IJITCE

ISSN 2347- 3657

# International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

# BLOCKCHAIN-BASED DIGITAL IDENTITY VERIFICATION SYSTEM FOR E-COMMERCE

Akash Hanumantha [1], Koganti Linga Pardhiv [2] Ubidi Bhupal [3], Mr. Kishor Golla[4]
[1,2,3]UG Scholar, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[1]akashhanumantha14@gmail.com, [2]kogantilingapardhiv@gmail.com, [3]bubidhi@gmail.com,
[4]kishorgolla1984@gmail.com

## *Abstract:*

A blockchain-based digital Identity verification systems play a crucial role in ensuring secure and trustworthy digital transactions by authenticating users before granting access to services. They prevent fraud, unauthorized access, and identity theft, which are prevalent in online platforms, particularly in e-commerce. Historically, identity verification was based on physical documents such as passports, national IDs, and driver's licenses, requiring in-person verification. With technological advancements, centralized digital verification systems emerged, utilizing databases managed by governments, financial institutions, and third-party authentication providers. However, centralized models face issues such as data breaches, identity theft, and a lack of user control over personal data. Examples include banking KYC (Know Your Customer) systems, email-based authentication, and social media logins, all of which store user data on vulnerable centralized servers. The need for a more secure, transparent, and user-controlled verification process has led to the adoption of blockchain technology. Growing concerns over data privacy, increasing cyber threats, and the inefficiency of centralized authentication systems drive the development of a blockchain-based identity verification system. Centralized models expose users to identity fraud, unauthorized access, and privacy violations, as they depend on third parties to store and manage sensitive information. The proposed system leverages blockchain's decentralized nature to store identity data securely, ensuring immutability and transparency. Users maintain full control over their information through cryptographic keys, reducing reliance on intermediaries. Smart contracts facilitate authentication without exposing personal data to external entities, preventing fraud and unauthorized access. Blockchain-based verification enhances security, eliminates single points of failure, and provides a seamless authentication mechanism for e-commerce platforms, strengthening trust between buyers and sellers while reducing operational risks and costs.

***Keywords: Blockchain-based digital identity, decentralized authentication, secure verification, data privacy, smart contracts, fraud prevention, user control, immutability, transparency, e-commerce security, cyber threat mitigation.***

## 1.INTRODUCTION

The project focuses on developing a blockchain-based digital identity verification system designed for e-commerce platforms to address increasing concerns over identity theft, fraud, and data breaches. By leveraging the decentralized and immutable nature of blockchain technology, the system aims to provide a secure, transparent, and efficient method for verifying user identities during online transactions. Unlike traditional systems that rely heavily on centralized databases and third-party verification services, the proposed solution utilizes a decentralized ledger and cryptographic techniques, offering users greater control over their personal data while reducing the risk of cyberattacks and enhancing trust in e-commerce platforms.

Current identity verification methods often face significant challenges, including weak password-based authentication, manual verification processes, and centralized data storage that increases vulnerability to data breaches. This research is motivated by the need to enhance security, streamline verification operations, empower users with control over their data, and comply with increasingly stringent data protection regulations. By integrating smart contracts, the proposed system automates verification processes, minimizes reliance on intermediaries, and ensures transparency, leading to improved operational efficiency and customer satisfaction across digital commerce ecosystems.

The blockchain-based identity verification system has wide-ranging applications beyond e-commerce, including online banking, healthcare, government services, educational institutions, and telecommunications. It can protect sensitive information, streamline user onboarding, and facilitate secure access to services across industries. With rising cyber threats and growing demands for privacy and security, implementing this system is crucial for safeguarding user identities, meeting regulatory requirements, and improving the overall digital experience in various sectors.

## 2. LITERATURE SURVEY

Pascual et al., 2018 [1] examined the increasing complexity of identity fraud, highlighting the vulnerabilities in centralized identity verification systems. The study emphasized that traditional authentication methods, such as passwords and OTPs, are inadequate against evolving cyber threats. The rise of synthetic identities and data breaches further demonstrates the need for robust identity verification mechanisms. The report suggests adopting advanced security frameworks to mitigate fraud risks in digital transactions.

Zyskind et al., 2015 [2] proposed a blockchain-based approach to decentralizing privacy and securing personal data. The study introduced a protocol that enables users to maintain control over their data while ensuring privacy and security through cryptographic techniques. By leveraging smart contracts, users can grant or revoke access to their identity information without relying on intermediaries. This decentralized model addresses data leakage risks associated with centralized identity verification systems.

