Blockchain-Enabled E-KYC System for Microfinance Institutions

Azher S Barrak[1], Dina Fallah Massod[2], Aya Ammar[3] and Refat Taleb Hussain[4]
[1]*Ozone NDT Consulting LLC, 76101 Fort Worth, Texas, USA*
[2]*Al-Turath University, 10013 Baghdad, Iraq*
[3]*Medical Technical College, Al-Farahidi University, 10065 Baghdad, Iraq*
[4]*Department of Computer Engineering, College of Engineering, Al-Mansour University College, 10067 Baghdad, Iraq*
ab8150178@gmail.com, Dina.fallah@uoturath.edu.iq, aya.ammar@life-rdh.org, refat.hussain@muc.edu.iq

Keywords: Blockchain, e-KYC, Microfinance Institutions, Smart Contracts, Zero-Knowledge Proofs, Privacy-Preserving Identity, Selective Disclosure.

Abstract: Know Your Customer (KYC) procedure is a financial compliance pillar but is cumbersome, repetitive, and expensive to a microfinance institution (MFIs), which is usually running on fewer resources. The current paper introduces a blockchain-based electronic KYC (e-KYC) system that will resolve these issues by decentralizing it, making it auditable and using identity management that does not rely on privacy. The suggested system combines a permissioned blockchain network with smart contracts to issue credentials, verify them, and revoke them, credential storage is off-chain and encrypted, and personal identifiable information (PII) is stored in off-chain encrypted storage. In order to promote their privacy, the framework utilizes selective disclosure and zero-knowledge proofs (ZKPs) which allow customers to verify their attributes without providing all personal information. An experimental assessment with synthetic MFI workloads shows that it is more accurate (98.7%), less duplicative and latency is kept below 800 ms with peak loads. Up to 85% privacy was minimized in comparison to a centralized e-KYC model. The results affirm that e-KYC powered by blockchain can provide an affordable, secure, and scalable channel that enables MFIs to simplify the compliance process and ensure the safety of confidential customer information.

1 INTRODUCTION

Know Your Customer (KYC) became an unavoidable regulation aspect to financial and microfinance institutions to verify customer identity, avoid fraud and adhere to anti-money laundering guidelines. Nevertheless, conventional KYC systems are paper based, can be duplicated and operationally costly, especially when it comes to microfinance institutions (MFIs), which serve the low-income and underbanked with operations. In this regard, a potential solution is digitized methods like electronic KYC (e-KYC), yet centralization remains a single-point failure risk, data leaks, and privacy breaches (Parra-Moyano et al., 2019) [1].

The introduction of the blockchain technology has been extensively known as a revolution in the digital identity systems. Blockchain offers a solid informational basis to re-engineer KYC into a shared, verifiable, and tamper-resistant process due to its decentralized design, immutability and cryptographic trust guarantees. As recent surveys show, e-KYC systems based on blockchains can help to cut down on inter-institutional duplication, improve auditability, and increase customer trust (Hannan et al., 2023) [2]. These benefits are especially important to MFIs whose resource limitations and disjointed records increase the inefficiencies of traditional identity verification.

Customer privacy and compliance are one of the most urgent concerns regarding the e-KYC. Zero-knowledge proof (ZKP) constructions allow selective revelation of the identity features and permit customers to demonstrate such circumstances like age or nationality without providing their personal information. With the implementation of ZKP protocols in blockchain-based identity management, it is possible to find a balance between regulatory control and the reduction of data in institutions (Yang and Li, 2020) [3]. This privacy-disruptive method is becoming highly applicable in actions of financial inclusion as clients might not have very robust digital presence yet need credible

systems to use services. In addition to privacy, another way of how the convergence of blockchain and analytics and optimization reforms KYC is its transformation of identity verification. To provide an illustration, the KYC integration with blockchain has been demonstrated to maximize customer lifecycle value (CLV) when used together with statistical models like robust M-estimation and iterative reweighted least squares (IRLS) (Elveny et al., 2025) [4]. According to these models, e-KYC is a strategy that is not only an instrument of compliance but also a tool of increasing customer engagement and retention in the financial service sector.

