models tied down in centralized frameworks. Like conventional approaches where a single specialist controls information and exchanges, blockchain works on a decentralized arrangement of hubs, as laid out in reference [52]. This move absent from centralization makes a worldview move, encouraging decentralized engineering where each taking part hub maintains a comprehensive duplicate of the whole blockchain. This plan speaks to a critical flight from the vulnerabilities related to single focuses of disappointment, subsequently essentially expanding the versatility, straightforwardness, and security of blockchain innovation. The concept of decentralization is profoundly established within the thought of a conveyed record, which is the establishment behind the imaginative design of blockchain frameworks. Not at all like conventional databases that are constrained to a single area, information in a blockchain is methodically conveyed over all hubs partaking within the organization. This disseminated record is critical since it

prevents people or organizations from singularly controlling or changing information. Instep, all changes to the record must go through an agreement handle, as point by point in reference [53]. This dispersed record component is not secured against unauthorized control as it was secured but, moreover, presents a level of straightforwardness and responsibility unmatched by centralized systems. Blockchain's decentralized engineering combined with a conveyed record makes a versatile biological system with no single point of disappointment. Each hub within the organization autonomously keeps up a total record of the blockchain, giving excess and lessening the chance of information misfortune or breach. The agreement handle required for all changes to the standard record guarantees a collective decision-making approach where no single company can singularly manage changes. This participatory administration show is consistent with the standards of inclusion and straightforwardness and lays the foundation for a more fair and law-based advanced environment.

2.2. CRYPTOGRAPHIC FOUNDATIONS

Blockchain essentially employs cryptographic strategies to secure exchanges and protect information astuteness. Hashing may be a fundamental cryptographic device that's utilized. A chain of pieces associated with cryptographic hashes is made on the blockchain by each square, which incorporates a hash of the one sometime recently. This association ensures that adjusting one block would require altering all taking after squares, a computationally illogical endeavor [54].

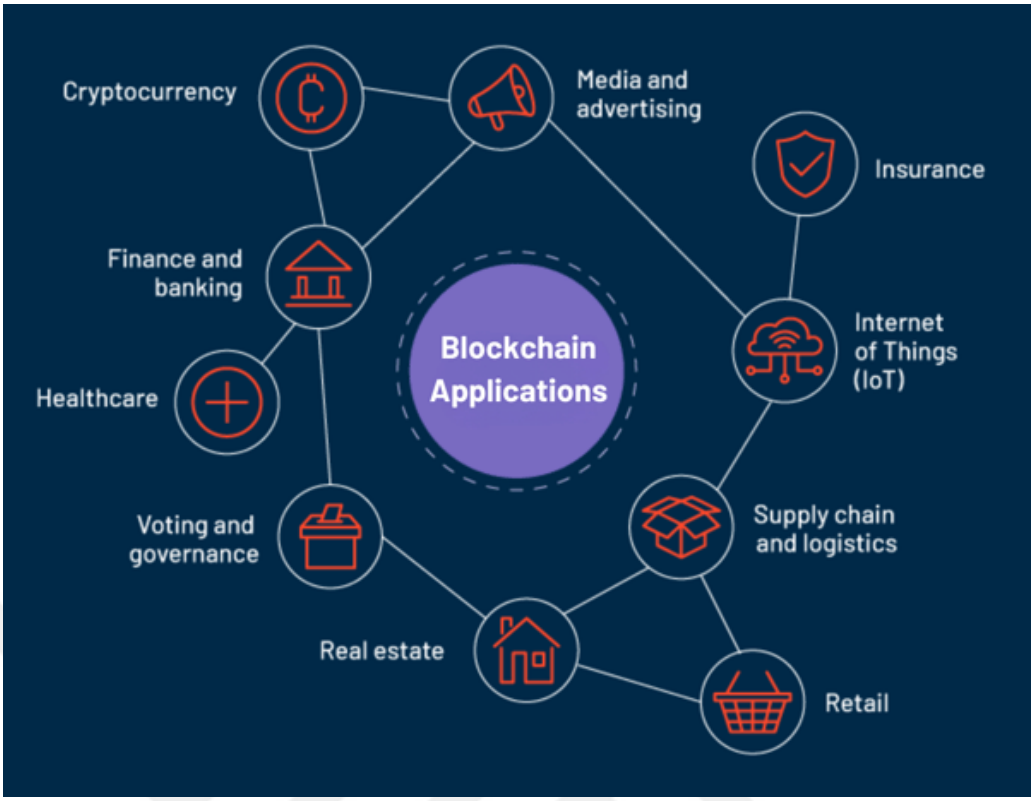

Figure 2.2. Applications of Blockchain.

Blockchain security, moreover, rests on public-key cryptography. An open key and a private key are the two cryptographic keys that each part of a blockchain organization has. Whereas the private key, which is as it was known to the proprietor, empowers decoding and the creation of advanced marks, the open key acts as an address to which other individuals may send scrambled communications. The security of blockchain exchanges is based on this hilter kilter cryptographic strategy [55].

2.3. CONSENSUS MECHANISMS

Blockchain systems utilize agreement methods to keep the ledger's state steady and concurred upon overall hubs. The strategies by which hubs concur on the authenticity of exchanges and the reference section of unused pieces to the chain are built up by these strategies [56]. One well-known agreement strategy utilized by Bitcoin is called Proof of Work (PoW). PoW requires clients, referred to as diggers, to unravel challenging numerical issues to favor exchanges and add unused pieces to the blockchain. Elective agreement strategies such as Confirmation of Stake (PoS),

Designated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) are being explored due to the energy-intensive nature of PoW. Whereas tending to issues with decentralization, adaptability, and vitality utilization, these approaches look to reach an agreement [57–60].

2.4. SMART CONTRACTS AND TURING COMPLETENESS

With the coming of savvy contracts, blockchain innovation goes past fundamental value-based capacities. Self-executing contracts, or shrewd contracts, have the conditions of the contract expressly encoded into the code. When specific prerequisites are fulfilled, they consequently execute and implement the foreordained controls [61]. The operation of keen contracts depends on the hypothetical thought of Turing completeness. If a framework or programming dialect can imitate a Turing machine—a speculative computing device that can illuminate each issue that can be communicated algorithmically—it is said to be a Turing total [62]. Turing total blockchain frameworks that give shrewd contract arrangements empower the improvement of A decentralized application (DApp) [63].

2.5. IMMUTABILITY AND AUDITABILITY

A key hypothetical component that ensures that once a square is included in the chain, its substance does not alter is the unchanging nature of blockchain information—the cryptographic associations between pieces and the agreement forms that control their inclusion permit this. The permanence of information on the blockchain increases its constancy by anticipating unlawful changes or altering [64]. Various divisions are affected by this permanence, as well as the straightforward and auditable character of blockchain exchanges. For case, in supply chain administration, the unmistakable and unchangeable record makes it less demanding to track the root and way of things. The capacity of inspectors, controllers, and clients to affirm the authenticity of exchanges advances belief in blockchain-based frameworks [65–70].

2.6. CHALLENGES AND FUTURE DIRECTIONS

Although blockchain innovation is promising, it faces numerous challenges that highlight the energetic nature of its advancement. As sketched out in reference [71], issues such as versatility, vitality utilization, interoperability, and administrative concerns still exist, and overcoming these impediments will require proceeding inquiries about advancement. Despite these challenges, the strength of blockchain has been illustrated by the endeavors of scholars and industry specialists to address and overcome these impediments, subsequently encouraging its application in different areas. At the same time, the hypothetical establishments of blockchain are experiencing unobtrusive changes, as clarified in reference [73]. On a fundamental level, the hypothetical establishments of blockchain incorporate permanence, unquestionable status, dispersed record innovation, decentralization, and different layers such as cryptographic framework, agreement forms, and shrewd contracts. Taken together, these essential components deliver uncommon qualities in blockchain, situating it as an imaginative innovation with broad application [74]. The steady interest in progress in these hypothetical establishments reflects a commitment to reinforcing the impact of blockchain within the advancement of decentralized and secure advanced exchanges, as reflected in reference [75]. Proceeded collaboration between viable arrangements and hypothetical systems will not, as it were, guarantee the strength of blockchain. However, moreover, its part is a transformative constraint that will proceed to shape the end of the scene of advanced exchanges and decentralized frameworks. Make it more grounded. As long as investigation and advancement endeavors proceed to extend and refine these hypothetical establishments, blockchain is balanced to have an enduring and critical effect on the innovative, financial, and social scene.

PART 3

MATERIALS AND METHODS

An inquisitive zone of investigating interior the ever-evolving field of speedy framework advances is the combination of blockchain advancement with Deep Extreme Learning Machine D.E.L.M [56]. The sharp framework environment can be interior and outbalanced by this synergistic joining, particularly when it comes to managing essential issues with security, security, and adaptability. As keen advances become more commonplace, it is more essential than ever to have solid security measures in place to secure unsteady information and regard client affirmation. Blockchain improvement, which is well known for being decentralized and unchangeable, gives a creative and energizing reply to these issues. Show-day innovative breakthroughs are, in common sense, subordinate to sharp frameworks, which can increase from advanced fake encounters programs to the Internet of Things IoT contraptions [76]. The colossal volumes of unsteady information these frameworks oversee have started to stress generally the security and security comes around of their wide choice. It is essential to explore cutting-edge courses of activity since schedule security measures intermittently drop level to offer up to affirmation against enthusiastic dangers. The amplification of fake encounters is extended by the advanced critical learning grouping known as the Noteworthy Exceptional Learning Machine. It might be a compelling instrument for speedy frameworks because of its capacity to analyze colossal volumes of information and recognize complex plans.

In advancement to developing the system's flexibility, this decentralization makes past any address that a single point of compromise does not result in a shocking breach. Since each center interior of the blockchain organization consolidates a copy duplicate of the whole record, repetition is made, which moves forward the blame resistance and steadiness of the framework. Also, blockchain's steady nature updates data judgment inside and out in sharp frameworks. Data posted to the blockchain is roughly

troublesome to clear or alter after it is there. This steady nature consolidates advances in a high degree of acknowledgment and understanding of the fast framework by ensuring a change and secure record of exchanges and information. Blockchain's lastingness gives a fundamental defense against information control in circumstances where data veracity is fundamental, compared to healthcare or back businesses. The straightforwardness intrinsic in blockchain exchanges presents a progressed level of obligation and acknowledgment in keen systems.

All organized clients may see each exchange that's enrolled on the blockchain, making the movement way open and auditable. This openness disheartens contradicting movements in expansion to making information taking after less asking. Understanding the source and history of information is vital in speedy frameworks since it is foremost for several contraptions and frameworks to communicate dependably. Since blockchain progression is obvious, assistants can effectively get to information provenance, which progresses to a trusting environment. The cementing of blockchain progression shapes the present for invigorating the security arrangement of sharp frameworks as an entire. Since they are related and subordinate to one another, sharp frameworks require a solid establishment to ensure the affirmation, openness, and insightfulness of their information. By organizing, blockchain takes after these rules, setting up a secure and reliable working environment for clever frameworks. It is pressing to secure the information made by savvy frameworks as they make and wrap up more commonplace. The eager nature of cybersecurity dangers finds that conventional security measures may not be agreeable to fight off progressed ambushes. The joining of blockchain progression offers a comprehensive and long persevering course of activity to the security issues that appear in fast framework settings because of its decentralized organization, clear exchanges, and interminable nature. The integration of blockchain advancement with Deep Extreme Learning Machine D.E.L.M marks an energetic step forward in the field of dexterous frameworks. D.E.L.M includes an extra layer to the blockchain's agreeable vitality, an overhauled alteration of profound learning calculations, particularly interior of the complex and energetic circumstances of dexterous framework situations. Proposition for making strides in the encounters, security, and adaptability of canny frameworks are crucial from this combination. Inquisitively among critical learning calculations, D.E.L.M is

built to be particularly unimaginable at picking up complex plans and changing to changing environments. An inquisitive zone of investigating interior the ever-evolving field of canny framework advances is the combination of blockchain improvement with Deep Extreme Learning Machine D.E.L.M [56]. The quick framework environment can be interior and out-modified by this synergistic joining, particularly when it comes to managing essential issues with security, affirmation, and adaptability. As sharp advances become more commonplace, it is more fundamental than ever to have solid security measures in place to secure precarious information and regard client security.