Azaria et al., 2016 [3] developed MedRec, a blockchain-based system for managing medical data access and permissions. The study demonstrated how blockchain ensures data integrity, security, and accessibility while granting patients control over their medical records. Although focused on healthcare, the principles of decentralized authentication and secure identity management are applicable to e-commerce identity verification. The research highlights blockchain's ability to eliminate third-party control while maintaining transparency and security.

Chen & Zhu, 2017 [4] explored the use of blockchain technology for personal archive services, analyzing its potential benefits and challenges. Their research highlighted blockchain's ability to create immutable records, ensuring the integrity of identity verification processes. They also addressed scalability concerns and the necessity for efficient consensus mechanisms to maintain a balance between security and performance. Their findings emphasize blockchain's ability to revolutionize digital identity management in multiple sectors, including e-commerce.

Do & Ng, 2017 [5] investigated a blockchain-based secure data storage system with private keyword search functionality. Their research provided insights into how blockchain ensures data confidentiality while allowing selective data retrieval through cryptographic techniques. The system prevents unauthorized access to sensitive identity information, making it highly relevant for identity verification in online platforms. Their study reinforces the significance of decentralized solutions in mitigating security risks associated with personal data management.

Mudliar et al., 2018 [6] presented an integrated framework for national identity verification using blockchain technology. The study outlined how government-issued digital identities stored on a decentralized ledger enhance security, reduce fraud, and improve accessibility. By eliminating the need for centralized control, blockchain-based national identity systems provide users with greater autonomy over their personal information. Their research supports the development of decentralized identity verification systems for e-commerce applications.

Soliman et al., 2015 [7] proposed DIV, a decentralized identity validation system for social networks, emphasizing the importance of self-sovereign identity. The research demonstrated how blockchain enhances identity authentication, preventing impersonation and unauthorized access. By utilizing smart contracts and cryptographic authentication, their system ensures secure and transparent identity verification without relying on centralized authorities. Their work highlights blockchain's ability to improve trust and security in digital interactions.

Elmansori et al., 2017 [8] analyzed the factors influencing e-government adoption, focusing on user concerns regarding data privacy and security. The study found that trust in digital services plays a critical role in adoption rates, with centralized identity systems often failing due to data breaches and inefficiencies. Their research suggests that blockchain-based identity management can enhance security, transparency, and citizen trust in online services.

Elmansori et al., 2018 [9] conducted a critical review of e-government service adoption, emphasizing challenges in centralized identity verification systems. Their study identified data breaches, lack of transparency, and security concerns as major barriers to adoption. The findings support the transition toward decentralized identity verification, reducing the risks associated with unauthorized access and data manipulation.

Al-Shuaili et al., 2019 [10] examined critical factors affecting the implementation of e-government systems, highlighting security and privacy as primary concerns. The research emphasized how blockchain could address these challenges by providing a transparent and tamper-proof identity verification framework. By decentralizing control, blockchain enhances user trust and mitigates risks associated with identity fraud. Their findings align with the need for decentralized identity management in e-commerce.

Yaga et al., 2018 [11] provided a comprehensive overview of blockchain technology, discussing its applications in identity verification and secure transactions. Their research outlined the benefits of decentralization, immutability, and cryptographic security in preventing unauthorized access and fraud. The study reinforced blockchain's role in enhancing digital identity authentication, particularly in online commerce and financial transactions.

Mahendran et al., 2018 [12] explored trusted computing and security mechanisms for protecting digital assets. Their research highlighted the importance of cryptographic authentication in safeguarding identity data from cyber threats. They emphasized that decentralized systems offer a more secure alternative to traditional identity verification models by eliminating single points of failure and enhancing data integrity. Their study supports the integration of blockchain in secure identity verification frameworks.

## 3. PROPOSED METHODOLOGY

The proposed system integrates blockchain technology with AI-driven cybersecurity to enhance identity verification and protect user data in a decentralized manner. The system eliminates the reliance on centralized databases, reducing risks associated with data breaches, fraud, and unauthorized access. Blockchain provides an immutable and secure method for managing digital identities, while AI strengthens cybersecurity by identifying anomalies, predicting potential threats, and providing real-time protection. The following steps outline the process for developing this integrated system.

