978-81-19848-73-7

BRIDGING THE BLOCKCHAIN KNOWLEDGE GAP: TACKLING CYBERSECURITY AND DATA PRIVACY CHALLENGES

SUYOGITA SINGH,

SHRI RAMSWAROOP MEMORIAL UNIVERSITY, BARABANKI, UTTAR PRADESH, INDIA, 225003

SATYA BHUSHAN VERMA

SHRI RAMSWAROOP MEMORIAL UNIVERSITY, BARABANKI, UTTAR PRADESH, INDIA, 225003

ANAMIKA AGRAWAL

SHRI RAMSWAROOP MEMORIAL UNIVERSITY, BARABANKI, UTTAR PRADESH, INDIA, 225003

[a]suyogitasingh0885@gmail.com , [b] Satyabverma1@gmail.com , [c] Agrawal.anamika18@gmail.com

KEYWORDS

Blockchain, Federated Learning, Cybersecurity, Data Privacy, Smart Environments, Small and Medium Enterprises (SMEs), Machine Learning, GDPR, Legal Framework, Transparency, Smart Contracts, Distributed Ledger

ABSTRACT

Blockchain technology has emerged as transformative force, holding the potential to revolutionize various industries by enhancing transparency, security, and efficiency. However, a significant knowledge gap hinders its widespread adoption. This paper addresses the challenge of bridging the blockchain knowledge gap, specifically focusing on cybersecurity and data privacy challenges. The authors explore the intersections of blockchain with Federated Learning (FL) and its applications in smart environments. Privacy and security concerns, including vulnerabilities in smart contracts and attempts to exploit blockchain technologies, are examined. The study highlights the limited attention given to security and privacy issues in blockchain scientific journals. The paper provides

Technology (DLT), IoT, Standardization, Security Threats, Privacy Concerns.

a comprehensive analysis of blockchain-based FL techniques, aiming to contribute to the responsible and secure deployment of blockchain technology. The focus extends to cybersecurity, with discussions on machine learning applications, particularly in context of Small and Medium Enterprises and the impact of cyber threats. The paper also delves into data privacy, discussing regulations such as GDPR, legal frameworks, and transparency issues, exemplified by the NHS Test-Trace app. The authors propose a roadmap for addressing these challenges, emphasizing the need for a multidimensional approach involving technology, legal, ethical, and organizational considerations. The ultimate goal is to foster responsible blockchain adoption, contributing to the development of secure and privacy-respecting blockchain ecosystems for societal benefit.

1. INTRODUCTION

Block chain technology is a unique force that has the power to revolutionize whole sectors and change the way that data and transactions are handled. It has a substantial effect on efficiency, security, and transparency in a variety of industries, including supply chain management and banking. However, SMEs, corporations, governmental organizations, businesses, and the general public all have a significant knowledge gap that prevents blockchain from being widely adopted and used effectively [1]. Almost all company strategies in the digital age have undergone substantial modifications as a result of the Internet of Things (IoT) and other advancements in information and communication technologies. One invention that has profoundly changed traditional business paradigms is blockchain technology.

2008 saw the introduction of Bitcoin by Satoshi Nakamoto in a white paper. With its foundation in the blockchain, a communal and unchangeable ledger, Bitcoin functions as a digital money. The current stage of blockchain technology is sometimes compared to the Internet in the middle of the 1990s, when its full potential and worth had not yet been realized. Nonetheless, a few nations have realized the potential of blockchain technology in recent years and have founded research centers focused on this area. Considerable attention has been paid to the use of blockchain in smart environments, such as transportation, medical systems, and industry, in an effort to fully realize its immense potential.

