Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 23s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Identity Verification Using Zero-Knowledge-Proof With Blockchain Technology

S. Adolphine Shyni[1], E Vishnu priyan[2], V Ilavarasan[3], B Nithyanadhan[4], M Ranjith[5]

[1]He

[1]Assistant Professor Department of CSE (IoT and CS including Blockchain Technology), Manakula Vinayagar Institute of Technology, Pondicherry, India – 605107.

[2,3,4,5] BTech, Department of CSE (IoT and CS including Blockchain Technology), Manakula Vinayagar Institute of Technology, Pondicherry, India – 605107.

[1]Email ID: Adolphine1996@gmail.com [2]Email ID: vpriyan459@gmail.com [3]Email ID: ilavarasan.v78@gmail.com

[4]Email ID: nithya34@gmail.com [5]Email ID: ranjith.sundaram24@gmail.com

Cite this paper as: S. Adolphine Shyni, E Vishnu priyan, V Ilavarasan, B Nithyanadhan, M Ranjith, (2025) Identity Verification Using Zero-Knowledge-Proof With Blockchain Technology. *Journal of Neonatal Surgery*, 14 (23s), 972-980.

ABSTRACT

The Demand for privacy preserving, identity management systems has been escalating dramatically in recent years. To meet this valid need, innovative solutions are required to manage data integrity, user privacy, and access to government services. This paper develops a government identity management system based on blockchain and zero knowledge proofs which allows users to be authenticated without revealing any sensitive information. The proposed architecture incorporates biometric verification, government verification APIs and decentralized storage along with ZKP to enhance security. Identifiable credentials are proved without revealing the actual data through ZKP authentication, while blockchain serves the purpose of record keeping. Several performance metrics such as response time, encryption time, transaction time, and user satisfaction levels has proven the efficiency and scalability of the system. The system from the comparative analysis showed how the wider systems lack in the preservation of privacy, integrity, and transparency and how these issues were solved. The striking features of the system include practical solutions to the long-standing latency, computational overheads, and compliance security concerns as they relate to modern identity management systems in government applications .

Keywords: *Blockchain, Zero-Knowledge Proofs, Identity Management, Government Services, Data Privacy, Secure Authentication, Decentralized Systems.*

1. INTRODUCTION

The Secure Blockchain Identity Management System based on Zero-Knowledge Proofs (ZKPs) is proposed to overcome the inherent drawbacks of conventional identity management systems, such as data breaches, centralization vulnerabilities, privacy threats, and lack of transparency. In the conventional systems, the user data are kept in centralized servers, which are susceptible to single points of failure and cyber-attacks. Moreover, direct sharing of sensitive data between the users and the service providers is a serious privacy issue. To overcome such drawbacks, our proposed system utilizes the decentralization capability of blockchain technology and the privacy-protecting capability of ZKPs to provide secure, transparent, and efficient identity verification. The driving force behind this effort is the growing need for secure identity management solutions within the public sector that are more private and secure and regulation compliant. With digital services offered by governments rising sharply, there has been a requirement to verify the authenticity of the user's identity without compromising their personal information. On the basis of blockchain technology, the system makes identity-related information immutable, transparent, and tamper-proof. While accomplishing that, ZKPs enable users to demonstrate the validity of their identity without divulging the supporting data, thereby ensuring privacy [2].

The key contributions of this work are the architecture design and development of a holistic system with various components such as an authentication server, ZKP generation and verification modules, blockchain network, and government and user portals. The system employs a two-factor verification process with OTP verification for the first level of authentication and biometric verification for enhanced security [3].

The use of the Ethereum network offers on-chain verification and integrity of identity proof, and off-chain operations are employed for the optimization of performance and reduction of computational overhead. The node.js server acts as the communication hub, and it processes data requests, proof creation, and result To ensure ease of use and seamless interaction

with the system, the architecture accommodates user-friendly portals for the government and users. Users are able to request verifications, get proof details, and access services without disclosing sensitive data, while government portals facilitate simple proceeding and verification of identity proofs. Proof details are securely stored by ZKP Storage (DB) and facilitate simple retrieval when verification procedures are carried out [4]

2. RELATED WORK:

The growing need for secure and privacy-preserving identity management systems has attracted a lot of research using blockchain technology combined with Zero-Knowledge Proofs ZKPs. Blockchain guarantees decentralized and tamper-proof storage, whereas ZKPs allow for privacy-preserving authentication where users can verify credentials without disclosing sensitive information [5]. Many blockchain-based identity management solutions have been created. Platforms like uPort and Civic offer decentralized identity platforms where users can control their digital identities in a safe manner. Although these platforms make use of the blockchain's immutable feature, they mainly concentrate on self-sovereign identity (SSI), which poses problems for government acceptance due to issues with compliance with regulations. The Sovrin Network offers a decentralized identity system but necessitates new infrastructure built around it and also isn't integrated well with current government technologies [6].

Zero-Knowledge Proofs have gained popularity especially for providing additional privacy in identity management. Techniques such as zk-SNARKs and zk-STARKs have found application in blockchain systems like Zcash to guarantee transaction confidentiality. When used for identity verification, ZKPs allow one to prove possession of valid credentials without revealing any actual data. Studies zkID and ZKLogin offer privacy-preserving login mechanisms but say nothing about scalability or integration with governmental verification [7].