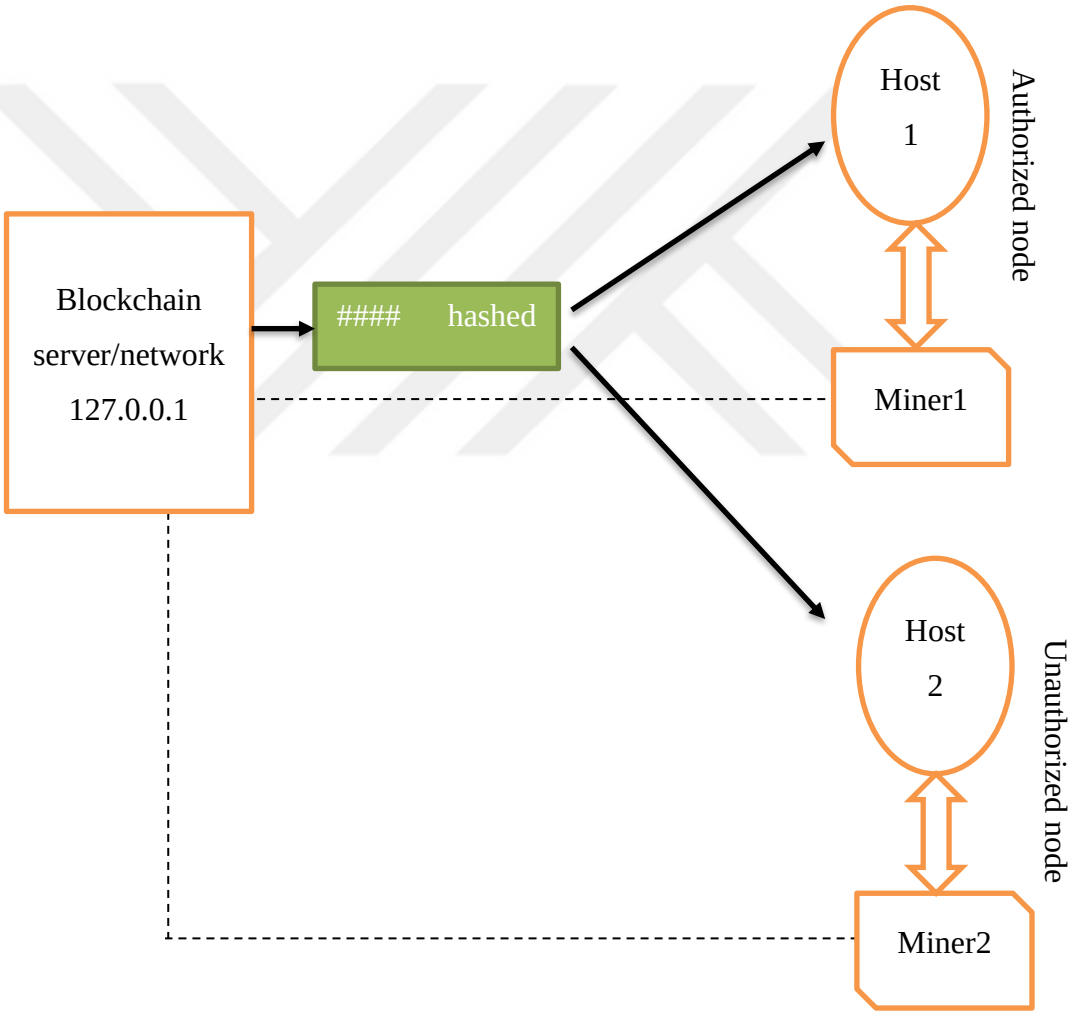

Figure 0.1: Flowchart of our model.

1. To produce data which can be prepared using JSON format;
2. To encode the data using SHA256 algorithm;
3. Developing blockchain e.g. server to broad cast the data.

4. Server to connected with host computer (locally) where this host will receive the data and will decode the data and will the display decoded data.
5. The host node will reply back to the server (blockchain) where the reception of data is over and the blockchain will update this transaction.
6. In order to change the coding (encryption of the data and to send that data again to the host node). In this case host node should not receive (see) the data. Accordingly, miner will update the blockchain back of this null transaction. As shown in Figure 3.1.

Blockchain progression, which is well known for being decentralized and unchangeable, gives an imaginative and energizing reply to these issues. Show-day creative breakthroughs are, in common sense, subordinate to sharp frameworks, which can grow from advanced fake encounter programs to the Internet of Things IoT contraptions [76]. The colossal volumes of unsteady information these systems have directly started to stress generally the security, and security comes approximately of their wide assurance. It is essential to examine cutting-edge courses of activity since scheduled security measures routinely drop levels to offer up to confirmation against excited risks. The run of fake bits of information is intensified by the advanced noteworthy learning grouping known as the Noteworthy Uncommon Learning Machine. It might be a compelling instrument for speedy frameworks because of its capacity to analyze colossal volumes of information and recognize complex plans. In improvement to developing the system's flexibility, this decentralization makes past any address that a single point of compromise does not result in a grievous breach. Since each center interior of the blockchain organization consolidates a copy duplicate of the overall record, emphasis is made, which moves forward the blame resistance and steadfastness of the framework. In addition, blockchain's consistent nature overhauls data judgment in speedy frameworks inside and out. Data posted to the blockchain is roughly troublesome to clear or adjust after it is there.

This steady nature advances a tall degree of acknowledgment interior the discernment of the fast framework by ensuring a modified secure record of exchanges and information. Blockchain's changelessness gives a fundamental defense against information control in circumstances where data veracity is fundamental, a bit just like the healthcare or back businesses. The straightforwardness that is normal in blockchain

exchanges presents a cutting-edge level of commitment and acknowledgment in keen systems. All organized clients may see each exchange that's enrolled on the blockchain, making the movement way open and auditable. This openness disheartens ill-disposed action in improvement to making information taking after less asking. Understanding the source and history of information is basic in canny systems since it is basic for several contraptions and frameworks to communicate steadily. Since blockchain headway is evident, assistants can effectively get to information provenance, which moves a trusting environment.

The union of blockchain advancement shapes the introduction for fortifying the security arrangement of sharp frameworks as a total. Since they are related and subordinate to one another, able frameworks require a solid establishment to ensure the affirmation., openness, and ability of their information. By orchestrating, blockchain takes after these rules, setting up a secure and reliable working environment for clever frameworks. It is critical to secure the information made by able frameworks as they make and wrap up more commonplace.

The enthusiastic nature of cybersecurity risks finds that ordinary security measures may not be palatable to fight off advanced assaults. The joining of blockchain advancement offers a comprehensive and long-lasting course of activity to the security issues that appear in adroit framework settings because of its decentralized orchestrate, clear exchanges, and never-ending nature. The integration of blockchain headway with Deep Extreme Learning Machine D.E.L.M marks a dynamic step forward in the field of adroit systems. D.E.L.M includes an extra layer to the blockchain's pleasant essentialness, an upgraded alteration of significant learning calculations, particularly the interior of the complex and exuberant circumstances of sharp framework situations. Proposals for making strides in the bits of information, security, and flexibility of smart frameworks are basic from this combination. Inquisitively among significant learning calculations, D.E.L.M. is built to be exceptionally great at picking up complex plans and changing to changing environments.

3.1. DEEP EXTREME LEARNING MACHINE

D.E.L.M may well be an adaptable and compelling illustration that can be associated with a wide amplification of spaces and assignments, from backslide to classification, as highlighted in reference [77]. The center of its reasonability lies in its predominant capacity in procedural collapsing rates combined with fast learning capabilities, making it a broadly utilized and sought-after course of action. In its routine outline, exceptional learning machines work as feedforward neural frameworks, passing data through a course of action of layers in one heading, making it easier to remove complex designs and highlights. In any case, the improvement displayed inside the learning arrangement of the proposed system is characterized by an uncommon strategy known as backpropagation. The D.E.L.M has been illustrated to be a lively and adaptable illustration that can be associated with a broad run of spaces and assignments, outlining its capabilities in both backslide and classification assignments and outlining its vigor and adaptability. [77] At the heart of this model's broad selection is its uncommon capacity in procedural convolution speed, which, alongside its fast-learning capabilities, enables capable and fruitful dealing with complex datasets. These highlights make D.E.L.M an incredible course of action that goes past routine obstructions and becomes an imperative resource for a group of applications. In its customary shape, Exceptional Learning Machines work as feedforward neural frameworks and take after the fundamental benchmarks of significant learning. This building empowers a unidirectional data stream through a course of action of layers, engaging the extraction of complex plans and highlighting basics in complex data sets. The feedforward nature of neural frameworks is vital to their capacity to see and handle information and shapes the introduction of D.E.L.M. 's adaptability with particular assignments. Be that as it may, the improvements displayed inside the learning organization of the proposed system talk to an introductory flight from customary approaches, and it is at this point that an unprecedented and competent technique known as backpropagation comes into play. Backpropagation acts as a catalyst to refine and illustrate execution and incorporates development refinement to the learning handle. This method licenses the illustration to iteratively modify parameters based on contrasts between expected to abdicate and honest to goodness, which almost empowers a diligent cycle of headway. The integration of backpropagation into the

learning arrangements of D.E.L.M talks to a critical advance in tending to wants of extended adaptability and isolated learning. Customary feedforward neural frameworks are excellent at plan affirmation, but joining backpropagation presents a feedback circle that iteratively moves forward the model's understanding. This input circle, combined with procedural convolution rates, grants D.E.L.M the ability to investigate complex data sets with extended precision and effectiveness. The embedded procedural collapsing rate in D.E.L.M contributes to its capacity to handle complex data structures. Procedural convolution incorporates deliberate data taken care of through convolutional layers, allowing the appearance to remove dynamic representations and highlights.

This method enables D.E.L.M to recognize sophisticated arrangements in datasets, what makes it necessary tool for multiple sets of applications problems that fall under the category of image verification, emotional freedom and other complex tasks requiring contemporary understanding about data structures with some adjustments for multi dimensional matrix. D.E.L.M's rapid learning facilitates the growth of its reputation in dynamic and developing domains promptly as active and growing areas tend to move forward quite swiftly leading to what is termed a burn rate which has been distinctively high with regards to most industries efficiently specifically. Those that have belonged or are referred extensively within software development where losing an array may leave one down significantly.

The ability to rejection of entropy so that a present level can be properly modified through some relevant changes and this capacity enables effective exploitation throughout associated learning from grouped datasets. This caters to the dynamics of situations where models should constantly iterate in accordance with changing blueprints and designs within one's database. In fact, the use of D.E.L.M involves much broader range of applications than one could expect at first sight Models are critical devices in instances of backslide empowered assignments beyond any doubt numbers is the objective to anticipate, and it chaps with its adaptability as well as usefulness. This also the same for classification tasks.

3.1.1. Overview of D.E.L.M in Various Domains

It makes use of the rapid-learning performance by D.E.L.M, which provides imminent character as a general adapter equipment for various utilizations In particular, let's mention the ability of this model to quickly learn complex schemes that make it suitable for tasks ranging from image recognition and standard language processing up to financial forecast. B. Thus, in such zones as picture acknowledgment , language understanding and financial market pricing involving the ability to quickly adapt to a lot of complex data around it is DELMs fast learning capacity which turns out that they are majorly beneficial for any organization or firm's activities.I am. This accompanies guarantee to its procedural convolution rate fast learning characteristics implanted in D.E.L.M that will make development as far better show signs of improvement for the most part when such reassigned included iterative preparing is concerned In cases where there is continuous learning and adjustments in real time, this highlight is cherished. Among such cases are, mellow monetary markets and developing symptoms of health situations that necessitate an uninterrupted adjustment to the changing patterns. The procedural complicity rate of D.E.L.M ensures beneficial and constructive training in these dynamic locales thus assures reality fit to real-life situations where timely response to progressing information is criticalMasu. The efficiency of the adjustments brought about due to D.E.L.M chief in rapid learning capabilities and speed procedural convolution makes a strong solution for assignment that involves flexibility and responsiveness during not only vibrant, but also changing datasets too over time or function as some other system change parts more often than might be expected inside pertinent situations such even if energetic model systems are revers It is based on the fast learning capacity of the D.E.L.M., which makes it a versatile and dynamic set-up for many applications—here, however; cognitive science rather than physics remains in focus with its implications regarding human intake as HPP's precursor to higher up 'spiritual vices'. Notably, to this end is the model's incredible ability in quickly studying complicated designs making it perfect for tasks which range from image recognition and natural language processing all through financial forecasting.

Energetic budgetary markets and advancing healthcare situations are cases of situations where ceaseless adjustment to changing designs is basic. D.E.L.M.'s procedural convolution rate encourages successful and proficient preparation in these energetic settings and guarantees pertinence to real-world scenarios where the opportune reaction to advancing information is primary. Masu. The combination of quick learning capabilities and procedural convolution speed makes D.E.L.M a robust arrangement for errands that require versatility and responsiveness within the context of energetic and advancing datasets.