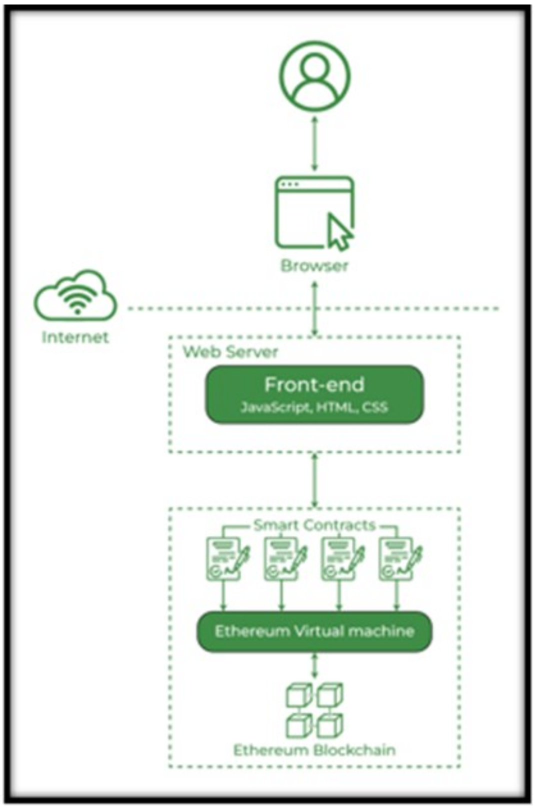


**Figure 1: Block Diagram.**

The proposed methodology typically includes the following key components:

**Requirements**: In this phase, the system's requirements are gathered, including the need for a decentralized identity verification system, integration with blockchain, and cybersecurity features. This includes choosing the appropriate blockchain platform (e.g., Ethereum) and selecting AI cybersecurity tools to monitor and protect the network.

**Developing Blockchain Technology**: The next step involves designing and developing the smart contract that will store user identities on the blockchain. The smart contract will handle user registrations, logins, and data access control. The blockchain will ensure that all actions are securely recorded and that personal data cannot be tampered with or altered.

**Developing User Interface**: A user-friendly interface is created to allow users to interact with the blockchain-based system. This interface includes features such as account creation, login, file uploads, and data access requests. The user interface needs to be simple and intuitive to encourage widespread adoption.

**Integrating Blockchain into User Interface**: The blockchain backend is integrated into the user interface. Smart contract functions are called through the frontend, allowing users to interact with the blockchain seamlessly for actions such as signing in, registering, or downloading data. This integration ensures that users can experience decentralized identity verification without needing to understand the underlying technology.

**Testing the Application**: Finally, the application is thoroughly tested to ensure its security, functionality, and user experience. Automated tests, manual tests, and penetration tests are conducted to validate that the system works as expected, and AI-driven cybersecurity algorithms are effective at preventing attacks.

**Applications:**

The blockchain-based digital identity verification system can be applied in:

- **E-Commerce Platforms**: Securing user accounts and transactions.
- **Online Banking**: Verifying customer identities for financial services.
- **Healthcare Services**: Protecting patient information and access to medical records.
- **Government Services**: Facilitating secure access to public services and benefits.
- **Educational Institutions**: Authenticating student identities for online learning platforms.
- **Travel and Hospitality**: Streamlining check-ins and reservations with secure identity verification.
- **Telecommunications**: Enhancing customer onboarding and service access.
- **Supply Chain Management**: Verifying identities within logistics and distribution networks.

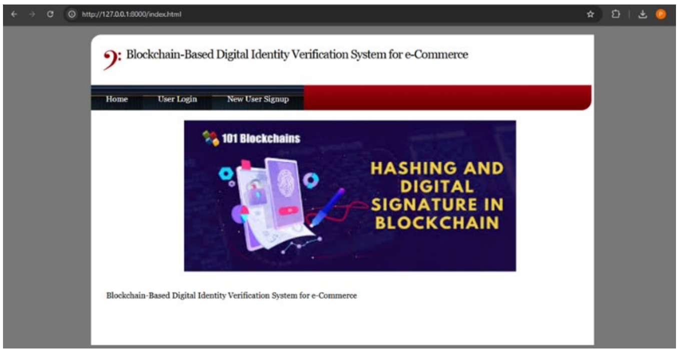
**Advantages:**

1. **Security**: Blockchain uses cryptographic algorithms to ensure data integrity and prevent unauthorized access.
2. **Transparency**: All transactions are visible to participants and cannot be modified, ensuring full transparency.
3. **Decentralization**: Since blockchain operates across a distributed network, there is no central authority controlling the data, reducing the risk of corruption or data breaches.

4. **Immutability**: Once data is added to the blockchain, it cannot be altered or erased, making it tamper-proof.
5. **Efficiency**: Blockchain automates processes through smart contracts, reducing the need for intermediaries and improving transaction speed.
6. **Cost Reduction**: By eliminating middlemen and reducing the need for intermediaries, blockchain lowers operational costs.