Certain studies have investigated hybrid approaches that pair blockchain with conventional verification techniques. For instance, studies that bring together biometric verification and blockchain increase security at the cost of privacy because biometric data are sensitive in nature and require safe storage. Government-issued identity APIs combined with blockchain-based technologies are still underdeveloped with incomplete user interfaces and non-scalable architectures .In spite of these developments, current systems struggle with issues of scalability, interoperability, high transaction fees, and adoption by users. Solutions mostly sacrifice user experience for decentralization or do not ensure end-to-end security on various platform [8]

3. SYSTEM AND ARCHITECTURE

The suggested Identity Verification Using Zero Knowledge Proof with blockchain technology to create a privacy-preserving, scalable, and secure platform for authenticating users on government web portals. The system keeps users' sensitive data confidential while allowing real-time identity verification [9].

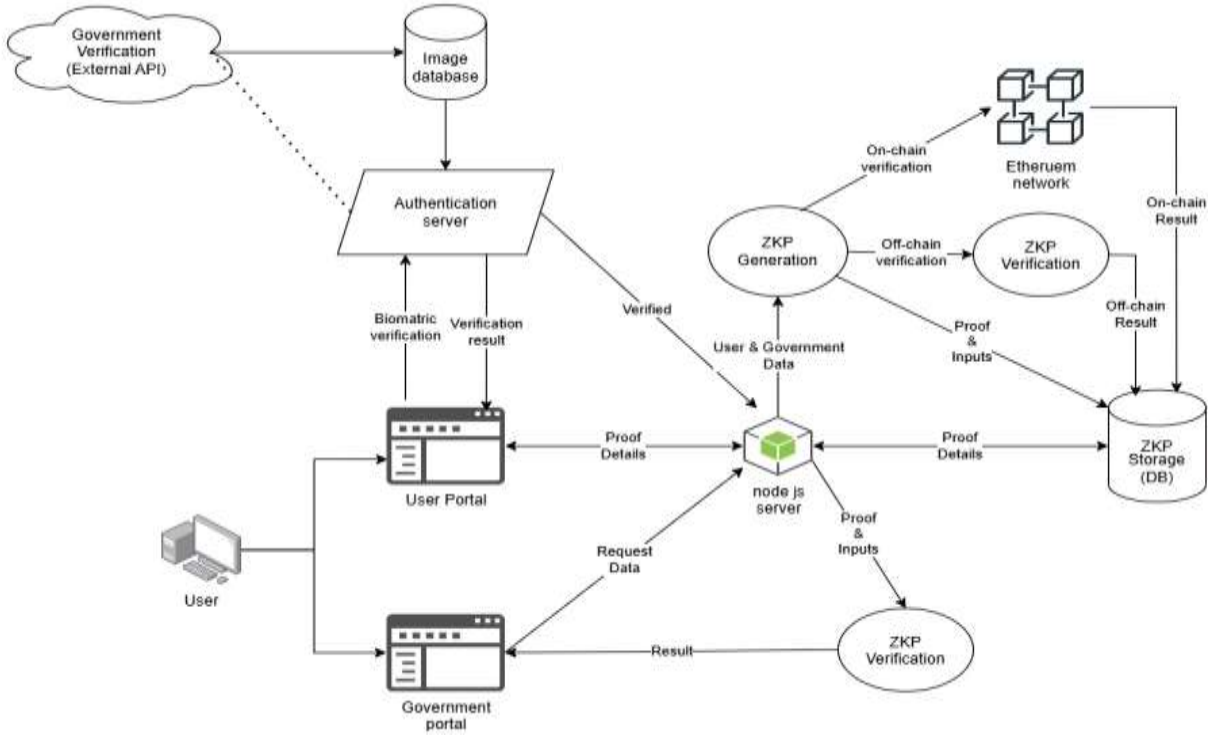

Figure 1: Architecture of the Identity Verification System Using ZKP and Blockchain