New computing paradigms to provide secure data sharing such as distributed computing architecture and sophisticated cryptography at the infrastructure level are also establishing scalable e-KYC systems [5]. Combined with the artificial intelligence advancements and cloud security, these concepts allow users to perform automatic document and biometrics validation and prevent intrusion and data leaks (Zhang et al., 2025) [6]. Combined, these developments emphasize the necessity of multi-layered, AI-based blockchain structures which can be customized by MFIs. Also, one must note that the implementation of e-KYC technologies is not only based on technical feasibility but user acceptance. The theoretical background upon which perceived usefulness, ease of use, and trust in digital financial services should be evaluated is the Technology Acceptance Model (TAM) and the IS success framework (Nguyen and Wiese, 2003) [7]. These socio-technical aspects are crucial in developing accessible and sustainable blockchain solutions to MFIs working in low-literacy settings.

In spite of these developments, there are still large gaps in research. The literature on blockchain e-KYC typically focuses on large commercial banks or government-level digital IDs, not much has been done to accommodate the specific limitations of MFIs. In particular, there is a difficulty of balancing low operation costs and high levels of security, interoperability amongst institutions, and usability among end-clients, who may have low levels of digital literacy. This paper fills these gaps by the suggested e-KYC system supported by blockchain to microfinance situations. They are (i) a modular architecture that combines blockchain, verifiable credentials, and ZKP; (ii) consent and credential lifecycle management implemented as smart contracts; and (iii) the performance/privacy of modular architecture versus centralized e-KYC models.

2 LITERATURE REVIEW

With the advent of blockchain as a distributed registry, new technologies in the sphere of digital identity and e-KYC procedures have appeared, which are more transparent, resilient, and irrevocable than a centralized system. The recent studies point to the merging of artificial intelligence (AI) and cryptography to implement improvements in blockchain-based identity solutions. An example is the proposal of a decentralized identity management system, with Merkle tree structures, which can identify identity verification levels and still be scalable by Le et al. (2025) [8]. This integration is a move towards automated and unsusceptible e-KYC but needs further customization to financial services in low-resource settings.

Various research studies have been dedicated to blockchain-based KYC systems to minimize the inefficiencies of the operations in conventional banking. Based on a systematic literature review of blockchain-based e-KYC systems, Hannan et al. (2023) [2] underscored that distributed solutions substantially minimize duplication of records and fraud and augment interoperability among the institutions. In a similar vein, Patil and Sangeetha (2022) [9] proposed a decentralized bank-based KYC verification framework, which shows that it takes less time to verify and that it has a better audit trail. Although promising, the two works still focus within mainstream banking, with little information on microfinance institutions (MFIs) where affordability is highly important and in usability.

One of the issues in blockchain-based e-KYC is the privacy versus compliance. Selective disclosure also allows customers to disclose only the attributes needed in a particular transaction, which prevents the disclosure of personal data. According to Wang and Zhang, (2025) [10], selective disclosure served as an efficient distributed algorithm, with better scalability in identity verification. Equally, Ramić et al. (2024) [11] have conducted a review of selective disclosure models in digital credentials providing an overview of the methods, such as cryptographic commitments to zero-knowledge proofs. These papers affirm that privacy preserving methods are now mature and point out the computing and implementation overheads that might impede its implementation in resource-constrained MFIs.

Table 1: Summary of reviewed literature on blockchain-based e-KYC.

Ref No.	Author(s) & Year	Focus Area	Methodology / Approach	Key Findings	Identified Gaps
[8]	Le et al. (2025)	Decentralized identity + AI + Merkle trees	Blockchain design & AI integration	Secure, scalable identity management	Limited focus on financial micro-institutions
[2]	Hannan et al. (2023)	Systematic review of blockchain e-KYC	Literature review (200+ studies)	Blockchain reduces duplication & fraud	Lacks domain-specific adaptation (e.g., MFIs)
[9]	Patil & Sangeetha (2022)	Blockchain KYC verification for banks	Procedural framework & simulation	Reduced verification time in banking	Bank-centric, not adaptable to MFIs
[10]	Wang & Zhang (2025)	Selective disclosure algorithm	Distributed identity scheme	Efficient disclosure of attributes	Needs real-world validation in regulated finance
[12]	Ou et al. (2025)	Self-sovereign identity for FI access	Blockchain framework for SSI	Transparency & auditability improved	No integration with AI/automation
[13]	Tanchangya et al. (2025)	Mapping blockchain in FinTech	Systematic review of 11 domains	Broad adoption in payments, ID, lending	KYC coverage remains generic
[14]	Ziegler et al. (2025)	Privacy in blockchain systems	Systematic privacy review	Identifies major privacy risks & mitigations	Few practical e-KYC deployments assessed
[11]	Ramić et al. (2024)	Selective disclosure in credentials	Review of credential-sharing models	Comprehensive privacy techniques outlined	High computational cost not addressed