3.1.2. Working Instrument of D.E.L.M

Exceedingly, learning machines have genuinely worked as feedforward neural systems. In this plan, information moves in one heading through an arrangement of layers and systems. Each layer contributes to the ultimate result by preparing the input data and extricating relevant information. Backpropagation strategy within the proposed system Within the learning stage of the proposed framework, a backpropagation strategy is utilized, which presents a deviation from the standard approach. To encourage changing weights inside a neural organization, backpropagation includes a flow of data back through the organization. This alter is pointed at diminishing mistake rates to extend precision.

3.1.3. Backpropagation for Enhanced Learning

Coordination backpropagation into a deep extreme learning machine (D.E.L.M) presents a transformative measurement by permitting data to stream in reverse through the layers of a neural organization, not at all like conventional feedforward procedures. This bidirectional stream permits the organization to get complex connections and designs inside the information. Keeping up steadiness is known to be a vital part of the learning process, and the proposed framework employs a key approach to realize this steadiness. This strategy keeps up the same weights all through the approval stage, lessening the chance of overfitting amid the learning stage. Overfitting, the wonder of overfitting a show to a preparing set, can influence a model's capacity to generalize

viably to found information. Guaranteeing reliable weights way better deciphers show an understanding of real-world circumstances, progressing execution, and versatility. D.E.L. M's backpropagation speaks to a paradigm shift that permits a bidirectional data stream and permits the demonstrate to dive more deeply into the complexity of information connections. The iterative weight alteration preparation moves forward the model's prescient exactness and gives a more nuanced and exact understanding of complex designs. At the same time, steady weights anticipate overfitting by emphasizing soundness, guaranteeing the show is strong and versatile within the context of advancing datasets. The synergistic integration of these components highlights the viability of backpropagation in moving forward the overall performance and unwavering quality of profound, extraordinary learning machines. Joining backpropagation into a D.E.L.M presents a transformative measurement by permitting data to stream in reverse through the layers of a neural organization, not at all like conventional feedforward methods. This bidirectional flow allows the arrangement to get complex connections and patterns within the data. The energetic nature of weight changes progresses the learning handle and permits the arrange to alter parameters iteratively, eventually progressing expectation precision. Keeping up steadiness is known to be a critical thought in the learning process, and the proposed system uses a key approach to attaining this stability. This strategy keeps up the same weights all through the approval stage, lessening the chance of overfitting amid the learning stage. Overfitting, the wonder of overfitting a show to a preparing set, can influence a model's capacity to generalize successfully to newly discovered information. Guaranteeing reliable weights and superior interpreters demonstrates understanding of real-world situations, improving execution and flexibility. Basically, D.E.L.M backpropagation permits bidirectional information flow, coming about in a worldview move.

3.1.4. Extracted Models

The ultimate organization of the D.E.L.M learning handle includes extricating the prepared show. This speaks to a critical step that typifies the information obtained by the framework and the understanding of the input information. This prepared demonstration typifies the ideal weights, arrangement, and parameters of the neural arrangement and serves as a capacity for bits of knowledge picked up amid the learning

stage. The extraction handle guarantees that the model's learning data is protected and clears the way for ensuing assignments. Utilizing the prepared demonstration, the framework moves to the genuine information expectation stage. By leveraging the information inserted within the extricated show, D.E.L.M. illustrates its prescient capabilities by making expectations based on genuine information. Whether in regions such as picture recognizable proof, normal dialect preparation, or budgetary determination, D.E.L.M. 's predictive capabilities reflect its flexibility and viability in a variety of applications.

The ultimate organization of the D.E.L.M learning preparation includes extricating the prepared show. This speaks to a vital step that typifies the information obtained by the framework and the understanding of the input information. This prepared show typifies the ideal weights, set up, and parameters of the neural arrangement and serves as a capacity for insights picked up amid the learning stage. The extraction handle guarantees that the model's learning data is protected and clears the way for ensuing errands. Utilizing the prepared show, the framework moves to the real information forecast phase.

3.1.5. Case Studies and Practical Applications

D.E.L.M. 's procedural convolution rate is utilized in normal dialect handling to empower compelling dialect understanding. Backpropagation innovation progresses the understanding of complex dialect designs, making estimation investigation, dialect interpretation, and chatbot intelligence more precise.

Money-related Estimating: D.E.L.M. 's capacity to rapidly learn modern abilities and adjust to changing showcase conditions is basic within the money-related field. Backpropagation methods progress forecast precision and are, in this manner, valuable for exercises such as algorithmic exchange, chance evaluation, and stock cost expectation.

D.E.L.M. Adaptability Overseeing distinctive sorts of information is helpful to the healthcare industry. Exact prescient investigation is encouraged by the capacity to

adjust to changing restorative datasets and modern learning through backpropagation. This makes a difference in planning medicines, anticipating infections, and making ideal utilization of restorative assets.

Picture acknowledgment: D.E.L.M. It is characterized by quick learning speed when recognizing complex designs in photographs. Backpropagation makes strides in exactness, permitting the distinguishing proof of more complex objects and highlights. Applications such as independent vehicle routes and therapeutic imaging can benefit from this. Normal

D.E.L.M. 's procedural convolution rate is utilized in standard dialect preparation to empower successful dialect understanding. Backpropagation innovation moves forward in the understanding of complex dialect designs, making assumption examination, dialect interpretation, and chatbot intelligence more precise.

Budgetary Determining: D.E.L.M. 's capacity to rapidly learn modern aptitudes and adjust to changing advertising conditions is basic within the monetary field. Backpropagation strategies make strides in forecast exactness and are, in this manner, valuable for exercises such as algorithmic exchanging, hazard evaluation, and stock cost expectation.

Adaptability Overseeing diverse sorts of information is advantageous to the healthcare industry. Exact prescient investigation is encouraged by the capacity to adjust to changing therapeutic datasets and modern learning through backpropagation. This makes a difference in planning medicines, anticipating illnesses, and making ideal utilization of restorative assets.

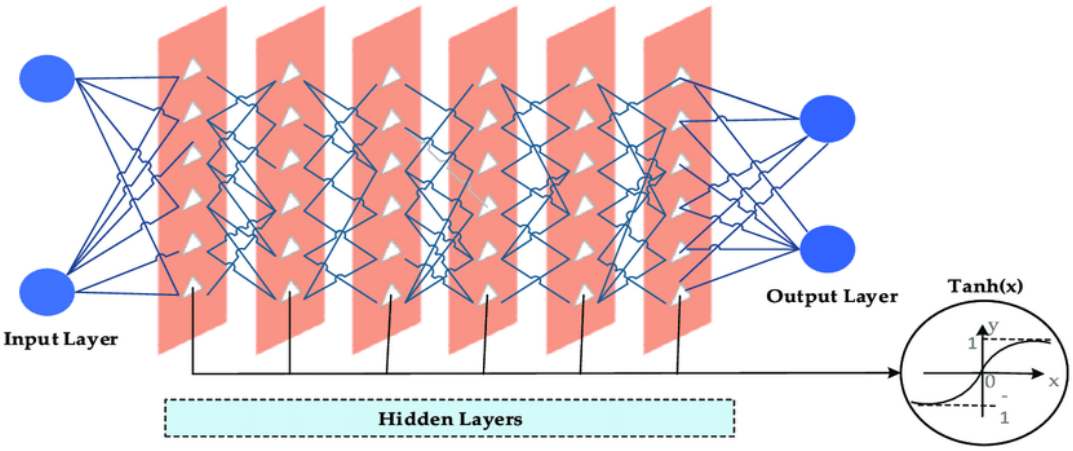

Figure 3.2. D.E.L.M Architecture.

As appeared in Figure 3.2, the proposed approach encourages the integration of D.E.L.M. into blockchain-based shrewd frameworks. This unused strategy points to the required advantage of D.E.L.M. 's predominant learning capacities. Combine. It has the decentralized and secure highlights of blockchain innovation. D.E.L.M. comprises three fundamental levels.

System Engineering: Input layer, yield layer, and a few covered-up layers. Not at all like conventional constrained learning machines, which regularly utilize covered-up layers with numerous neurons, the D.E.L.M. system contains more complex engineering. It has a few covered-up layers that complicate the framework and permit it to distinguish complex patterns within the information. This key perspective of progressing by and large organized execution may be a takeoff from the conventional single covered-up layer design. A comparative ponder of the viability of increasing the covered-up layer with a settled number of neurons is displayed in Table 1. It appears that including covered-up layers to the network moves forward compared to other machine learning procedures. This execution change shows how well the proposed D.E.L.M. system performs and is sweet at overseeing complex information structures. Feedforward and backpropagation methods can be effortlessly coordinated into the D.E.L.M. engineering. This integration is vital to alter the weights of the arrangement to diminish the mistake rate and progress exactness.

Backpropagation may be a bidirectional data stream that makes a difference in systems to get complex information designs better. The adaptability and effectiveness of the framework are expanded by the D.E.L.M. engineering, which guarantees ceaseless learning by more than once changing weights based on comparisons between anticipated and genuine comes about. It is critical to note this, given the deep architecture of D.E.L.M., which varies from conventional constrain learning machine plans. D.E.L.M. 's significant plan. Utilizing numerous covered-up layers introduces a reliable number of neurons in each layer, though a standard limit learning machine can contain numerous neurons in a single covered-up layer. The reason for this alteration is to progress and organize execution by permitting. As appeared in Figure 1, the proposed approach encourages the integration of D.E.L.M. into blockchain-based intelligent frameworks. This unused strategy points to the required advantage of D.E.L.M. 's prevalent learning capacities. Combine. It has the decentralized and secure highlights of blockchain innovation. D.E.L.M. comprises three essential levels. System engineering:

Input layer, yield layer, and a few covered-up layers. Unlike conventional constrained learning machines, which regularly utilize covered-up layers with numerous neurons, the D.E.L.M. system encompasses a more complex architecture. It has several hidden layers that complicate the system and permit it to identify complex designs within the information. This key perspective of progressing by and large organized execution could be a flight from the conventional single covered-up layer engineering. A comparative consideration of the viability of augmenting the covered-up layer with a settled number of neurons is displayed in Table 1. It appears that including hidden layers to the organization progresses the results compared to other machine learning techniques. This execution enhancement shows how well the proposed D.E.L.M. system performs and is nice at overseeing complex information structures. Feedforward and backpropagation procedures can be effectively integrated into the D.E.L.M. engineering. This integration is vital to modify the weights of the arrangement to diminish mistake rate and progress precision.

Backpropagation may be a bidirectional data stream that makes a difference in systems to better get complex information designs. The adaptability and productivity of the

framework are expanded by the D.E.L.M. design, which guarantees ceaseless learning by more than once changing weights based on comparisons between anticipated and genuine comes about. It is critical to note this, given the profound design of D.E.L.M., which varies from conventional constrain learning machine designs. D.E.L.M.'s significant plan. Utilizing different covered-up layers presents a consistent number of neurons in each layer, while a standard limit learning machine can contain numerous neurons in a single covered-up layer. The purpose of this alteration is to progress and organize execution by permitting.

Table 3.1. Method Accuracy Comparison Using KDDCUP-99 and NSLKDD Datasets.

Method	NSLKDD Accuracy (%) [78]	KDDCUP-99 Accuracy (%) [79]
ANN	81.2	90.39
SVM	69.52	89.94
Decision Tree	81.5	91.12
Proposed Method	93.91	94.60

The assessment layer of brilliant frameworks is basic to keeping up solid security conventions. Several measurable capacities are utilized to optimize framework execution in this situation. As appeared in Figure 2, these properties incorporate exactness, mistake rate, affectability, specificity, untrue positive esteem, and positive prescient esteem. To progress the security of brilliant frameworks, these variables must be examined entirely. Backpropagation is a critical strategy in this circumstance. Weight setting, feedforward engendering, reverse blunder engendering, and discriminability overhauls are a few of the vital forms in this approach. Utilizing these procedures, the framework adjusts and extends its usefulness depending on the inputs obtained during the assessment stage.

Each neuron within the covered-up layer employments a sigmoid enactment work within the backpropagation calculation. This determination of enactment capacities makes both the sigmoid input work and the D.E.L.M. covered-up layer. Segregation Upgrading Progressive Modules or D.E.L.M. Covered-up Layers helps the framework recognize designs and highlights within the approaching data. Measuring show execution is a critical portion of evaluating a system. Typically fulfilled by employing

a calculation of 2 to play down the whole of squares for the aiming result. This sort of evaluation is vital for assessing the exactness and execution of the framework. In any case, this requires the framework to alter the weights to address and rectify common mistakes.