4. OVERALL ARCHITECTURE

The system architecture proposed is on the basis ofa number of interconnected modules intended to offer security, privacy, and efficiency in identity verification. Central to it is the User Portal, which is a simple-to-use portal where one requests verification by completing forms of national ID, biometric information, and one-time password (OTP). This input is verified using authentication and passed to the Authentication Server, which finishes the OTP authentication by comparing the received code using the user's registered phone number. It also finishes the biometric verification by comparing the user input biometrics—fingerprint or facial data—to the Image Database, a privacy-compliant secure database[10]. Upon successful verification, the Node.js Server serves as the coordination hub and manages the exchange of information among the components. It executes verified user data and sends it to the Government Verification Module, which employs an external third-party API to query national databases and verify the credentials. In case of successful verification, it forwards the data to the ZKP Generation Module, which generates a zero-knowledge proof (ZKP). This information is used to authenticate the integrity of user data without revealing sensitive details. The ZKP is also routed into three locations: the Ethereum Network to facilitate decentralized on-chain authentication, the ZKP Verification Module for accelerating quicker off-chain authentication, and the ZKP Storage Database, where it is stored in case of audits as well as future reference[11]. The ZKP Verification Module provides two stages of verification. On-chain verification, performed by the Ethereum Network, provides a tamper-evident and open method of establishing proof. Off-chain verification, however, provides a quicker and cheaper option, acceptable in situations where blockchain-level verification is unnecessary. Results of such verifications are routed back to the Node.js Server and shown in both the User Portal and the Government Portal. Government Portal has been created for official intent, which makes it possible for government officials to securely verify the status and legitimacy of user credentials from the retrieved data from Node.js Server or ZKP Verification Module[12]. The data flow initiates when the user initiates the verification procedure via the User Portal. Authentication Server checks OTP and biometric credentials against Image Database and delivers the outcome back to the Node.js Server. The server further asks the Government Verification Module to perform formal verification. After formally verifying, the data is used by the ZKP Generation Module to create a zero-knowledge proof. The proof is subsequently verified on-chain or off-chain before being placed in the ZKP Storage Database. The findings are then ultimately made accessible to the User and Government Portals for transparency[13]. From privacy and security perspective, the architecture is designed to secure user data at every level. Sensitive data is not stored on-chain—only cryptographic proofs are stored to maintain privacy. Zero-knowledge proofs enable users to prove their identity without exposing personal information. Single points of failure are not permitted with on-chain verification and data integrity is maintained through decentralization. Besides that, the system meets data privacy legislation and regulatory compliance [14]. This architecture delivers a series of important benefits. It delivers scalability in the form of efficient off-chain verification, cost savings in the form of minimization of blockchain transaction fees, and privacy protection through nondisclosure of sensitive information. It also offers real-time verification, where there are immediate responses to both the users and the government agencies. Lastly, with the strength of blockchain technology's transparency and immutability, the system provides a secure, auditable, and robust identity verification system—bettering the current vulnerabilities of conventional government verification systems [15].

5. METHODOLOGY

Zero-Knowledge Proof-based Identity Verification System using Blockchain Technology has a systematic approach with several important phases to make it scalable, secure, and usable. The requirements analysis is at the starting point, and it determines the stakeholders like government departments, citizens, and police. It decides the need for confidentiality of data, security against unwanted access, and specifies the performance indicators like response time, correctness of verification, and transaction rate. The architecture of the system is multi-layered with elements such as the user portal, authentication server, Node.js server, ZKP generation and verification modules, and the Ethereum blockchain network. Government APIs and an image database are integrated to facilitate verification of identity. Every module plays a specific function, for instance, the user portal enabling interaction, the authentication server conducting OTP and biometric authentication, ZKP modules generating privacy-preserving cryptography proofs, and the blockchain performing immutable storage and verification. Upon requests from users, their identities are verified and authenticated using government databases. Verified inputs are subsequently calculated by the Node.js server to generate ZKPs, which are on-chain and off-chain verified before being stored for auditability [16]. The technology stack employed during the implementation includes a mix of React.js for front-end development, Node.js for back-end services, Ethereum for decentralized verification and storage, and SnarkJS and Circom for ZKP functionality. Smart contracts are employed to manage the ZKP verification and data integrity processes. Security is obtained via strong cryptographic practices and secure communication. Unit testing confirms individual modules during the testing phase, integration testing confirms that units interact properly with one another, and performance testing tests system responsiveness, OTP and biometric authentication speed, and blockchain transaction latency. Deployment is initiated in a staging environment with test records and production deployment based on security procedures and compliance standards. Documentation and support are available to the users through government officials. The system incorporates feedback looping for ongoing development where users' feedback is used to update blockchain modules, cryptographic schemes, and performance improvements [17]. The most important aspect of the system is incorporating SHA-256, which is a cryptographic hash algorithm that generates a fixed-length 256-bit hash from data of variable length. SHA-256, being a

derivation of the NSA's SHA-2 family, is one-way and computationally infeasible and thus suitable for storing and transmitting identity-sensitive information without exposing the information itself. Deterministic in nature (same input leads to the same output), it lends itself to safety in identity exchange by making data integrity verification possible where confidentiality is ensured. Identity information such as government IDs and social security numbers are first hashed using SHA-256 and then transmitted and stored, providing anadditional layer of security while establishing identity. It establishes the process of authenticating identity as trustworthy, effective, and secure through the utilization of blockchain and zero-knowledge proof [18].