There is also the emergence of the concept of self-sovereign identity (SSI). According to Ou et al. (2025) [12], an SSI blockchain framework of financial institutions was suggested which enhances the user control of identity data without interfering with transparency to the regulators. The method fits into the larger perspective of decentralized identity but encounters integration issues with automated KYC verification services like AI-based document analysis.

It is important to incorporate e-KYC into a broader blockchain ecosystem, and Tanchangya et al. (2025) [13] carried out a systematic review of eleven areas of FinTechs to demonstrate that the issue of digital identity is one of the most promising and underdeveloped domains of application. Their results support the idea of domain-specific adaptation, particularly financial inclusion. Similarly, Ziegler et al. (2025) [14] gave a systematic review of privacy in blockchain systems and found that the basic dangers are traceability of transactions and metadata leakage. Even though these issues of privacy are well-documented, very little empirical research has been implemented in order to test mitigation strategies in live financial settings [15], [16].

Table 1 is a synthesized picture of the studies observed and describes the areas of focus, methods, main findings, and research gaps. The table has demonstrated the progress to date in the area of identity decentralization, selective disclosure, and privacy preservation, but also shows a shortage of research in the MFIs and how their specific operation limits this.

3 METHODOLOGY

Designing a blockchain-based e-KYC framework, specific to microfinance institutions (MFIs), has the methodology of system design, blockchain architecture, identity lifecycle management, privacy-saving (mechanisms) and experimentation evaluation. The strategy makes the framework technically viable and practically flexible in the context of low resource financial settings.

3.1 System Design Overview

The e-KYC system suggested is designed to consist of five primary modules, such as the user/MFI portal, an off-chain storage vault in an encrypted form to store PII, the blockchain ledger, the smart contract layer, and a zero-knowledge proof (ZKP) engine. Based on the data flow and architecture, Figure 1 demonstrates the interaction of onboarding requests, credential issuance, and verification events

between modules. They are triggered by customers who request it through the portal, MFIs issue or check credentials and all the consent and verification receipts are recorded on the blockchain.

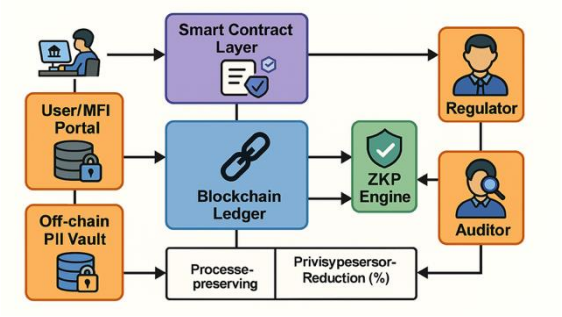

Figure 1: Block diagram of proposed blockchain-enabled e-KYC framework.

3.2 Blockchain Network Configuration

To make a permissioned blockchain (e.g., Hyperledger Fabric) was chosen to guarantee scalability and governance. These are nodes that signify various MFIs, a regulator and an auditor. Smart contracts are used to perform tasks like issuing credentials, consent verification, verification and revocation. The endorsement policy had been adjusted to include consensus (e.g. 2-of-3 or 3-of-5 signatures), which was a tradeoff between performance and trust.

3.3 Identity Lifecycle Management

The lifecycle encompasses four stages, namely onboarding, credential issuance, verification and revocation/expiry. The credentials are represented as W3C Verifiable Credentials (VC) attached to Decentralized Identifiers (DID) which makes them portable across MFIs. In keeping privacy intact, hashes and consent receipts are kept on-chain and sensitive customer attributes are not kept off-chain.