The weight dissemination of the backpropagation preparation encompasses a critical effect on the learning and adjusting capacity of the framework. Carefully changing the weights relegated to each association in a neural arrangement moves forward the, by and large, usefulness of the system and optimizes its reaction. The system's capacity to memorize from encounters and ceaselessly make strides in its functionality depends intensely on this energetic weight alteration. Another critical step within the backpropagation handle is feedforward proliferation. In this stage, the input information is sent through the neural network layer by layer and, at last, produces the output. The precision of the method is basic because it specifically impacts the system's capacity to create faultless choices based on the data it gets. In expansion to feedforward propagation, backward blunder proliferation allows you to alter the configuration of your framework in reaction to blunders recognized amid assessment. The capacity to move forward a system's inner representation and decision-making capabilities over time depends on this iterative criticism circle.

The assessment layer of brilliant frameworks is basic to keeping up solid security conventions. Several factual capacities are utilized to optimize framework execution in this situation. As appeared in Figure 2, these properties incorporate precision, blunder rate, affectability, specificity, wrong positive value, and positive prescient esteem. To make strides in the security of brilliant frameworks, these components must be altogether examined. Backpropagation is a vital strategy in this circumstance. Weight setting, feedforward engendering, reverse mistake engendering, and discriminability upgrades are a few of the imperative forms in this approach. Utilizing these methods, the framework adjusts and extends its usefulness depending on the inputs obtained during the assessment stage.

Each neuron within the covered-up layer employs a sigmoid enactment work within the backpropagation calculation. This determination of enactment capacities creates

both the sigmoid input function and the D.E.L.M. covered-up layer. Segregation Improving Various Leveled Modules or D.E.L.M. Covered up Layers help the framework recognize designs and highlights within the incoming data. Measuring and demonstrating execution is an imperative portion of evaluating a system. This is accomplished by employing a figure of 2 to play down the entirety of squares for the expected result. This sort of evaluation is critical for assessing the precision and execution of the framework. Be that as it may, this requires the framework to alter the weights to address and adjust common blunders.

PART 4

RESULTS AND DISCUSSIONS

This comprehensive archive points to the perplexing points of interest of conveying a D.E.L.M. inside a carefully planned design. The premise of our work lies within the utilization of input information from the NSL-KDD dataset [78], which is utilized as the premise for preparing and approving D.E.L.M. Serve. Our essential objective is to use the viability of this device in recognizing pernicious behavior and organizing compromise. To guarantee dependable assessment, we carefully partitioned the dataset employing an irregular apportioning strategy. Particularly, 85% of the whole sum (comprising 125,973 tests) was for preparation, and the remaining 15% (22,543 tests) was saved for approval. This apportioning methodology is critical for preparing the show on a substantial subset of the information while keeping up an isolated set for approval. This permits you to assess how well D.E.L.M. generalizes to modern, untested information. Recently, when applying thorough explanatory methods to the information, a preprocessing step was required. The reason for this preprocessing was to dispose of information peculiarities and decrease the plausibility of blunders. Our objective was to make strides in the general quality and unwavering quality of consequent analyses performed utilizing D.E.L.M. by disposing of potential irregularities and mistakes. It was conducted. The center of our inquiry is to abuse the capabilities of D.E.L.M. Recognize malevolent movement and interruptions through a combination of covered-up associations, actuation capacities, and covered-up layers. The choice and configuration of these structural components encompass a critical effect on the model's capacity to recognize designs and draw quick conclusions. Presenting covered-up layers into the D.E.L.M. engineering makes a progressive system that permits the demonstration to capture complex representations of the input information. Deliberately changing the weight structure between these covered-up layers plays a key part in encouraging the data stream and moving forward the model's capacity to get complex connections inside the information. The center of D.E.L.M. 's

engineering is the enactment work chosen for the neurons within the covered-up layer. Cautious determination of these features is basic to how successfully the demonstration can capture nonlinear connections and complex designs within the information. The interaction between covered-up layers, actuation capacities, and weight structures makes a difference in realizing D.E.L.M. The capacity to identify inconspicuous subtleties in input information eventually permits for more exact recognizable proof of pernicious movement and organized interruptions. This comprehensive report points to the perplexing points of interest of conveying D.E.L.M. inside a carefully planned design. The premise of our work lies within the utilization of input information from the NSL-KDD dataset [78], which is utilized as the premise for preparing and approving D.E.L.M. Serve. Our essential objective is to leverage the adequacy of this tool in distinguishing pernicious behavior and organizing compromise. To guarantee dependable assessment, we carefully apportioned the dataset employing an arbitrary dividing technique. Specifically, 85% of the full sum (comprising 125,973 tests) was for training, and the remaining 15% (22,543 tests) was reserved for approval. This dividing methodology is critical for preparing the demonstration on a significant subset of the data while keeping up an isolated set for approval. This allows you to assess how well D.E.L.M. generalizes to unused, untested information. Sometime recently, when applying thorough analytical procedures to the data, a preprocessing step was required. The reason for this preprocessing was to dispose of information irregularities and decrease the plausibility of mistakes. Our objective was to make strides in the general quality and unwavering quality of ensuing analyses performed utilizing D.E.L.M. by dispensing with potential irregularities and blunders. It was conducted. The center of our investigation is to abuse the capabilities of D.E.L.M. and distinguish pernicious action and intrusions through a combination of covered-up associations, actuation capacities, and covered-up layers. The choice and setup of these building components feature a noteworthy effect on the model's capacity to recognize designs and draw quick conclusions. Introducing hidden layers into the D.E.L.M. architecture makes a progressive system that permits the demonstration to capture complex representations of the input information. Deliberately changing the weight structure between these covered-up layers plays a key part in encouraging the data stream and progressing the model's capacity to get complex connections inside the data. The center of D.E.L.M. 's engineering is the activation work chosen for the

neurons in the covered-up layer. Cautious determination of these highlights is basic to how viably the model can capture nonlinear connections and complex designs within the information. The interaction between covered-up layers, enactment capacities, and weight structures helps realize D.E.L.M. The ability to identify inconspicuous subtleties in input information eventually permits more exact recognizable proof of noxious movement and organized interruptions.

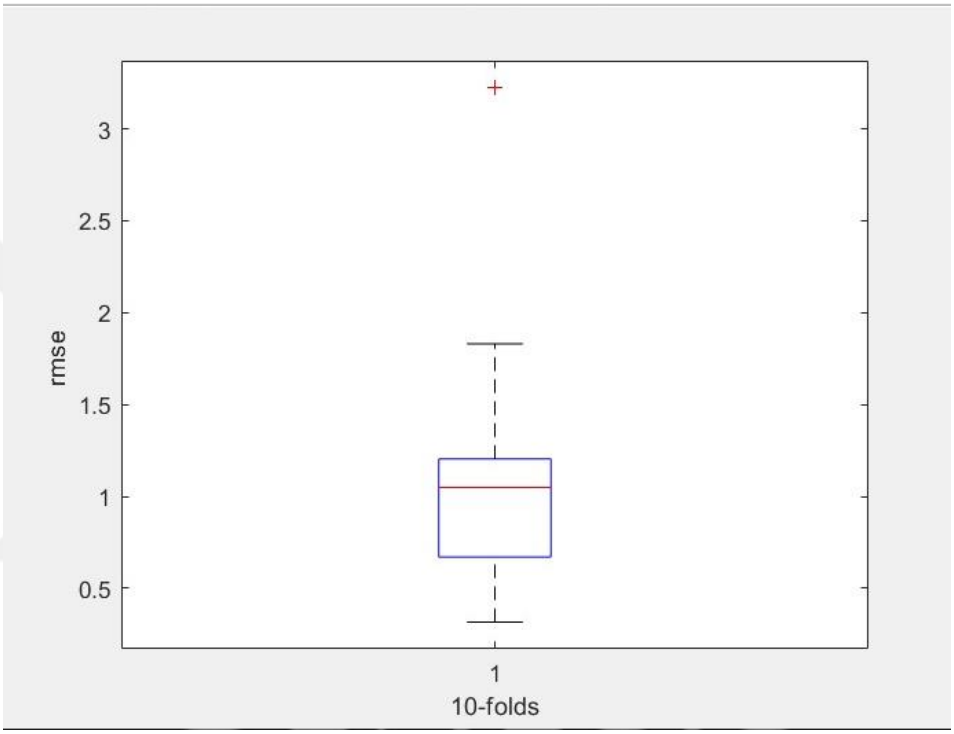

Figure 4.1. Performance assessment of a deep extreme learning machine system model based on ABC and CNN.

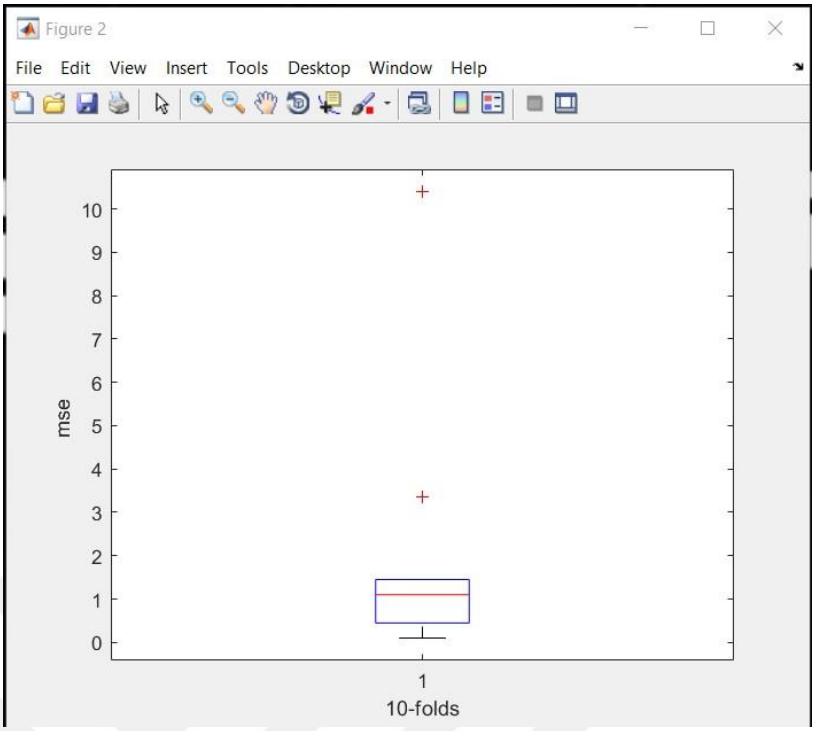

Figure 4.2. Performance assessment of a deep extreme learning machine system model based on ABC and CNN.

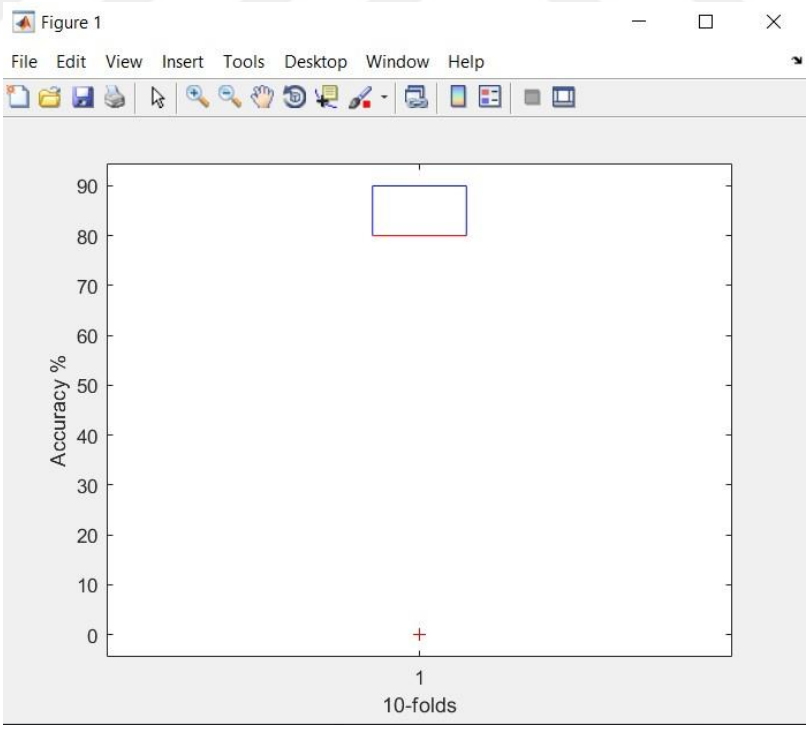

Figure 4.3. Performance assessment of a deep extreme learning machine system model based on ABC and CNN.