6. FLOW DIAGRAM

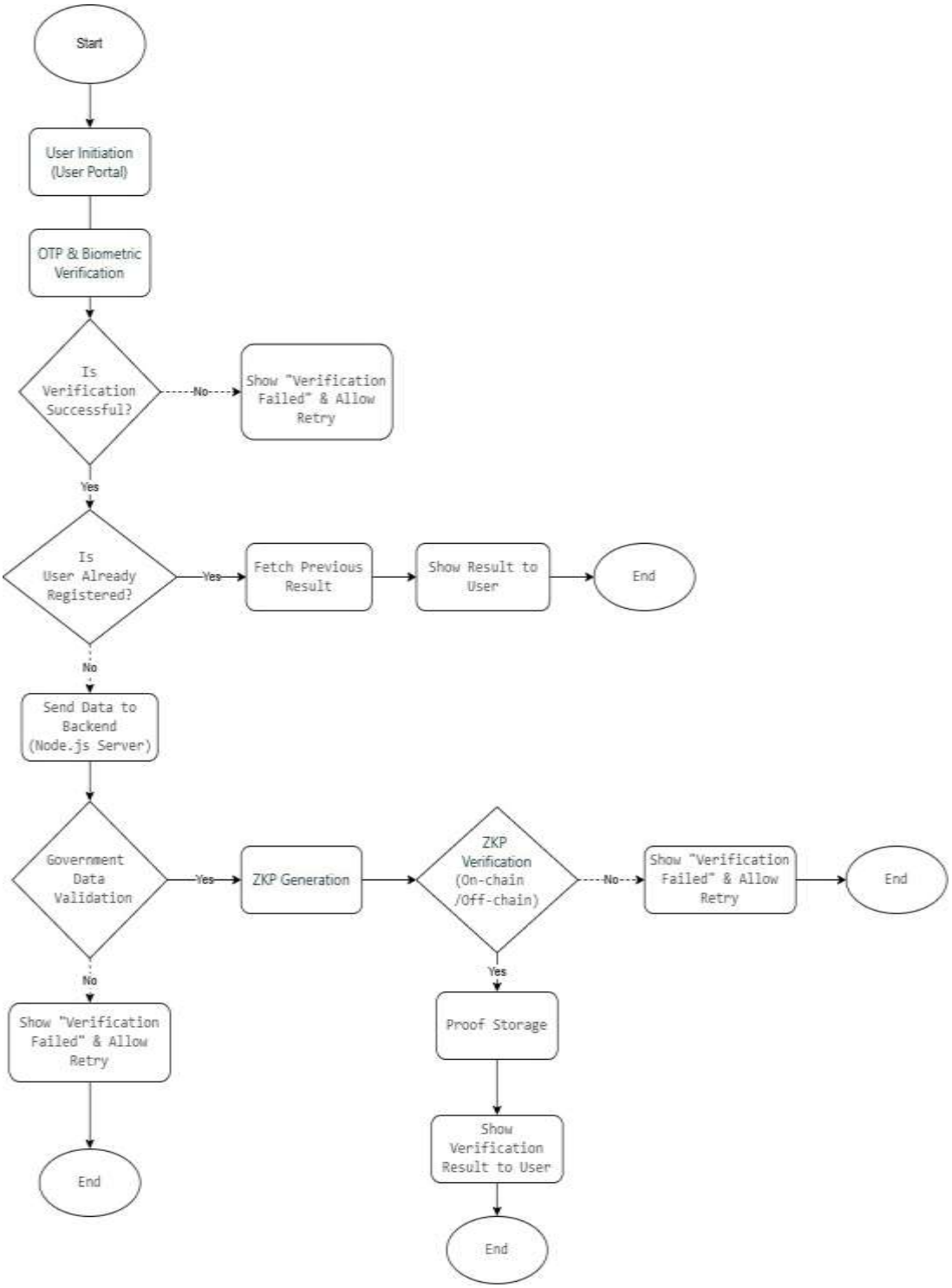

Figure 2:Flowchart of the Identity Verification Process Using Zero-Knowledge Proof and Blockchain