## 4. EXPERIMENTAL ANALYSIS

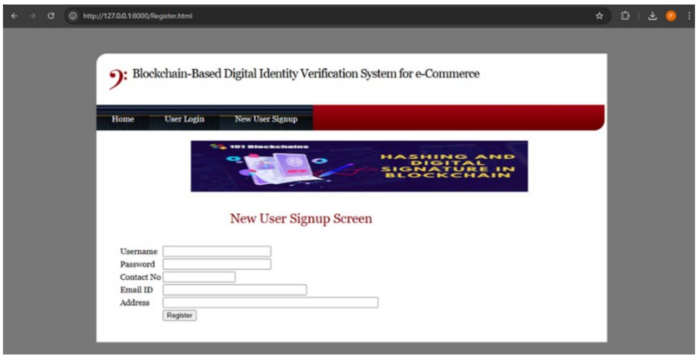
The Figure 2 represents Home Page of Project Site. It shows a website focused on providing a blockchain-based digital identity verification system for e-commerce. It leverages core blockchain concepts like hashing and digital signatures and potentially integrates with the 101 Blockchains platform for educational or technological support. The user interface is designed to be informative and user-friendly, with clear navigation and a focus on the key features of the system. The Figure 3 represents Signup Page of Project Site.


http://127.0.0.1:8000/index.html
Home
User Login
New User Signup
101 Blockchains
HASHING AND DIGITAL SIGNATURE IN BLOCKCHAIN

Blockchain-Based Digital Identity Verification System for e-Commerce

Blockchain-Based Digital Identity Verification System for e-Commerce

**Figure 2: Home Page**


http://127.0.0.1:8000/Register.html
Home
User Login
New User Signup
101 Blockchains
HASHING AND DIGITAL SIGNATURE IN BLOCKCHAIN
Register

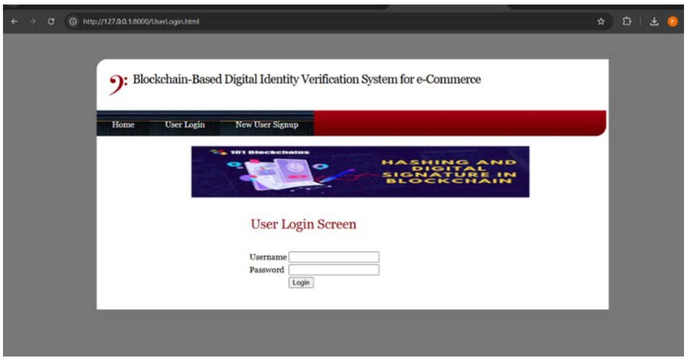
Blockchain-Based Digital Identity Verification System for e-Commerce

New User Signup Screen

Username
Password
Contact No
Email ID
Address

**Figure 3: Signup Page**

The signup form, accessed by clicking the "Signup" button on the homepage, is clearly structured and user-friendly. It features distinct input fields for essential personal details, including "Name," "Mobile," "Email," "Username," "Password," and "Confirm Password." Each field is accompanied by a descriptive label to guide the user through the registration process. The "Name" and "Mobile" fields allow for the input of a user's full name and mobile phone number, respectively. The "Email" field requires a valid email address, likely for verification and communication purposes. The "Username" field allows the user to create a unique identifier for their account. The "Password" and "Confirm Password" fields ensure secure account creation by requiring users to enter and confirm a password, preventing typos and enhancing security. Finally, a prominent "Register" button at the bottom of the form allows users to submit their information and complete the signup process. The Below Fig. 10.3 represents Login Page of Project Site.



http://127.0.0.1:8000/UserLogin.html

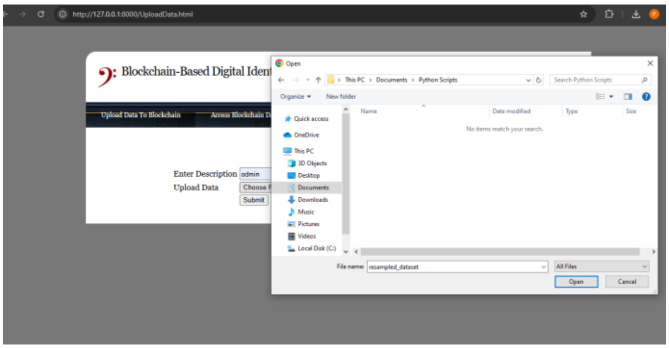
Blockchain-Based Digital Identity Verification System for e-Commerce

User Login Screen

Username
Password
Login

**Figure 4: Login Page**

The login form, accessible via the "Login" button on the homepage, presents a straightforward and secure interface for returning users. It consists of two primary input fields: "Username" and "Password." The "Username" field prompts users to enter the unique username they created during the signup process. The "Password" field, appropriately masked for security, requires users to input the corresponding password associated with their account. Below these fields, a prominent "login" button allows users to submit their credentials for verification. Upon successful authentication, users are granted access to their personalized accounts and the platform's mental health support services. The Below Fig. 10.4 represents File Upload of Project Site.



http://127.0.0.1:8000/UploadData.html

Blockchain-Based Digital Iden

No items match your search.