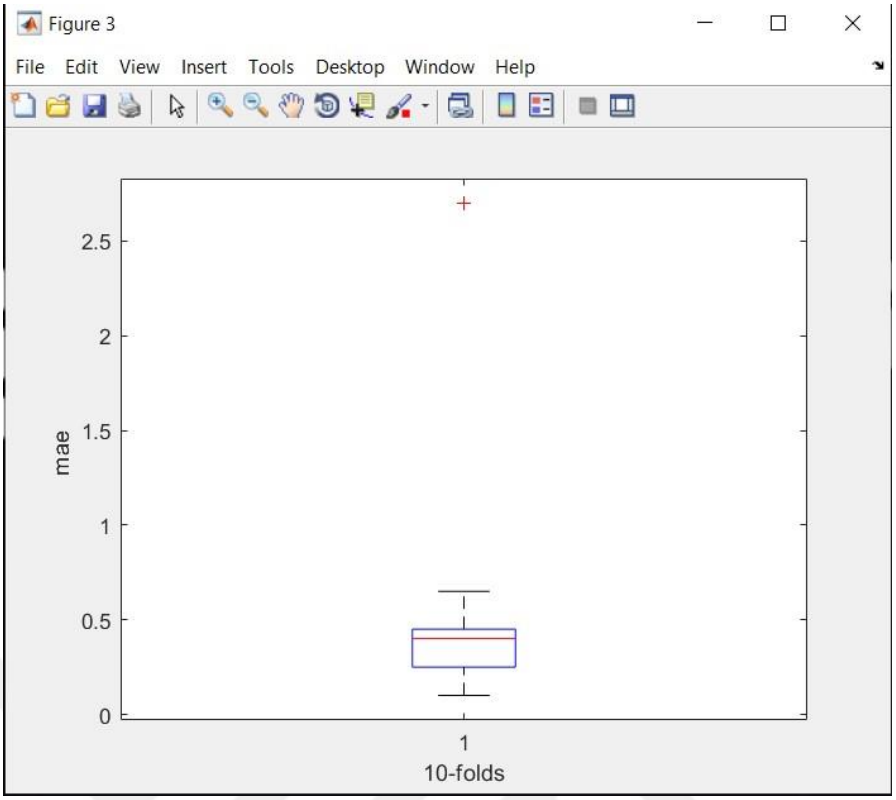

Figure 4.4. Performance assessment of a deep extreme learning machine system model based on ABC and CNN.

Inside the examination of passing on the Deep Extreme Learning Machine D.E.L.M., a carefully curated dataset serves as the linchpin, promoting a nuanced perspective into the model's capacity to recognize between conventional organized behavior changes and potential interferences. This dataset, meticulously divided into 12,833 attack tests and 9,710 normal tests, shapes the cauldron where the experiences of the system appear, showing its capacity to investigate the complex scene of organized works. Central to the model's lifecycle is the essential endorsement step, a point where speculative ability focuses on genuine world application needs. Here, the show experiences intensive testing to survey its wellness in applying the lessons assembled from the planning set to novel, subtly cases.

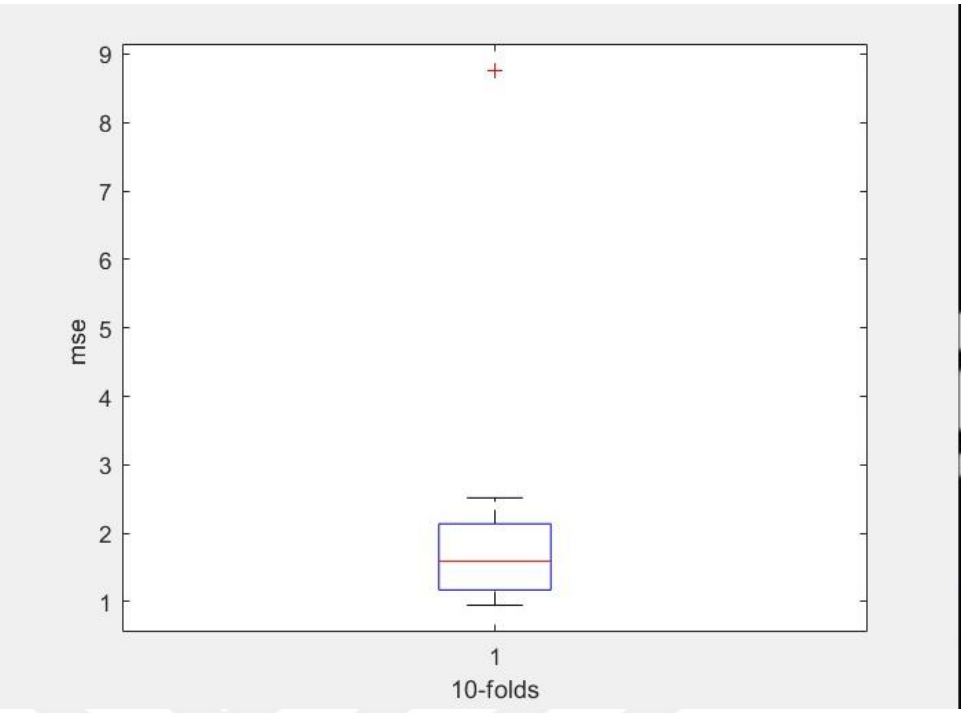

Figure 4.5. Performance assessment of a deep extreme learning machine system model based on CNN.

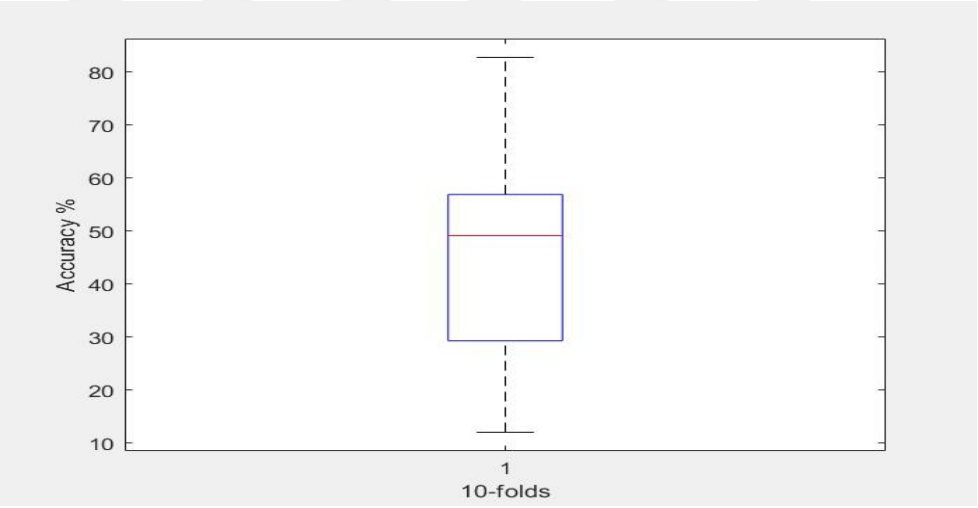

Figure 4.6. Performance assessment of a deep extreme learning machine system model based on CNN.

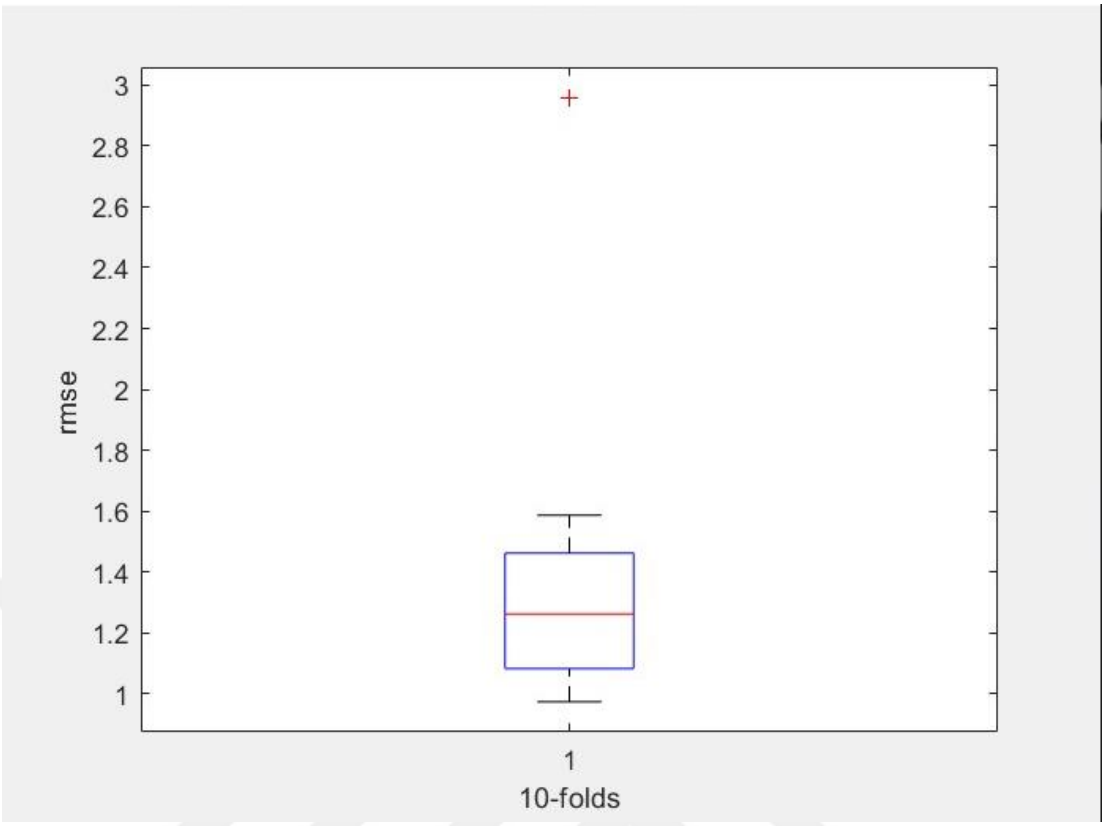

Figure 4.7. Performance assessment of a deep extreme learning machine system model based on CNN.

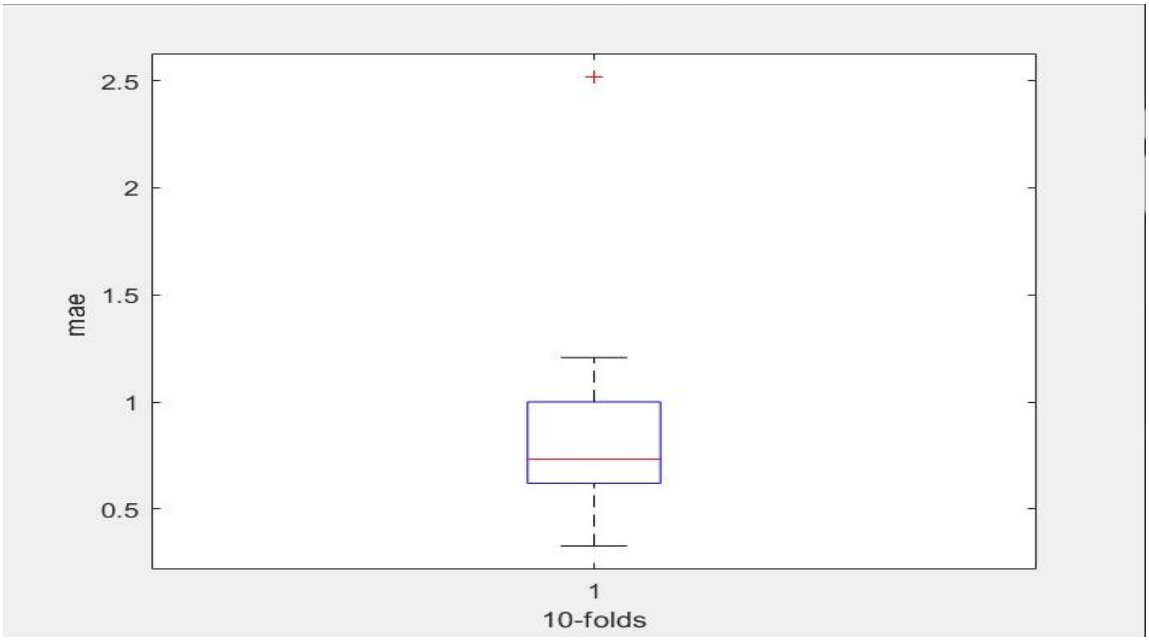

Figure 4.8. Performance assessment of a deep extreme learning machine system model based on CNN.

The consideration of allocating the dataset into an ambush and standard tests gives a granular central point, enabling a correct and nuanced examination of the model's execution. This comprehensive dataset, totaling 22,543 tests, set up the observational foundation upon which the proposed savvy system refines its understanding of designs, varieties from the standard, and potential dangers of interior organized behavior. Of this wide collection, 12,833 tests talk to reenacted assaults deliberately made as opposing circumstances to test the model's exactness and adaptability completely. In separate, the remaining 9,710 tests capture the safe and standard works that constitute the foundation of standard orchestrate behavior. The deliberate outline between ambush and standard tests focuses on reflecting the distinctive scene of genuine world-organized circumstances, avoiding discretion to form a smaller than-anticipated representation of the challenges quick systems encounter inside the ever-changing and frequently whimsical space of the Net of Things IoT. This dataset serves as a pot for surveying the D.E.L.M.'s practicality in interruption location, giving a microcosm of the enthusiastic and multifaceted scenarios experienced in IoT circumstances.