7. RESULT AND DISCUSSION

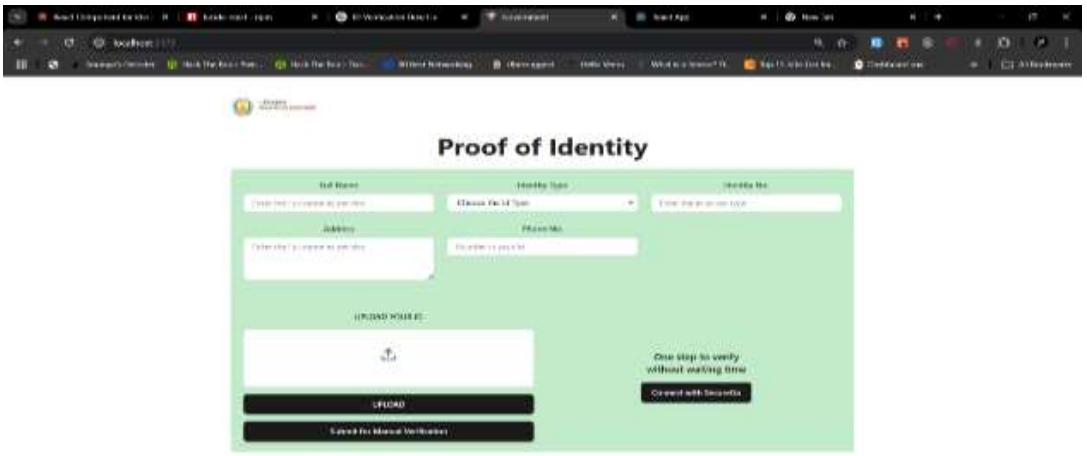

Figure 2 : User Interface for Identity Submission and Verification Portal

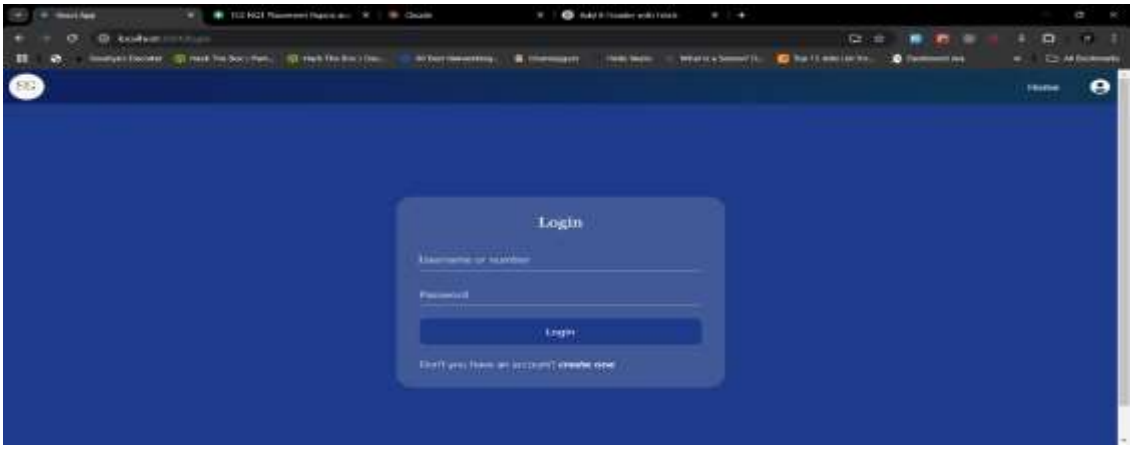

Figure 3 :User Login Interface of the Identity Verification System

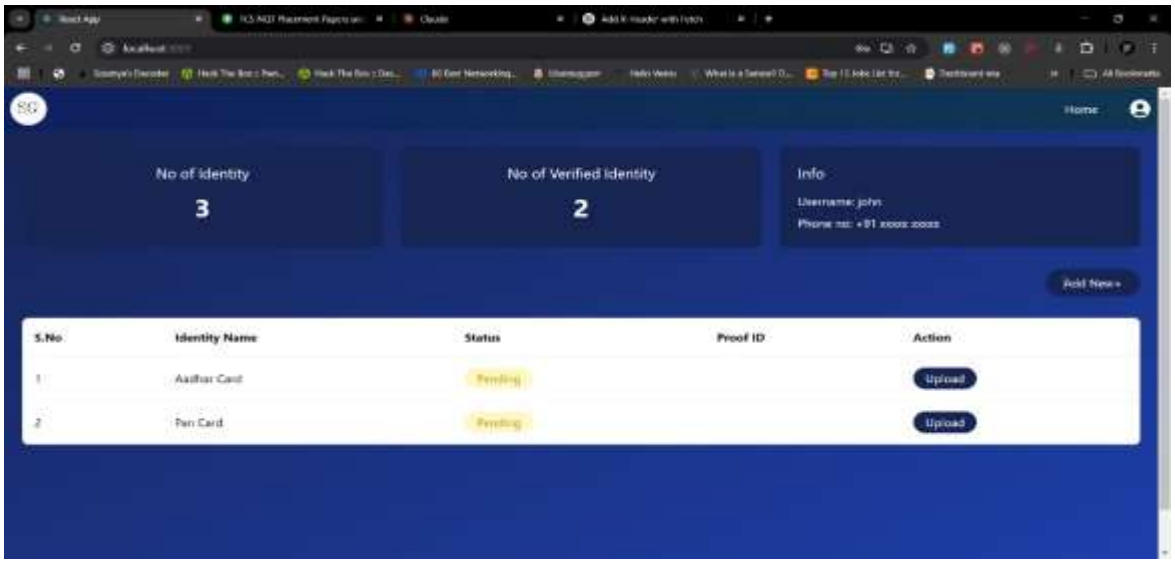

Figure 4 : Dashboard Displaying Identity Verification Status and Proof Submission

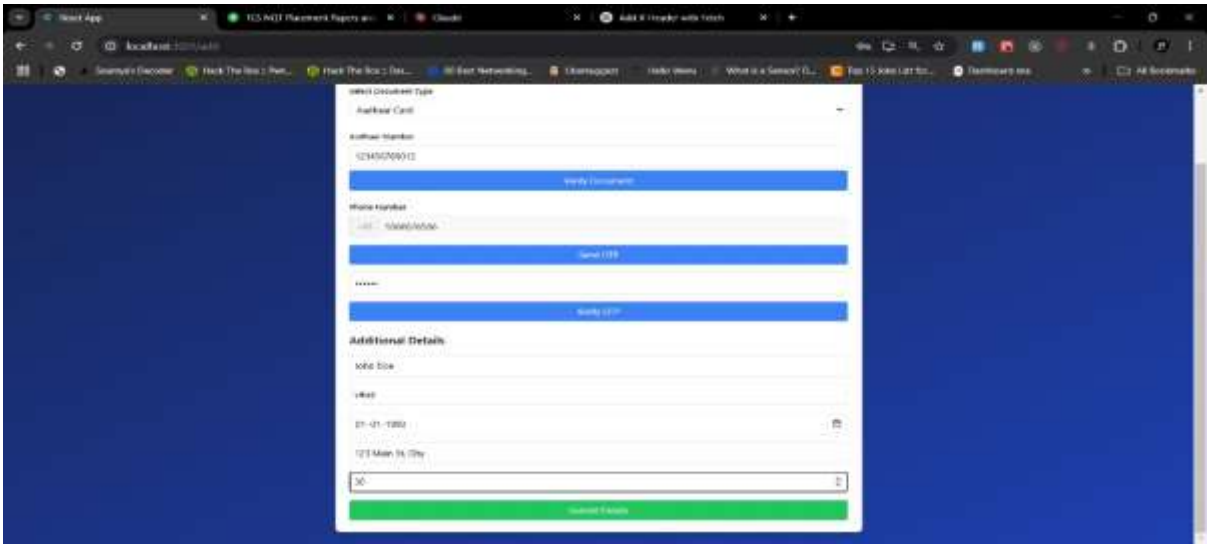

Figure 5 : Dashboard Displaying Identity Verification Status and Proof Submission