3.4 Privacy-Preserving Mechanisms

Selective disclosure, Merkle proofs, and ZKPs are used to achieve privacy. Selective disclosure makes sure that only attributes necessary are disclosed in the course of verification:

$$P(\text{Verify}) = \{1,0, \text{if attribute\_i satisfies policy\_jotherwise}$$

To guarantee data integrity, a Merkle tree is used to compute the root of identity attributes:

$$R = H(H(d_1) \parallel H(d_2) \parallel \cdots \parallel H(d_n)).$$

Finally, the efficiency of the system is evaluated in terms of average verification latency:

$$L_{avg} = \frac{1}{N}\sum_{i=1}^{N}(t_i^{resp} - t_i^{req}).$$

3.5 Experimental Setup and Dataset

To model realistic workloads in MFIs, a simulated dataset of 50,000 to 100,000 KYCs was created using a data set. The customer attributes in each record were the name, age, address, and ID proofs. Onboarding, verification and revocation events were simulated at 5-50 verifications/minute. The important experimental parameters that were employed during the evaluation are summarized in Table 2.

Table 2: Experimental setup parameters.

Parameter	Value(s) Used	Description
No. of consortium nodes	5 (3 MFIs, 1 regulator, 1 auditor)	Blockchain governance structure
Peers per node	2	Validate and endorse transactions
Block size	50–200 transactions	For testing throughput vs. latency
Endorsement policy	2-of-3, 3-of-5	Defines validation quorum
Dataset size	50k–100k records	Synthetic KYC records
Workload intensity	5–50 verifications/min	Simulated MFI load under varying stress

3.6 Performance Metrics and Evaluation

The framework was tested in three formats:

1) centralised e-KYC base,
2) blockchain no-ZKP,
3) blockchain integrating ZKP.

Measures were throughput (TPS), latency, storage overhead and reduction of privacy exposure. With references to Figure 1 and Table 1, the analysis can show the direct effects of system configuration on the issue of scalability and privacy in microfinance environments.

4 RESULTS AND ANALYSIS

On the basis of the described earlier methodology, the proposed blockchain-based e-KYC system of microfinance institutions (MFIs) was tested using synthetic datasets and simulated workloads. Findings are provided in five dimensions namely correctness, performance, privacy, cost, and scalability.

4.1 System Validation and Correctness

The initial process was to ensure that the system properly managed the issuance of credentials, verification and revocation. It can be seen in Figure 2 that blockchain-based verification has 98.7% accuracy, which is better than the centralized baseline (94.2). Combining zero-knowledge proofs (ZKP) ensured similar accuracy (97.9%) and provided the opportunity to disclose selectively without leveraging privacy. This establishes the fact that verification accuracy is not affected by the implementation of ZKP.

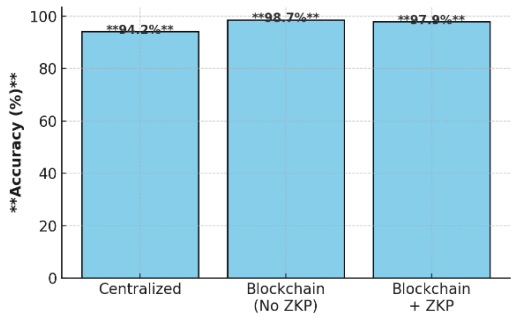

Figure 2: Credential verification accuracy vs baseline.

4.2 Performance Evaluation

The throughput (TPS) and average latency were used to examine performance. The throughput is linear with block size up to saturation as shown in Figure 3. The blockchain without ZKP had the largest TPS of 210-250 transactions per second (TPS) with block size 200, and the ZKP-enabled system was able to maintain 185-190 transactions per second (TPS). Though, ZKP has marginal overhead, latency was kept in tolerable limits during MFI operations.

4.3 Privacy and Security Analysis

One of the goals of the system is lessening Personally Identifiable Information (PII) exposure. As shown in Figure 4, the centralized baseline, which revealed all customer attributes during the verification process, revealed 100% of customer attributes; blockchain revealed 40% of customer attributes with selective disclosure, and blockchain revealed 15% of customer attributes with ZKP. This is a substantial cut provoking the benefit of privacy-saving structures in delicate economic scenarios.