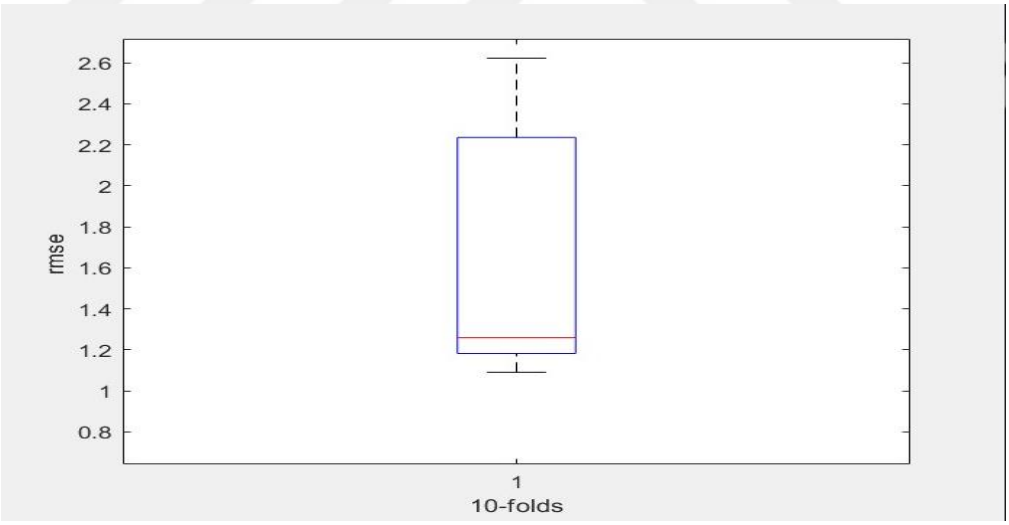

Figure 4.9. Performance assessment of a deep extreme learning machine system model based on CFFBP.

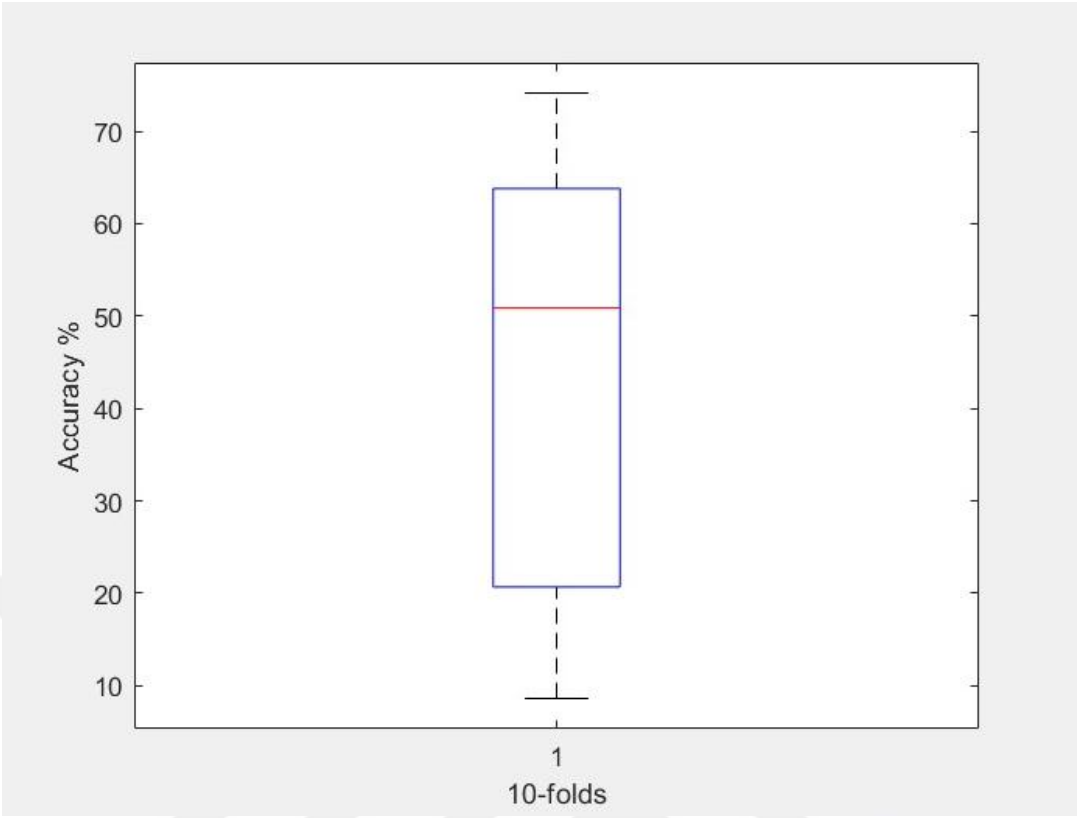

Figure 4.10. Performance assessment of a deep extreme learning machine system model based on CFFBP.

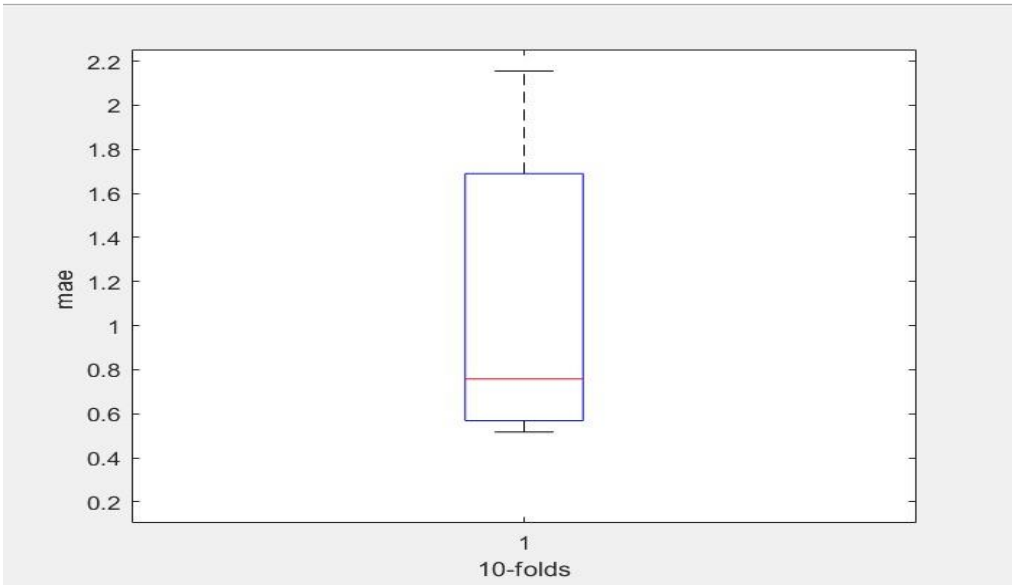

Figure 4.11. Performance assessment of a deep extreme learning machine system model based on CFFBP.

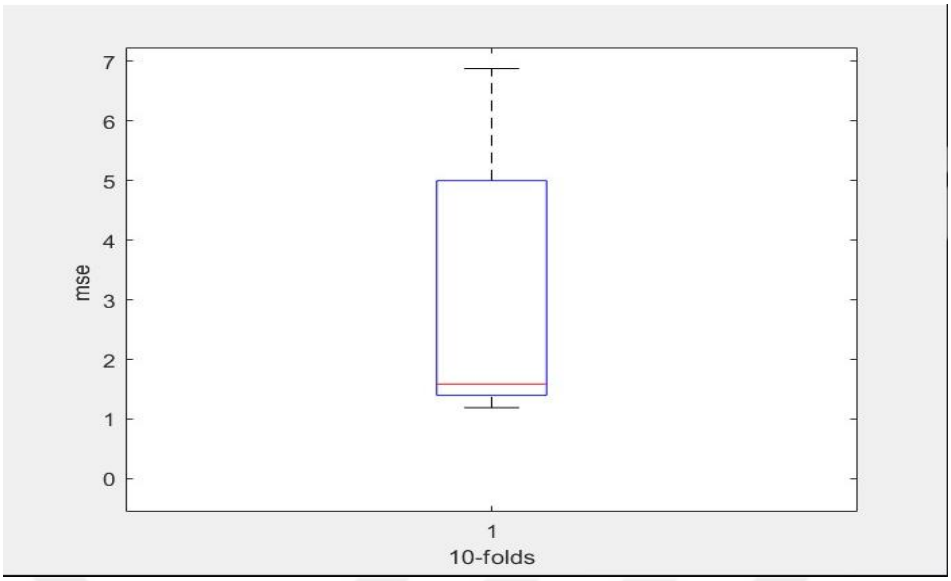

Figure 4.12. Performance assessment of a deep extreme learning machine system model based on CFFBP.

The deliberateness consolidation of adversarial circumstances inside the shape of reenacted assaults challenges the model's vigor and flexibility, mirroring genuine world scenarios where malignant on-screen characters seek to abuse vulnerabilities. In parallel, the works embedded inside the dataset reflect the planned organizational behavior that shapes the foundation of commonality, creating an all-encompassing and specialist test of the IoT scene. The cautious division of the dataset is not because it serves the reason of appearing endorsement but to edify broader considerations inside the space of cybersecurity and machine learning. By deliberately categorizing tests into ambush and commonplace events, the dataset mirrors the complexity of real organized circumstances, where inconsistencies are compared with plan works out. This deliberateness representation licenses the D.E.L.M. to investigate the complexities of orchestrate behavior with an expanded level of precision and flexibility, essential characteristics inside the setting of IoT, where changeability and capriciousness are the standard. The capability drawn between attack and standard tests in this dataset may be a pondered choice aimed at capturing the core of real-world challenges gone up against by adroitly systems. The dataset, in this way, serves as more than a testing ground; it becomes a microcosm that exemplifies the complexities, challenges, and dynamism innate inside the tremendous scene of the Internet of Things. Through this thought curation, the investigation is not only because it was moving the understanding of the D.E.L.M.'s execution but also contributes to the

broader conversation on the application of brilliant systems inside the ever-evolving space of IoT cybersecurity.

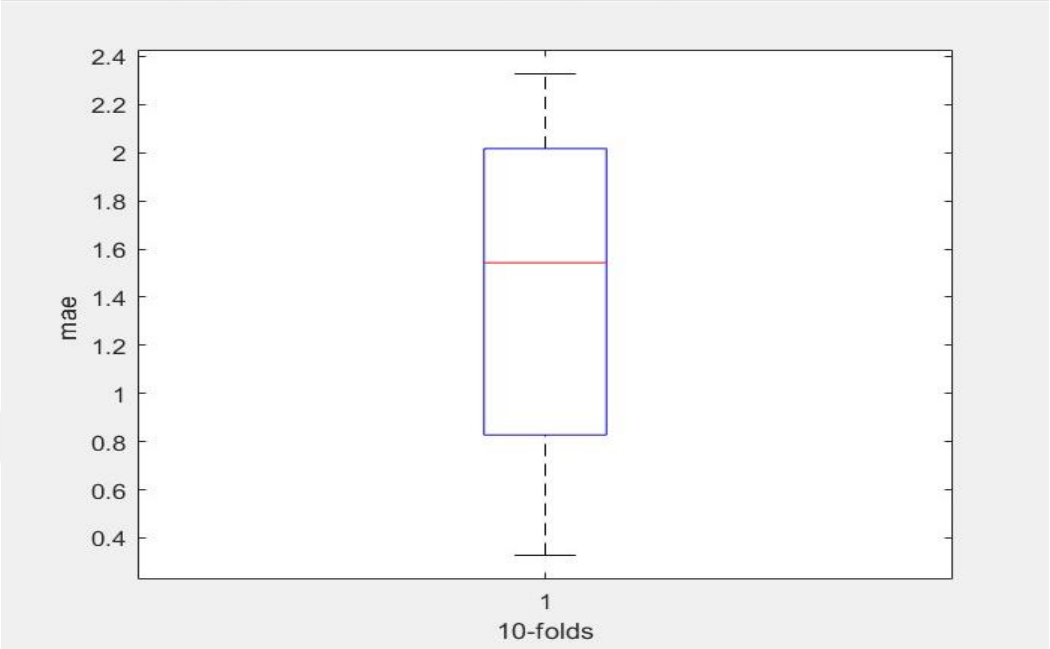

Figure 4.13. Performance assessment of a deep extreme learning machine system model based on FFPP.