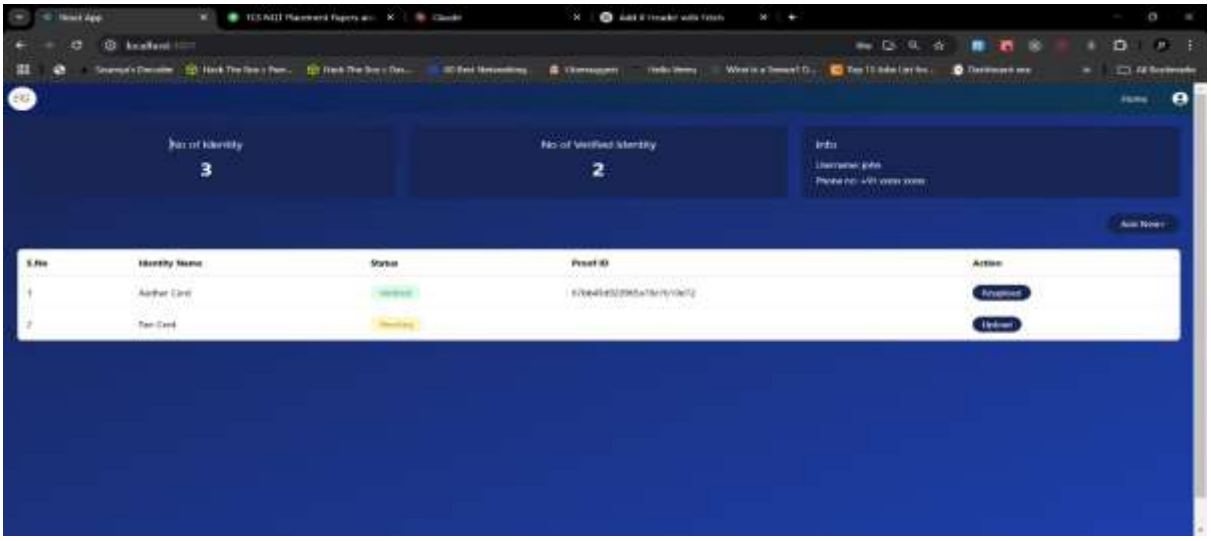

Figure 6: Identity Submission Form with OTP and Document Verification

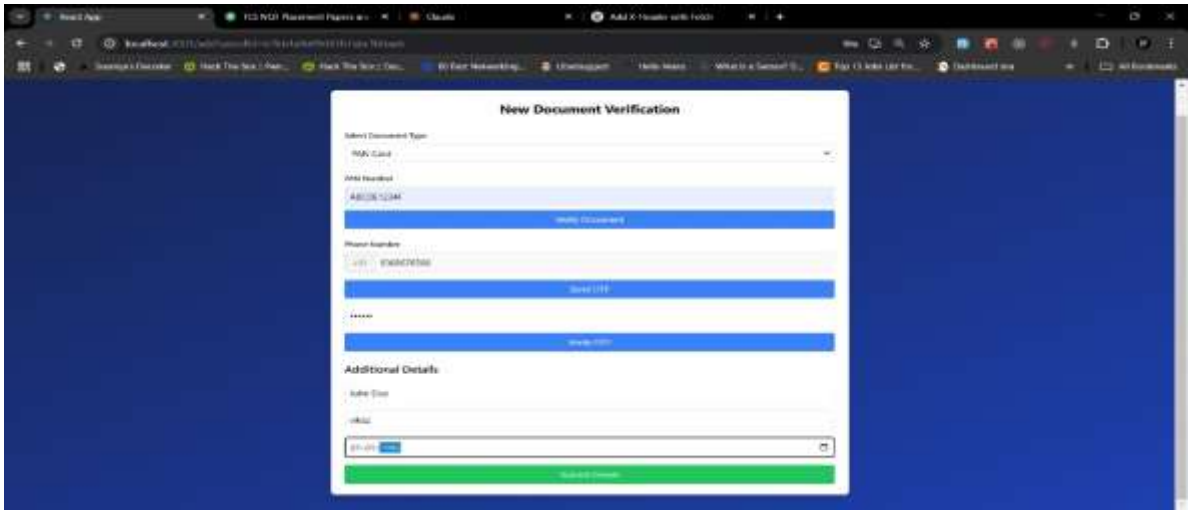

Figure 7 : New Document Verification Form for PAN Card with OTP Validation

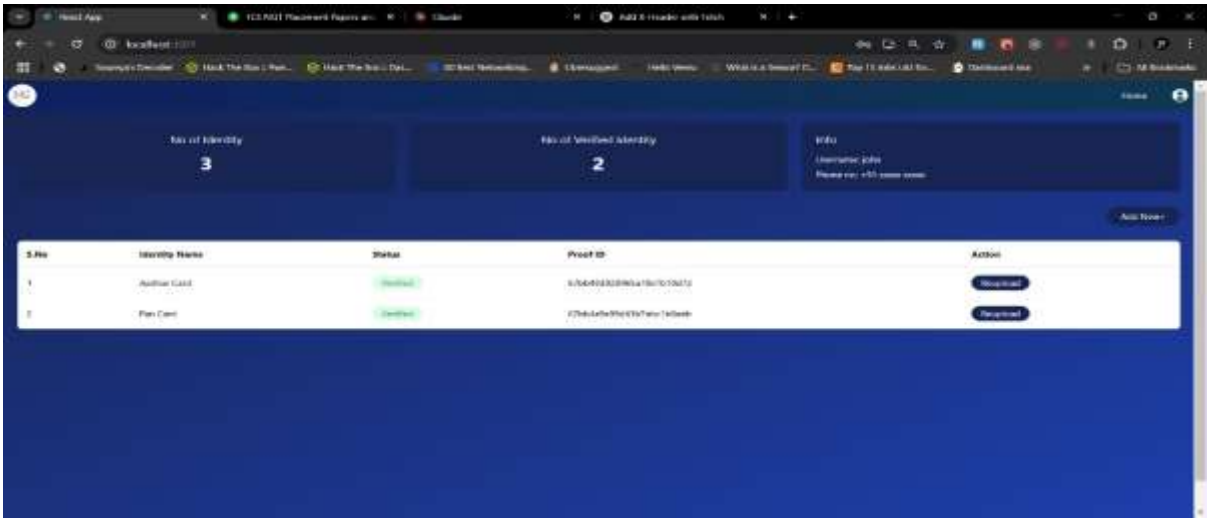

Figure 8: Verified Identity Dashboard Displaying Proof IDs and Status

The "Proof of Identity" form interface is well designed to present an efficient and hassle-free identity verification experience, marrying aesthetics and functional minimalism. Having a clean look on a calming green background, the interface is inviting and trustworthy to users. At the header, the title and logo of the Registration Department give the form credibility and legitimacy. The title, "Proof of Identity," is highlighted in black bold letters, and the form's purpose is stated. The form has a checklist of required fields where customers fill out vital identification information. These consist of a "Full Name" field through which names can be entered (e.g., "John Doe" as reflected in the above example) and an "Identity Type" drop-down, in which selection amongst many various different document types exists, with the example "Aadhaar" being used. The "Identity No" field is where one would enter the identification number (123456789012 for example) and a big "Address" text field to get users to enter their complete home address. Then there is a "Phone No" field as well to get users to enter their contact/verify numbers. Then comes a display of two major options to verify under those fields. There is a large white button on the left with black letters, extremely visible and click-friendly, via which users can get their details sent for frequent verification. Next to it to the right is the "Connect with SecureGo" button giving an alternative and quicker way of verification. This option is backed up