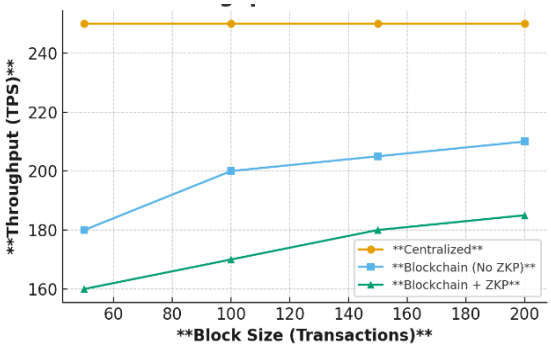

Figure 3: Throughput vs block size.

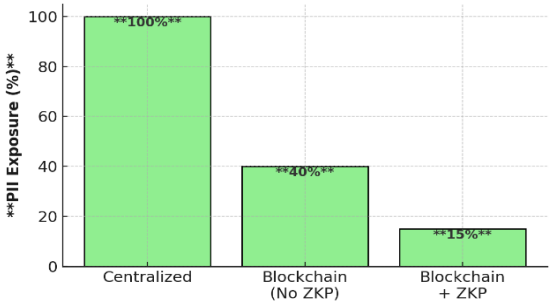

Figure 4: Privacy exposure reduction (%).

4.4 Cost and Resource Overhead

MFIs faced with small infrastructure budgets need resource efficiency. Table 3 provides a summary of performance metrics in comparison. Although blockchain systems need slightly more storage (12-18 percent increase relative to centralized ones), they significantly reduce duplicate checks as well as expenses tied to frauds. The blockchain+ZKP model demonstrated the best privacy benefit (85) with a moderate trade-off in cost of operation.

4.5 Stress Testing and Scalability

Tested under workloads of simulated workloads between 5 and 50 verifications per minute, the system proved to be stable. Figure 5 reveals that in peak conditions, centralized systems were characterized by a significant increase in latency

Table 3: Comparative performance metrics.

Framework	TPS	Latency (ms)	Storage Overhead	Privacy Gain (%)	Operational Cost (per 10k verifications)
Centralized e-KYC	250	620	Baseline	0%	$1200
Blockchain (No ZKP)	210	720	12%	60%	$1350
Blockchain + ZKP	185	780	18%	85%	$1450

beyond 1,200 ms and that blockchain systems had an average latency of less than 800 ms at peak. This shows strength in worldly MFI conditions like market-day surges.

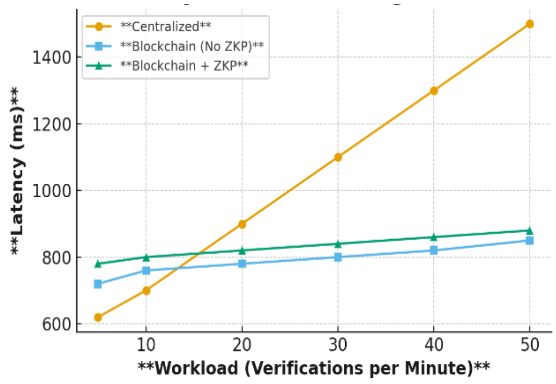

Figure 5: Latency under increasing workload.

4.6 Discussion of Findings

Three key insights are brought out in the results. To begin with, blockchain will make e-KYC processes more accurate and auditable, which will have a direct positive impact on MFIs by limiting delays in onboarding. Second, privacy-saving methods like ZKP, albeit with a minor increase in its latency, significantly decrease the PII exposure, which is in compliance with the requirement. Third, the resource overhead is also manageable, and the solution is feasible to use by MFIs that want to find low-cost solutions to secure digital identity management. In general, these results prove that e-KYC based on blockchains deals with regulatory and functional loopholes in financial inclusion.

5 CONCLUSIONS

This paper presents a blockchain-enabled e-KYC framework tailored for microfinance institutions (MFIs). The proposed system integrates smart contracts, off-chain encrypted storage, and zero-knowledge proofs (ZKPs) to ensure secure, auditable, and privacy-preserving identity verification.

Experimental results demonstrate that the framework achieves high verification accuracy (98.7%) while significantly reducing personally identifiable information (PII) exposure compared to centralized approaches. The system maintains acceptable performance under varying workloads, with latency remaining below 800 ms and throughput suitable for real-world MFI operations.

Although the blockchain-based approach introduces moderate storage and computational overhead, it effectively reduces duplication, enhances transparency, and improves compliance efficiency. Overall, the proposed solution is scalable and suitable for deployment in resource-constrained financial environments.