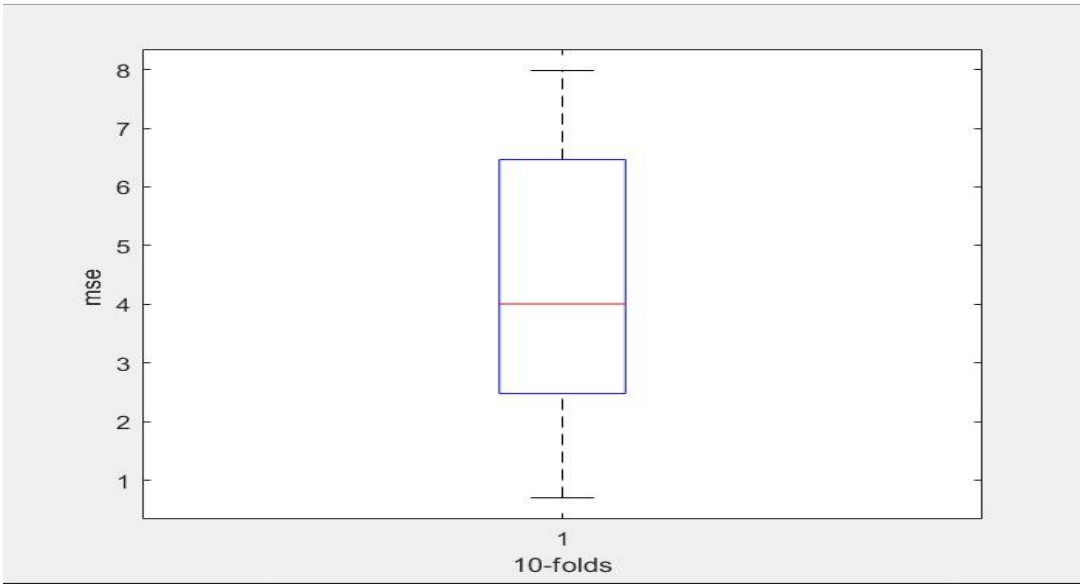

Figure 4.14. Performance assessment of a deep extreme learning machine system model based on FFPP.

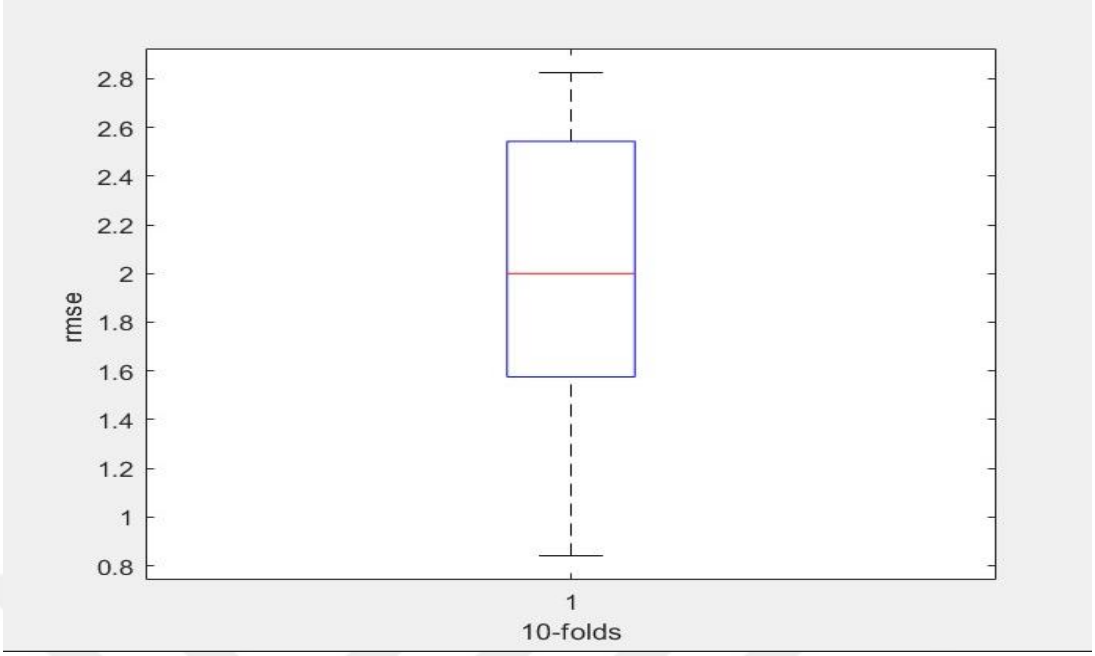

Figure 4.15. Performance assessment of a deep extreme learning machine system model based on FFPP.

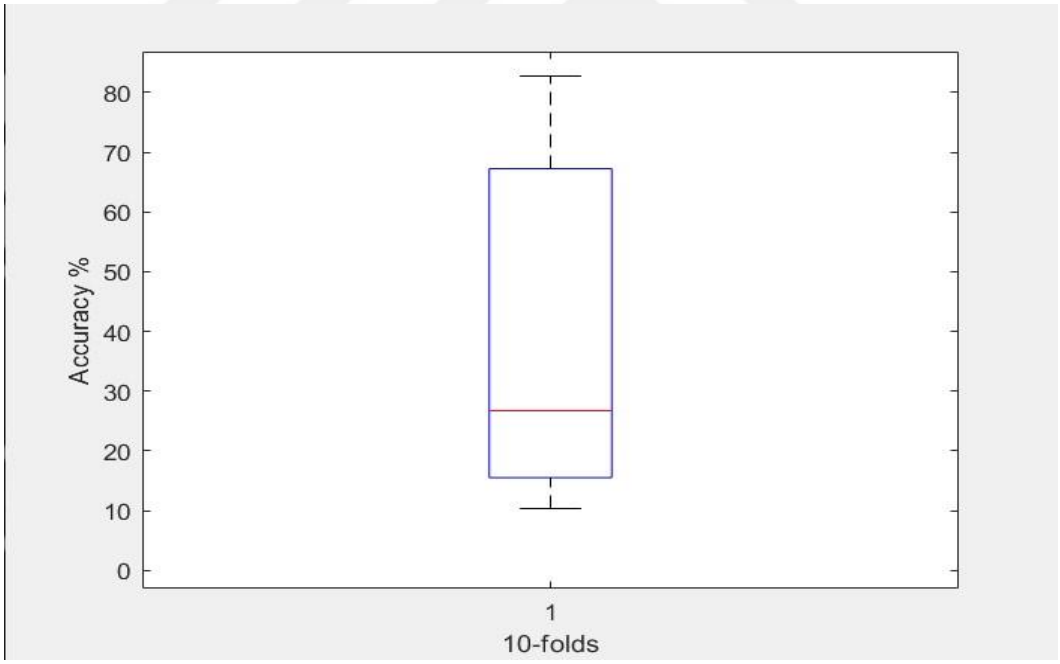

Figure 4.16. Performance assessment of a deep extreme learning machine system model based on FFPP.

Inside the examination of passing on the Significant Exceptional Learning Machine D.E.L.M., a carefully curated dataset serves as the linchpin, publicizing a nuanced perspective into the model's capacity to recognize between conventional organized

behavior changes and potential intrusions. This dataset, critically divided into 12,833 ambush tests and 9,710 commonplace tests, shapes the cauldron where the experiences of the system appear, showing its capacity to investigate the complex scene of organized works. Central to the model's lifecycle is the fundamental endorsement step, a point where theoretical ability is focalized with real-world application needs. Here, the show experiences intensive testing to evaluate its wellness in applying the lessons accumulated from the planning set to novel, intangibly cases. The consideration of allocating the dataset into the attack and standard tests gives a granular focal point, enabling a correct and nuanced examination of the model's execution. This comprehensive dataset, totaling 22,543 tests, sets up the observational foundation upon which the proposed savvy system refines its understanding of designs, varieties from the standard, and potential dangers inside arranged behavior. Of this wide collection, 12,833 tests talk to reenacted assaults intentionally made as opposing circumstances to test the model's exactness and adaptability completely. In separate, the remaining 9,710 tests capture the safe and standard works that constitute the foundation of conventional orchestrate behavior. The deliberate division between attack and standard tests focuses on reflecting the distinctive scene of genuine world-organized circumstances, avoiding assertion to form a smaller than anticipated representation of the challenges shrewd frameworks encounter inside the ever-changing and frequently sporadic space of the Net of Things IoT. This dataset serves as a pot for evaluating the D.E.L.M.’s practicality in interruption discovery, giving a microcosm of the enthusiastic and multifaceted scenarios experienced in IoT circumstances. The deliberate consolidation of opposing circumstances inside the shape of recreated assaults challenges the model's vigor and flexibility, mirroring genuine world scenarios where vindictive on-screen characters explore to abuse vulnerabilities. In parallel, the kind of work embedded inside the dataset reflects the planned, organized behavior that shapes the foundation of commonality, creating an all-encompassing operator test of the IoT landscape. The cautious division of the dataset is not only because it serves the inciting reason of appearing endorsement but also illuminates broader thoughts inside the space of cybersecurity and machine learning. By deliberately categorizing tests into ambush and commonplace events, the dataset mirrors the complexity of genuine arranged circumstances, where abnormalities are compared with plan work. This deliberateness representation grants the D.E.L.M.

PART 5

CONCLUSION

Emergence blockchain technology coupled with D.E.L.M constitutes an important development in the IoT and, indeed in intelligent systems that provides innovative solutions to security protection flexibility among other dynamic issues discussed here under process – serving parameters agents include aspects such as operative statuses management subset contextual decisions mechanisms artificial structures serve required substitutional effects quantity The proposed model based on these facts is shown DELM., illustrates that interruption takes place due to enabled training and approval procedure in particular concerning the location of disturbance,. high accuracy rate figures trends nd removal falseideas The decentralized architecture on blockchain eliminates tamper-proof information capacity, thus minimizing threat as a result central verification servers were developed via process low lead. The present inquiry however focuses on the interventionist effect of blockchain application and D.E.L.M, stimulated within smart systemic ecology . The partnership between these innovativenesses highlights enhanced security measures, decreased energy metabolic rate and transformed cognate consumer environment. With smart frameworks continue to evolve, security steps would actually want to be strong for the reason of protecting sensitive information and guaranteeing customer safety. The blockchain principles of decentralization and inherent permanence make it a viable solution for encrypting heterogeneous data that is being generated in intelligently networked scenarios. This ponder lays the foundation for future investigation and development in coordination with D.E.L.M. and blockchain within the Internet of Things. Extra inquiry about and improvement endeavors seem to make strides in current strategies, illuminate unused issues, and open unused avenues to consistently coordinate blockchain innovation into complex IoT innovation systems as this field develops. The results of this investigation open the entryway to a more secure, robust, and privacy-friendly Internet of Things by making a difference in how blockchain and D.E.L.M. work together in shrewd frameworks. Within the setting of the IoT and, more particularly, brilliant frameworks, the combination of blockchain innovation with D.E.L.M. constitutes a progressive step

forward in fathoming issues critical in terms of security, security, and versatility. The suggested structure, underlined by D.E.L.M., gives finding encouraging outcomes in the preparation and acceptance stage especially regarding interruption detection achieving high accuracy ratios and reducing false , predictions among others,. Decentralized engineering is the difference that blockchains make with regard to tamper-proof information capacity and hence, risks posed by centralised confirmation servers thus are relieved. This investigation points out the revolutionary nature of joint usage blockchain and D.E.L..M within smart systems contexts environment. These innovations cooperate properly, with the combination working together to give better and reliable security actions, lesser energy consumption level of plus improved individualization With increasing focus on frameworks taking conceptual spins to be more intricate, best quality security measures are required so as to secure undeniable data and guarantee the encryption of clients' individual information. Blockchain's decentralization and unalterability denote it as a potent solution, considered to secure broadly produced facts in smart grid situations. This observation provides the foundation for future research and development in the convergence of D.E.L.M., blockchain within IoTs setting out various new opportunities awaiting due diligence to facilitate smarter lifestyle solutions that are efficient, secure convenient hence reliable backed by relevant stakeholders such as governments commercial organisations etc worldwide Additional effort should throw the light on advanced solutions, outline modern riddles and set way for future engagement of blockchain technology in complicated IOT innovation systems as this discipline progresses. What arises from this analysis unlocks the door to a safer, more resilient and privacy preserving IoT by changing how blockchain technologies and D.E.L.M operate on connected systems.

REFERENCES

1. Atzori, L., Iera, A., Morabito, G. (2017). Understanding the internet of things: definition, potentials, and societal role of a fast-evolving paradigm. Ad Hoc Networks, 56, 122–140.