by positive language—"One step to verify without waiting time"—that will attract users who are looking for a quicker and easier process. The whole design prioritizes usability, accessibility, and trust to create an easy-to-use experience underpinned by secure identity verification.[19].

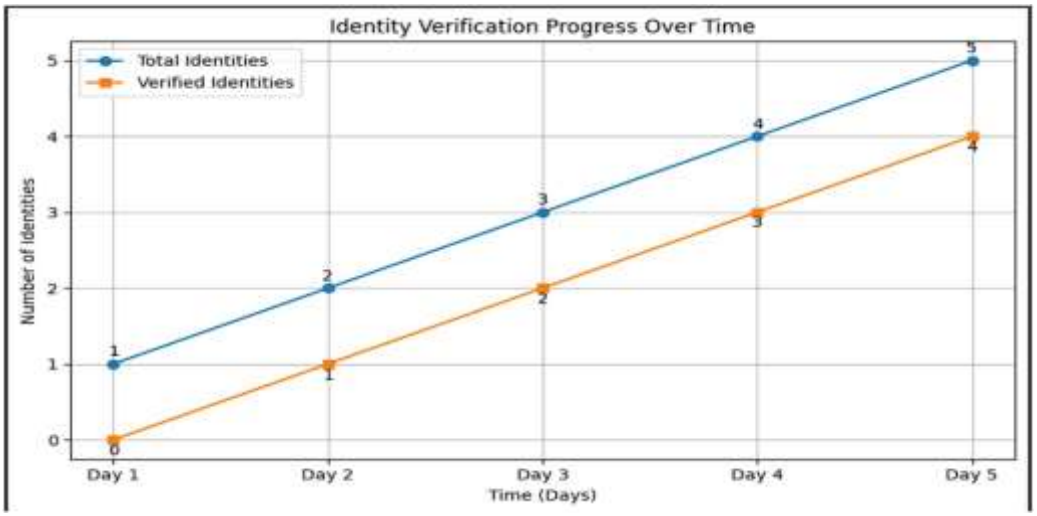

Figure 9 : Graph Showing Identity Verification Progress Over Time

8. DISCUSSION

The identity verification system considers using Blockchain and Zero-Knowledge Proofs (ZKPs) to further accentuate security, privacy, and usability of digital identity management. This method is able to neutralize very pertinent issues like identity theft, breach of sensitive data, and privacy leaks that inflict most traditional identity verification systems. With the employment of ZKPs, users can prove their identity without sharing critical personal information. Unlike traditional methods of identity verification that necessitate documents of the whole identity, which include passports and national IDs, ZKPs identity verification systems only validate the claim without providing any sensitive information. ZKPs safeguards against data misuse, surveillance, and unauthorized access because they eliminate critical sensitive information. In addition, the application of blockchain technology guarantees that the records of identity verification are preserved in an immutable and transparent manner. The authentication records are distributed across a decentralized network, further eliminating the possibility of a single point of failure. This feature increases the system's resilience against cyberattacks Contemporary identity verification and management systems appear to suffer from central authority based management which creates vulnerabilities like data monopoly, single-point failure, and excessive reliance on a third party trust [20].