As a result, there have been significant research projects and publications examining the various uses for blockchain technology. Simultaneously, federated learning (FL) has gained popularity as a data analysis method due to its capacity to protect privacy and security, especially in environments that are crucial to safety, including industrial and medical systems [2]. Numerous research endeavours have verified that Federated Learning (FL) has emerged as a critical artificial intelligence technique in smart cities. FL is a particular machine learning technique that allows training parameters to be updated dynamically while local datasets are preserved. In order to accomplish this, data records are divided across specific physical or virtual machines inside each federated domain. This enables quick and safe dataset training, which helps to find undiscovered and unstructured patterns. Collaborative learning with rapid training and testing procedures ensures high accuracy and data privacy and offers various advantages for smart environment design. When combined with FL systems, blockchain technology has the ability to dramatically change data analytics by enhancing security and privacy and managing sensitive and important data. By focusing on security and privacy issues, smart environments can successfully facilitate federated learning by leveraging blockchain as a basic technology. Notably, some studies have examined ways to exploit smart contract weaknesses and hack cryptocurrency like Ethereum and blockchain technology. Privacy concerns such as user identity and transaction quantification are important considerations. While several scholars have recently been engaged in this field of study. The papers concerning the security and privacy of blockchain research papers that are indexed in ISI databases have not undergone a comprehensive, methodical evaluation. For instance, looked at blockchain developments between 2013 and 2018 and recommended using blockchain to address IoT security concerns. [3-5]. Another study focused on security-aware blockchain models in power systems using the Web of Science database. Conti and his team of researchers looked over eight years of Bitcoin news, from 2012 to 2019. Meanwhile, using information from Web of Science and Scopus, Sisi and colleagues concentrated on blockchain strategies and analysis that took energy into account. [6] Nonetheless, there hasn't been much discussion of security and privacy issues in scientific blockchain journals. Given how significant these problems are This category covers a range of methods for the statistical and mathematical analysis of scientific papers as well as an examination of smart surroundings. This thorough study of research studies enables the identification of key issues, emerging trends, and prominent figures in the field of blockchain-based FL techniques, all of which drive future research decisions. The thorough investigation of blockchain-based FL methods in scientific databases aims

to solve privacy and security issues, which are still significant issues in collaborative learning.

In order to bridge the blockchain knowledge gap, this study focuses on two important areas: data privacy and cybersecurity. These difficulties call for an all-encompassing strategy that takes organizational, legal, ethical, and technological aspects into account. The purpose of this paper is to enable stakeholders to make well-informed decisions on the responsible and secure use of blockchain technology by analyzing these issues and providing insights into possible solutions. In order to ensure the responsible adoption of blockchain technology and to fully realize its promise, it is imperative to close the knowledge gap surrounding it. The next parts examine data privacy issues, examine the complexities of blockchain technology, and analyze its consequences for cybersecurity. [8–10] In order to overcome these obstacles, increase awareness, and promote a responsible blockchain adoption culture, the paper offers a road map. In the end, the objective is to contribute to the development of secure, transparent, and privacy-respecting blockchain ecosystems for the benefit of society at large.

1.1.CYBERSECURITY

Cybersecurity encompasses actions to protect computer systems and data from interference or unauthorized access. Examining cybersecurity in relation to the Internet of Things and smart devices prompts questions that necessitate evaluation across different aspects of the digital world. One approach to addressing these challenges is to standardize terminology to better understand the sources of network breaches, detection techniques, and preventative strategies. Artificial intelligence and machine learning can greatly contribute to securing data and thwarting cyber threats.

1.2.CYBERSECURITY AND MACHINE LEARNING

As IT infrastructure expands, ML algorithms like Support Vector Machines become central in processing and managing data. ML applications extend beyond recreational activities, with practical uses in various industries such as identifying fake news, implementing spam filters, detecting online fraudulent activities, and enhancing marketing campaigns. However, the expansion of cyberspace increases the potential attack surface for security threats, emphasizing the influence of human factors on IoT security [11-12]. GDPR, in conjunction with IoT, presents challenges in ensuring the safety and security of these devices.

1.3.CYBERSECURITY AND SMEs

Small and Medium Enterprises in UK face challenges in understanding cybersecurity. SMEs are exploring the use of Intrusion Detection mechanisms, AI, and ML to fortify data security, especially as they integrate physical objects into the digital realm through IoT. The study also investigates the role of governmental policies such as GDPR in facilitating this process [13].

1.4.CYBERSECURITY AND ATTACKS TARGETING SMEs

The study examines the impact in various threat levels posed by attacks like Ransomware, Malware, and Social Engineering on SMEs. It compares Open-Source devices with Commercial Network Intrusion Detection Systems, emphasizing collaboration among businesses, organizations, and government policies to counter cyber threats. [14] The paper explores ML approaches employed by security devices, highlighting the challenges SMEs face in implementing anomaly-based systems.