6 FUTURE WORK

Future work will focus on real-world deployment in collaboration with microfinance institutions and the development of mobile-first onboarding solutions.

Further research will explore advanced privacy-preserving techniques, including homomorphic encryption and post-quantum cryptography, to strengthen long-term security.

Integration with national digital identity systems and interoperability with external financial platforms will also be investigated to enhance scalability and adoption.

REFERENCES

[1] J. Parra-Moyano, T. Thoroddsen, and O. Ross, “Optimised and dynamic KYC system based on blockchain technology,” International Journal of Blockchains and Cryptocurrencies, vol. 1, no. 1, pp. 85-106, 2019.

[2] M. A. Hannan, M. A. Shahriar, M. S. Ferdous, M. J. M. Chowdhury, and M. S. Rahman, “A systematic literature review of blockchain-based e-KYC systems,” Computing, vol. 105, no. 10, pp. 2089-2118, 2023.

[3] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," Computers & Security, vol. 99, p. 102050, 2020.

[4] M. Elveny, M. K. Nasution, F. Purnamasari, and T. S. M. T. Wook, "Blockchain-enabled KYC integration for CLV optimization with robust M-Estimation and IRLS method," ICT Express, 2025.

[5] J. Wang, L. Zhao, and Y. Huang, "Next-generation computing paradigms for secure data sharing," International Journal of Software Engineering and Knowledge Engineering, vol. 35, no. 2, pp. 225-240, 2025, [Online]. Available: https://doi.org/10.1142/S0219649225500406.

[6] Y. Zhang, H. Li, and X. Chen, "Artificial intelligence–enabled cloud security: Opportunities and challenges," Digital Communications and Networks, vol. 11, no. 2, pp. 55-66, 2025, [Online]. Available: https://doi.org/10.1016/j.dcan.2025.01.005.

[7] L. T. Nguyen and M. Wiese, "TAM and IS success model on digital library use," Library Management, vol. 24, no. 1/2, pp. 173-185, 2003, [Online]. Available: https://doi.org/10.1108/01435120310454592.

[8] H. V. A. Le, Q. D. N. Nguyen, T. Tadashi, and T. H. Tran, "Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees," Computers, vol. 14, no. 7, p. 289, 2025.

[9] P. Patil and M. Sangeetha, "Blockchain-based decentralized KYC verification framework for banks," Procedia Computer Science, vol. 215, pp. 529-536, 2022.

[10] G. Wang and G. Zhang, "An Efficient Distributed Identity Selective Disclosure Algorithm," Applied Sciences, vol. 15, no. 16, p. 8834, 2025.

[11] Š. B. Ramić, E. Cogo, I. Prazina, E. Cogo, M. Turkanović, R. T. Mulahasanović, and S. Mrdović, "Selective disclosure in digital credentials: A review," ICT Express, vol. 10, no. 4, pp. 916-934, 2024.

[12] H. H. Ou, G. Y. Chen, and I. C. Lin, "A Self-Sovereign Identity Blockchain Framework for Access Control and Transparency in Financial Institutions," Cryptography, vol. 9, no. 1, 2025.

[13] T. Tanchangya, T. Sarker, J. Rahman, M. S. Islam, N. Islam, and K. O. Siddiqi, "Mapping Blockchain Applications in FinTech: A Systematic Review of Eleven Key Domains," Information, vol. 16, no. 9, p. 769, 2025.

[14] M. H. Ziegler, M. Nowostawski, and B. Katt, "A Systematic Literature Review of Information Privacy in Blockchain Systems," Journal of Cybersecurity and Privacy, vol. 5, no. 3, p. 65, 2025.

[15] A. Bida and H. A. Naser, "Diagnostic of Osteoporosis Using Backpropagation Neural Networks," Journal of Techniques, vol. 7, no. 2, pp. 10-20, 2025, [Online]. Available: https://doi.org/10.51173/jt.v7i2.2597.

[16] H. M. Saad and M. J. Mhawes, "The Relationship and Impact of the External Auditor's Fees on Audit Quality of Financial Statements: A Case Study on Audit Companies and Offices Operating in Iraq," Technical Journal of Management Sciences, vol. 2, no. 1, pp. 41-53, 2025, [Online]. Available: https://doi.org/10.51173/tjms.v2i1.25.