2. Giaoutzi, M., Scholten, H.J. (2017). A common operational picture in support of situational awareness for efficient emergency response operations. Journal of Future Internet, 2(1), 10–35.

3. Abdullah, S., Arshad, J., Khan, M.M., Alazab, M., Salah, K. (2023). Prised tangle: A privacy-aware framework for smart healthcare data sharing using iota tangle. Complex & Intelligent Systems, 9(3), 3023–3041.

4. Khalil, U., Malik, O.A., Uddin, M., Chen, C.-L. (2022). A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. Sensors, 22(14), 5168.

5. Mohammadi, M., Al-Fuqaha, A., Sorour, S., Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923–2960.

6. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I.S., Mazura, M., Harrison, M., Eisenhauer, M., et al. (2022). Internet of Things strategic research roadmap. In: Internet of Things-global Technological and Societal Trends from Smart Environments and Spaces to Green ICT, pp. 9–52. River Publishers.

7. Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J. (2020). Internet of things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54, 101728.

8. Balbi, G., Fickers, A. (2020). History of the International Telecommunication Union (ITU): Transnational Techno-diplomacy from the Telegraph to the Internet. Oldenburg: De Gruyter.

9. Kumar, N.M., Mallick, P.K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815–1823.

10. Bansal, S., Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware, and communication. International Journal of Wireless Information Networks, 27, 340–364.

11. Jiang, X., Zhang, H., Yi, E.A.B., Raghunathan, N., Mousoulis, C., Chaterji, S., Peroulis, D., Shakouri, A., Bagchi, S. (2020). Hybrid low-power wide-area mesh network for IoT applications. IEEE Internet of Things Journal, 8(2), 901–915.

12. Grammatikis, P.I.R., Sarigiannidis, P.G., Moscholios, I.D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 5, 41–70.

13. Serˆodio, C., Cunha, J., Candela, G., Rodriguez, S., Sousa, X.R., Branco, F. (2023). The 6G ecosystem as support for IOE and private networks: Vision, requirements, and challenges. Future Internet, 15(11), 348.

14. Zhang, H., Wang, J., Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. Energy, 180, 955–967.

15. Hellani, H., Sliman, L., Samhat, A.E., Exposito, E. (2021). On blockchain integration with supply chain: Overview on data transparency. Logistics, 5(3), 46.

16. Garrido, G.M., Sedlmeir, J., Uludaˇg, ̈O., Alaoui, I.S., Luckow, A., Matthes, F. (2022). Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. Journal of Network and Computer Applications, 207, 103465.

17. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review.

18. Ali, M., Karimipour, H., Tariq, M. (2021). Integration of blockchain and federated learning for the Internet of Things: Recent advances and future challenges. Computers & Security, 108, 102355.

19. Egala, B.S., Pradhan, A.K., Dey, P., Badarla, V., Mohanty, S.P. (2023). Fortified-chain 2.0: Intelligent blockchain for decentralized smart healthcare system. IEEE Internet of Things Journal.

20. Javaid, M., Haleem, A., Singh, R.P., Suman, R., Gonzalez, E.S. (2022). Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. Sustainable Operations and Computers, 3, 203–217.

21. Freund, G.P., Fagundes, P.B., Macedo, D.D.J. (2021). An analysis of blockchain and GDPR under the data lifecycle perspective. Mobile Networks and Applications, 26, 266–276.

22. Munirathinam, S. (2020). Industry 4.0: Industrial Internet of Things (IIoT). In: Advances in Computers vol. 117, pp. 129–164. Elsevier.

23. Zhong, R.Y., Xu, X., Klotz, E., Newman, S.T. (2017). Intelligent manufacturing in the context of Industry 4.0: a review. Engineering, 3(5), 616–630.

24. Jabbar, A., Akhtar, P., Dani, S. (2020). Real-time big data processing for instantaneous marketing decisions: A problematization approach. Industrial Marketing Management, 90, 558–569.

25. Lee, J., Bagheri, B., Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18–23.

26. Rebelo, R.M.L., Pereira, S.C.F., Queiroz, M.M. (2022). The interplay between the Internet of Things and supply chain management: Challenges and opportunities based on a systematic literature review. Benchmarking: An International Journal, 29(2), 683–711.

27. Musa, A., Dabo, A.-A.A. (2016). A review of RFID in supply chain management: 2000–2015. Global Journal of Flexible Systems Management, 17, 189–228.

28. Yangui, S., Goscinski, A., Drira, K., Tari, Z., Benslimane, D. (2021). Future Generation of Service-oriented Computing Systems. Elsevier.

29. Allioui, H., Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. Sensors, 23(19), 8015.

30. Sobb, T., Turnbull, B., Moustafa, N. (2020). Supply chain 4.0: A survey of cybersecurity challenges, solutions and future directions. Electronics, 9(11), 1864.

31. Latif, S., Idrees, Z., Huma, Z., Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. Transactions on Emerging Telecommunications Technologies, 32(11), 4337.

32. Jagatheesaperumal, S.K., Ahmad, K., Al-Fuqaha, A., Qadir, J. (2022). Advancing education through extended reality and Internet of Everything enabled metaverses: Applications, challenges, and open issues. arXiv preprint arXiv:2207.01512.

33. Iansiti, M., Lakhani, K.R., et al. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118–127.

34. Jasi ̄unas, J., Lund, P.D., Mikkola, J. (2021). Energy system resilience–a review. Renewable and Sustainable Energy Reviews, 150, 111476.

35. Vergne, J.-P. (2020). Decentralized vs. distributed organization: Blockchain, machine learning and the future of the digital platform. Organization Theory, 1(4), 2631787720977052.

36. Singh, A., Parizi, R.M., Zhang, Q., Choo, K.-K.R., Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security, 88, 101654.

37. Neha, Gupta, P., Alam, M. (2022). Challenges in the adaptation of IoT technology. A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems, 347–369.

38. Rizi, M.H.P., Seno, S.A.H. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, 20, 100584.

39. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623. IEEE. Hassan, M.U., Rehmani, M.H., Chen, J. (2019).

40. Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, 512–529.

41. Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M. (2021). A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects. IEEE Communications Surveys & Tutorials, 23(2), 1160–1192.

42. Alkadi, O., Moustafa, N., Turnbull, B. (2020). A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions. IEEE Access, 8, 104893–104917.

43. Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 1–16.

44. Sodhro, A.H., Pirbhulal, S., Muzammal, M., Zongwei, L. (2020). Towards blockchain-enabled security technique for industrial Internet of Things based decentralized applications. Journal of Grid Computing, 18, 615–628.

45. Ali, A., Al-Rimy, B.A.S., Tin, T.T., Altamimi, S.N., Qasem, S.N., Saeed, F. (2023). Empowering precision medicine: Unlocking revolutionary insights through blockchain-enabled federated learning and electronic medical records. Sensors, 23(17), 7476.

46. Nair, M.M., Kumari, S., Tyagi, A.K. (2021). Internet of things, cyber-physical system, and data analytics: Open questions, future perspectives, and research areas. In: Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020, pp. 325–339. Springer.

47. Ajakwe, S.O., Kim, D.-S., Lee, J.M. (2023). Drone transportation system: Systematic review of security dynamics for smart mobility. IEEE Internet of Things Journal.

48. Milosch, J., Pearce, N. (2019). Collecting and Provenance: A Multidisciplinary Approach. Rowman & Littlefield Publishers.

49. Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A., Arshad, H., et al. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494.

50. Mohsan, S.A.H., Othman, N.Q.H., Li, Y., Alsharif, M.H., Khan, M.A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intelligent Service Robotics, 16(1), 109–137.

51. Mehta, P., Gupta, R., Tanwar, S. (2020). Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. Computer Communications, 151, 518–538.

52. Alkadi, R., Alnuaimi, N., Yeun, C.Y., Shoufan, A. (2022). Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues. IEEE Access, 10, 14463–14479.

53. Lee, S., Kim, S. (2021). Blockchain as a cyber defense: opportunities, applications, and challenges. IEEE Access, 10, 2602–2618.

54. Garcia-Font, V. (2021). Conceptual technological framework for smart cities to move towards decentralized and user-centric architectures using DLT. Smart Cities, 4(2), 728–745.

55. Li, J., Kassem, M. (2021). Applications of distributed ledger technology (DLT) and blockchain-enabled smart contracts in construction. Automation in Construction, 132, 103955.

56. Iftikhar, Z., Javed, Y., Zaidi, S.Y.A., Shah, M.A., Iqbal Khan, Z., Mussadiq, S., Abbasi, K. (2021). Privacy preservation in resource-constrained IoT devices using blockchain—a survey. Electronics, 10(14), 1732.

57. Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., Forte, M. (2019). Blockchain-enabled supply chain: An experimental study. Computers & Industrial Engineering, 136, 57–69.

58. Weber, R.H. (2010). Internet of things–new security and privacy challenges. Computer Law & Security Review, 26(1), 23–30.

59. Al-Turjman, F., Zahmatkesh, H., Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3), 3677.

60. Karati, A., Biswas, G. (2019). Provably secure and authenticated data sharing protocol for IoT-based crowdsensing network. Transactions on Emerging Telecommunications Technologies, 30(4), 3315.

61. Miraz, M.H., Ali, M. (2018). Blockchain-enabled enhanced IoT ecosystem security. In: Emerging Technologies in Computing: First International Conference, iCETiC 2018, London, UK, August 23–24, 2018, Proceedings 1, pp. 38–46. Springer.

62. Singh, M., Singh, A., Kim, S. (2018). Blockchain: A game-changer for securing IoT data. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 51–55. IEEE.

63. Axon, L. (2015). Privacy-awareness in blockchain-based PKI. CDT Technical Paper Series, 21, 15.

64. Hardjono, T., Pentland, A. (2019). Verifiable anonymous identities and access control in permissioned blockchains. arXiv preprint arXiv:1903.04584.

65. Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal, 6(5), 7702–7712.

66. Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., Zhao, Y. (2018). Edgechain: An edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet of Things Journal, 6(3), 4719–4732.

67. Hong, H., Hu, B., Sun, Z. (2019). Toward secure and accountable data transmission in narrowband Internet of Things based on blockchain. International Journal of Distributed Sensor Networks, 15(4), 1550147719842725.

68. Su, M., Wu, B., Fu, A., Yu, Y., Zhang, G. (2020). Assured update scheme of authorization for cloud data access based on proxy reencryption. Ruan Jian Xue Bao. Journal of Software, 31(5), 1563–1572.

69. Koe, A.S.V., Lin, Y. (2019). Offline privacy-preserving proxy re-encryption in mobile cloud computing. Pervasive and Mobile Computing, 59, 101081.

70. Pise, P.D., Uke, N.J. (2016). Efficient security framework for sensitive data sharing and privacy preserving on big-data and cloud platforms. In: Proceedings of the International Conference on Internet of Things and Cloud Computing, pp. 1–5.

71. Baboolal, V., Akkaya, K., Saputro, N., Rabieh, K. (2019). Preserving privacy of drone videos using a proxy re-encryption technique: poster. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 336–337.

72. Hong, H., Sun, Z. (2018). Sharing your privileges securely: a key-insulated attribute-based proxy re-encryption scheme for IoT. World Wide Web, 21, 595–607.

73. Gong, J., Mei, Y., Xiang, F., Hong, H., Sun, Y., Sun, Z. (2021). A data privacy protection scheme for the Internet of Things based on blockchain. Transactions on Emerging Telecommunications Technologies, 32(5), 4010.

74. Cheryl, B.-K., Ng, B.-K., Wong, C.-Y. (2021). Governing the progress of the Internet of Things: ambivalence in the quest of technology exploitation and user rights protection. Technology in Society, 64, 101463.

75. Alam, T. (2021). IBchain: Internet of Things and blockchain integration approach for secure communication in smart cities. Informatica, 45(3).

76. Liu, L., Li, Z. (2022). Permissioned blockchain and deep reinforcement learning enabled security and energy-efficient healthcare Internet of Things. IEEE Access, 10, 53640–53651.

77. Lashkari, B., Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. IEEE Access, 9, 43620–43652.

78. Anonymous. (Accessed: 15 Jan 2020). NSL-KDD. https://www.kaggle.com/hassan06/nslkdd

Dini, P., Saponara, S. (2021). Analysis, design, and comparison of machine-learning techniques for networking intrusion detection. Designs, 5(1), 9.

RESUME

Mohammed Talib RAHEEM from Iraq, from Al-Diwaniyah Governorate, located in south Iraq. I obtained my primary and secondary certificates in the same city. After that, I received a bachelor's degree in computer engineering from Al-Qadisiyah University. To search for more learning and academic progress, I moved to Karabuk, Turkey, in 2021 to obtain a master's degree.