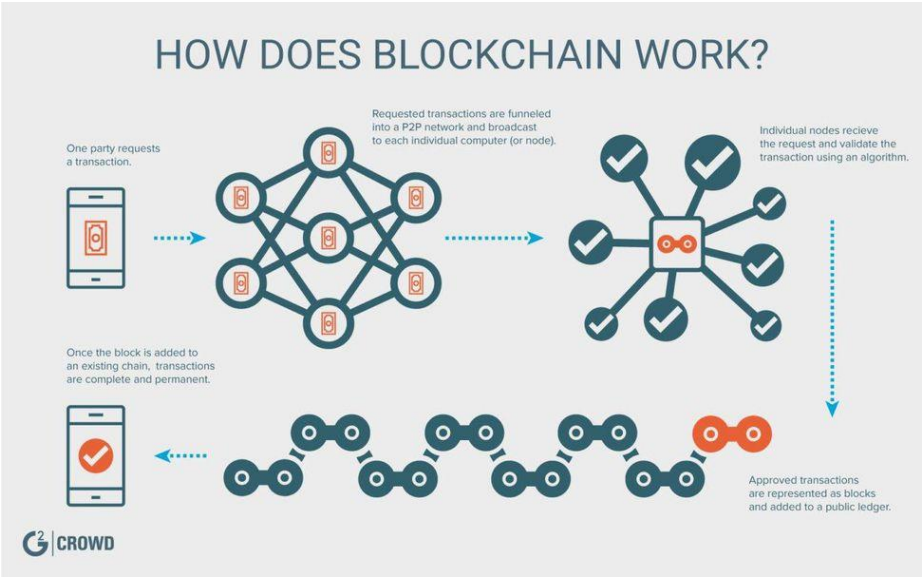

FIGURE 1. BLOCKCHAIN CYBERSECURITY

2. MACHINE LEARNING FOR ENHANCED CYBERSECURITY AGAINST ATTACKS

Understanding Machine Learning (ML) and its applications is an evolving and nuanced field. Each associated with specific underlying algorithms [15].

Applications of Supervised Learning include predictive text in tweets, temperature calculations, and pricing strategies. Unsupervised Learning involves tasks like detecting online fraudulent activities, while Reinforcement Learning is demonstrated in scenarios like video games with reward systems. These ML methodologies rely on algorithms, drawing insights from datasets for development.

The research gauged SMEs' perceptions and awareness of ML and its practical applications. Algorithms like Neural Networks, Support Vector Machines, Deep Networks methods were identified within cybersecurity software used by SMEs. Intrusion Detection and Prevention Systems (IDPS), whether commercial or open-source, rely on ML and AI understanding to protect SME data from sophisticated hackers and bots.

Anomaly detection through ML is highlighted as effective in detecting zero-day attacks compared to traditional methods. Addressing this knowledge gap involves leveraging various devices, including open-source solutions, and promoting community involvement for ongoing security [16].

3. DATA PRIVACY

3.1.GENERAL DATA PRIVACY REGULATION (GDPR)

Data privacy principles are encapsulated in GDPR and the preceding Directive 1995/46/EC, emphasizing that the processing of personal data should designed to serve mankind. Achieving this requires Data Controllers to comply with legal standards, justifying data processing based on necessity and proportionality.

GDPR mandates a Data Protection Impact Assessment for high-risk health data collection, evaluating and mitigating risks. UK and EU data protection laws prioritize cooperation, ethics, transparency, and robust control mechanisms [17-18].

3.2. LEGAL FRAMEWORK FOR DATA PRIVACY IN UK AND EU

The Data Protection Act 2018 (DPA) and General Data Protection Regulation in the UK and EU govern the handling of personal data. These regulations are based on eight key principles that promote fair, accurate, and current data processing. GDPR also introduces additional principles that align with human rights standards for data collection and processing.

3.3. TRANSPARENCY ISSUES: NHS TEST-TRACE APP

There were issues raised regarding the UK Government and NHS X's contact tracing app, specifically in relation to GDPR compliance, health surveillance capabilities, and data storage.

The Joint Committee on Human Rights highlighted worries about the app's rapid development and implementation.

3.4. DATA STORAGE METHOD AND GDPR COMPLIANCE

It is crucial to establish clear methods and solutions for data and storage. While GDPR has improved personal data protection, ongoing research is needed to support users' rights, particularly in areas such as sharing personally identifiable information (PII), collecting location data, sharing child PII, law enforcement access, and data aggregation through advertising and marketing.

3.5. SMART CONTRACT

To strengthen government transparency and public trust, effective data privacy and accountability policies are necessary. Blockchain technology can offer traceability, transparency, vaccine identification, and delivery assurance. Within the realm of Big Data (BD) management, blockchain and smart contracts can improve accountability and transparency.

4. BLOCKCHAIN FOR SECURITY

Blockchain, a prominent Distributed Ledger Technology (DLT), ensures data integrity and exchange in trustless environments. It functions as a decentralized, peer-to-peer distributed ledger, contributing to operational enhancements in diverse sectors like healthcare and finance. [19]

Research explores how blockchain can mitigate emerging cybersecurity threats, proposing frameworks and experimental beta solutions. Platforms like Ethereum and Hyperledger Fabric are used, with Hyperledger Fabric favored for its ease of development. Practical solutions address critical cybersecurity issues, though they require changes to existing infrastructures.