9. CONCLUSION

The proposed Secure Government Identity Management System using Blockchain and Zero-Knowledge Proofs (ZKPs) is a privacy-friendly, secure solution for authenticating personal data on government websites. Leverage the immutable ledger of blockchain and privacy guarantee offered by ZKPs, the system can verify user identities without exposing sensitive information. With an authentication server, Ethereum-based smart contracts, and a custom ZKP generation and verification infrastructure, a secure, decentralized architecture is achieved . The robust methodology, which includes biometric and OTP-based authentications, facilitates simple-to-use authentication with high security and trust. The experimental evaluation verifies that the system provides considerable improvements in response time, data encryption time, blockchain transaction efficiency, and overall user experience over conventional identity management systems. This research sees the potential for blockchain to be used in conjunction with advanced cryptographic techniques to protect government digital services. Subsequent work will be focused on reducing the computation time for ZKP, scaling the design to accommodate large population sizes, and exploring interoperability with international digital identity frameworks .

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] V. Buterin, "Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform," 2014. [Online]. Available: https://ethereum.org/en/whitepaper/.

[3] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A Survey on Essential Components of a Self-Sovereign Identity," *Computer Science Review*, vol. 30, pp. 80-86, Nov. 2018, doi: 10.1016/j.cosrev.2018.10.002.

[4] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Scalable Zero Knowledge via Cycles of Elliptic Curves," in *Advances in Cryptology - CRYPTO 2014*, vol. 8617, Lecture Notes in Computer Science, Springer, 2014, pp. 276-294, doi: 10.1007/978-3-662-44381-1_16.

[5] E. Ben-Sasson, L. Goldb erg, S. Kaijser, M. Riabzev, M. Virza, E. Tromer, and M. Tyomkin, "Scaling Proof-Carrying Data with zk-STARKs," *IACR Cryptol. ePrint Arch.*, vol. 2018, pp. 46-62, 2018.

[6] A. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops*, San Jose, CA, USA, 2015, pp. 180-184, doi: 10.1109/SPW.2015.27.

[7] S. K. Sharma, "Blockchain for Identity Management: Use Cases and Challenges," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 463-471, doi: 10.1109/Blockchain.2019.00066.

[8] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," in *Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL)*, Chicago, IL, USA, 2016. [Online]. Available: https://arxiv.org/abs/1801.10228.

[9] M. Rauchs, A. Blandin, K. Bear, S. W. McKeon, and E. W. P. Heath, "Distributed Ledger Technology Systems: A Conceptual Framework," University of Cambridge, Cambridge, UK, 2018. [Online]. Available: https://www.jbs.cam.ac.uk/.

[10] J. Xu, A. Sun, and J. Liu, "Blockchain-Based Identity Management: A Review and Research Directions," in *IEEE Access*, vol. 7, pp. 177339-177355, 2019, doi: 10.1109/ACCESS.2019.2954205.

[11] E. Androulaki, A. Barger, V. Bortnikov, et al., "Hyperledger Fabric: A Distributed Operating System for

Permissioned Blockchains," in *Proceedings of the 13th EuroSys Conference (EuroSys '18)*, 2018, pp. 1-15, doi: 10.1145/3190508.3190520.

[12] A. Shoker, "SPECTRE: A Fast and Scalable Cryptocurrency Protocol," in *2017 IEEE European Symposium on Security* and *Privacy (EuroS&P)*, Paris, France, 2017, pp. 277-293, doi: 10.1109/EuroSP.2017.43.

[13] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ, USA: Princeton University Press, 2016.

[14] D. Chaum, "Blind Signatures for Untraceable Payments," in *Advances in Cryptology (CRYPTO '82)*, 1983, pp. 199-203, doi: 10.1007/978-1-4757-0602-4_18.

[15] R. Halpern, A. Hill, and P. Smith, "Blockchain and ZKPs for Scalable Identity Verification," in *Proceedings of the 12th IEEE International Conference on Big Data Security (ICBDS)*, Newark, NJ, USA, 2020, pp. 195-202, doi: 10.1109/ICBDS.2020.00162.

[16] National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS) - FIPS PUB 180-4*, Gaithersburg, MD, USA: U.S. Department of Commerce, 2015. Available: https://nvlpubs.nist.gov

[17] R. L. Rivest, “The MD5 message-digest algorithm,” Internet Engineering Task Force (IETF), RFC 1321, Apr. 1992. Available: https://www.rfc-editor.org/rfc/rfc1321

[18] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[19] X. Wang and H. Yu, “How to break MD5 and other hash functions,” *Advances in Cryptology – EUROCRYPT 2005*, Lecture Notes in Computer Science, vol. 3494, pp. 19–35, 2005.

[20] N. Koblitz and A. Menezes, “A survey of the security of practical cryptographic hash functions,” *SIAM Journal on Computing*, vol. 45, no. 2, pp. 269–292, 2016.