4.1. BLOCK CHAIN AND IOT

In an interconnected IoT world, blockchain features can significantly reduce cyber threats by enhancing cybersecurity. Traditional IT systems, reliant on centralized intermediaries, can benefit from blockchain's decentralized approach.

4.3. DATA STORAGE AND IMMUTABILITY

Distributed Ledger Technology (DLT) systems, exemplified in various domains, ensure system accountability, transparency, and traceability. Research showcases the

potential of DLT in e-commerce, healthcare, security devices, and food products, ensuring sustainability in these areas.

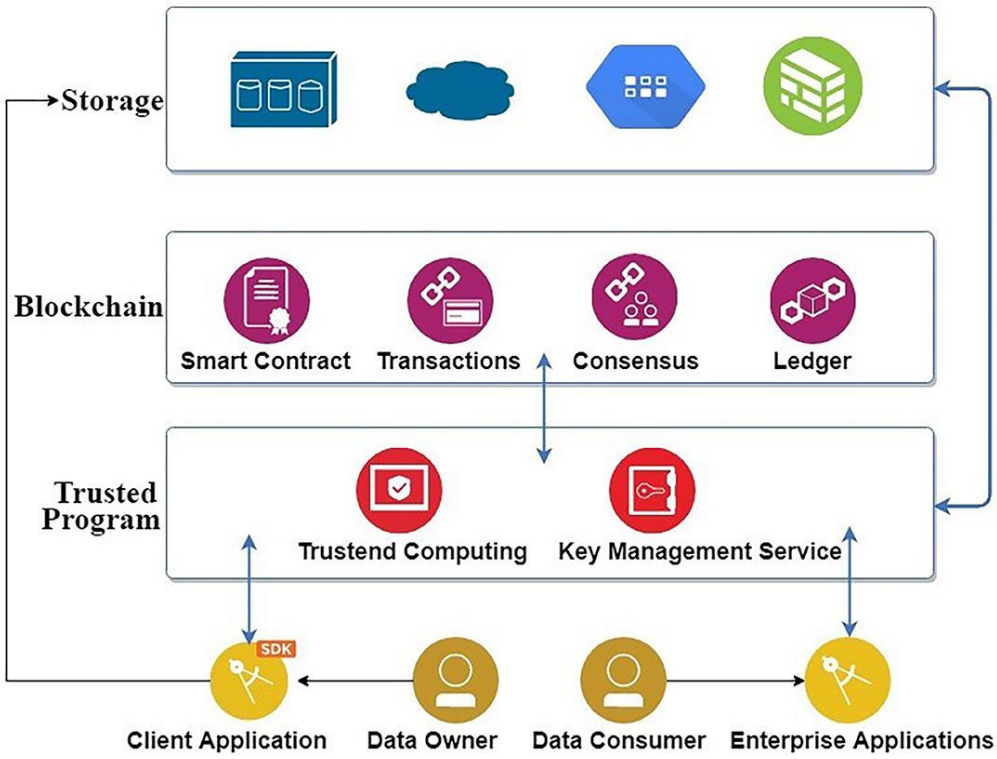

FIGURE 2. A BLOCKCHAIN PLATFORM FOR ENSURING USER CONTROL

5. STANDARDIZATION OF IOT INTERFACE

Ensuring legal data acquisition and processing through IoT smart devices such as smartphones, sensors, tablets, and desktops requires addressing security vulnerabilities in user applications and interfaces, as seen with concerns like cookies. The stability of IoT systems is influenced by various network types, including cellular networks, local and personal area networks (PAN/LAN), low-power wide area networks (LPWAN), and campus area networks (CAN). While some IoT devices provide seamless data access connectivity, different interfaces can create challenges in accurately identifying and processing data. Therefore, implementing a cohesive framework is crucial to establish a standardized system that mitigates security risks through network protocols that define profiles, including essential information like Personal Identification Numbers (PINs), account numbers, and password encryption

5.1. ADMINISTRATOR 1: PUBLIC LAN/WAN/CAN

Administrator 1 holds primary responsibility for implementing network communication protocols to manage and store personally identifiable information (PII), enforce data access control, and integrate cryptographic measures. Small and medium-sized enterprises (SMEs) must adhere to regulatory standards, necessitating the creation of comprehensive and auditable records to demonstrate compliance with best practices. Multiple operational scenarios are simulated using legal precedents to establish preferred principles, standards, and legal frameworks. Additional goals include safeguarding confidentiality, integrity, and availability while minimizing data usage. Stakeholders initiate and validate product blocks to activate wallets, create pseudonymous identities with public and private key pairs, and use these keys for signature and verification processes. Administrator 1 manages network communication policies to regulate user behaviour and specific protocols.

5.2. ADMINISTRATOR 2: PRIVATE LAN NETWORK

In a private LAN network, Administrator 2's job is to use criteria to guarantee network system traffic accountability, transparency, and traceability. Data entry points are made to preserve group integrity, guaranteeing that every user and entry is accessible to everyone who needs to know. In contrast to the data gathered by Administrator 1, the acquired data directs the development and testing of audit and assessment parameters. Administrator 2's insights are essential for evaluating ISO 27001 and Data Protection Act/General Data Protection Regulation (DPA/GDPR) regulations in a variety of operational scenarios and figuring out the best possible operating expenses. Optimal operating system strategies inside a corporation are formed by analysing data, identifying patterns, and aggregating information using tools like Big Data (BD), Analytics, and Machine Learning (ML).

6. CONCLUSION

For small and medium-sized businesses (SMEs) and other organizations, developing a successful cybersecurity plan requires funding from the public and private sectors. This involves teaching management and employees how to successfully use artificial intelligence (AI) and machine learning (ML) into the workplace. From SMEs to government organizations, intrusion detection and prevention strategies can be successful if they highlight and maintain the advantages of cybersecurity and its defences against online threats. However, because different legal, ethical, and consent-based interpretations exist, it is difficult to achieve comprehensive worldwide data security coverage. For the benefit of all, trust in organizations and

technology is crucial, especially when collecting personal information from many locations to assist global resource initiatives.

7. REFERENCES

- Rawindaran N, Jayal A, Prakash E. Artifcial intelligence and machine learning within the context of cyber security used in the UK SME Sector. In: AMI 2021—the 5th advances in management and innovation conference 2021. Cardif Metropolitan University. 2021.
- Wylde V, Prakash E, Hewage C, Jon. Platts. Covid-19 Crisis: Is our Personal Data Likely to be Breached? In AMI 2021 - The 5th Advances in Management and Innovation Conference 2021. Cardif Metropolitan University, 2021.
- Balasubramanian R, Prakash E, Khan I, Platts J. Blockchain technology for healthcare. In: AMI 2021—the 5th advances in management and innovation conference 2021. Cardif Metropolitan University; 2021.
- Gallaher MP, Link AN, Rowe B. Cyber security: economic strategies and public policy alternatives. Chentanham: Edward Elgar Publishing; 2008.
- Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC. A survey of intrusion detection in Internet of Things. J Netw Comp Appl. 2017;84:25–37.
- Are Your Operational Decisions Data-Driven? 2021. https://www. potentiaco.com/what-is-machine-learning-defnition-typesappli cations-and-examples/. Accessed 11 Jul 2021.
- Biju SM, Mathew A. Internet of Things (IoT): securing the next frontier in connectivity. ISSN. 2020. 127 Page 12 of 12 SN Computer Science (2022) 3:127 SN Computer Science
- Cahn A, Alfeld S, Barford P, Muthukrishnan S. An empirical study of web cookies. In: Proceedings of the 25th international conference on world wide web; 2016. pp. 891–901.
- Cressy R, Olofsson C. European SME Financing: An Overview. Small Business Economics, 1997. pp 87–96.
- 10 General Data Protection Regulations (GDPR). https://ico.org.uk/ for-organisations/guide-to-dataprotection/guide-to-the-generaldata-protection regulation-gdpr/. Accessed 16-10-2020.
- Roesch M, et al. SNORT: lightweight intrusion detection for networks. Lisa. 1999;99:229–38.

- Dunham K, Melnick J. Malicious bots: an inside look into the cyber-criminal underground of the internet. Boca Raton: Auerbach Publications; 2008.
- Kabiri P, Ghorbani AA. Research on intrusion detection and response: a survey. Int J Netw Secur. 2005;1(2):84–102.
- Fraley JB, Cannady J. The promise of machine learning in cybersecurity. In: SoutheastCon 2017, IEEE; 2017. pp. 1–6.
- Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2015;18(2):1153–76.
- Machine learning algorithm cheat sheet for azure machine learning designer. 2021. https://docs.microsoft.com/en-us/azure/machi ne-learning/algorithm-cheat-sheet. Accessed 3- Mar 2021.
- Anthi E, Williams L, Rhode M, Burnap P, Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. J Inf Secur Appl. 2021;58:102717.
- Catak E, Catak FO, Moldsvor A. Adversarial machine learning security problems for 6G: mmWave beam prediction use-case. arXiv:2103.07268.2021.
- Guinchard A. Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? Int Rev Law Comput Technol. 2021;35(1):84–97.