Enter Description admin
Upload Data
File name: resampled_dataset

**Figure 5: File Upload**

The Figure shows that users to upload data, with an associated description, to a blockchain. The system likely focuses on digital identity and provides tools for both uploading and accessing data stored on the blockchain. The file selection dialog shows the user choosing a specific file, "resampled dataset," suggesting that the data is prepared or processed for the blockchain system.

## 5. CONCLUSION

The integration of blockchain technology with digital identity verification systems offers a robust and efficient solution to address the increasing concerns over privacy, security, and data management in e-commerce and online transactions. Blockchain's decentralized nature ensures that user data is not stored in a single point of failure, making it significantly harder to compromise or manipulate. By combining blockchain with AI-driven cybersecurity measures, the proposed system provides a secure, transparent, and scalable method for verifying identities, ensuring that users have complete control over their personal information. In this system, the use of smart contracts plays a critical role in automating and verifying various actions related to identity management. Smart contracts are tamper-proof and transparent, providing both the user and the service provider with a trusted, immutable record of transactions. This decentralized approach helps mitigate risks related to identity theft, fraud, and unauthorized access, offering an enhanced level of protection compared to centralized systems.

The blockchain-based identity verification system is also designed to be user-friendly and accessible, providing easy registration, authentication, and data management processes. The seamless integration of these components ensures that users can engage with the system confidently, knowing their personal data is securely encrypted and stored in a decentralized manner. Moreover, the addition of AI cybersecurity systems helps in continuously monitoring, detecting, and responding to potential security threats, enhancing the system's resilience. Through this project, it is clear that blockchain technology, paired with AI, provides a scalable and innovative solution to the growing demand for secure, verifiable digital identities. The blockchain system not only improves security and privacy but also reduces administrative costs and complexities associated with centralized identity management systems. As the digital landscape continues to evolve, solutions like the one presented in this project will become even more critical in ensuring trust and security in digital interactions.

In terms of scalability, the system can be expanded to support a wider range of applications, such as financial services, healthcare, and government services. The decentralized nature of blockchain makes it highly adaptable and suitable for various industries that require secure, verifiable identity management. Additionally, the future scope of the project includes improving the system's interoperability with other blockchain networks and existing digital identity systems, fostering a more unified and global approach to digital identity verification.

## REFERENCES

[1] Pascual, A., Marchini, K., & Miller, S. (2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity

[2] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In 2015 IEEE Security and Privacy Workshops. San Jose, CA: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7163223/

[3] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In 2016 2nd International Conference on Open and Big Data (OBD).

[4] Chen, Z., & Zhu, Y. (2017). Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging. In 2017 IEEE International Conference on AI & Mobile Services (AIMS). Honolulu, HI: IEEE.

[5] Do, H., & Ng, W. (2017). Blockchain-based System for Secure Data Storage with Private Keyword Search. 2017 IEEE 13Th World Congress On Services. doi: 10.1109/SERVICES.2017.23

[6] Mudliar, K., Parekh, H., & Bhavathankar, P. (2018). A comprehensive integration of national identity with blockchain technology. In 2018 International Conference on Communication information and Computing Technology (ICCICT).

[7] Soliman, A., Bahri, L., Carminati, B., Ferrari, E., & Girdzijauskas, S. (2015). DIVa: Decentralized identity validation for social networks. In 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).

[8] Elmansori, M., Atan, H., & Ali, A. (2017). Factors Affecting E-Government Adoption by Citizens in Libya: A Conceptual Framework. I-Manager's Journal On Information Technology, 6(4). doi: 10.26634/jit.6.4.13845

[9] Elmansori, M., Atan, H., & Ali, A. (2018). Adoption of E-government Services in Libya: A Critical Review. Saudi Journal Of Humanities And Social Sciences (SJHSS), 3(4), 553-560. doi: 10.21276/sjhss.2018.3.4.4

[10] Al-Shuaili, S., Ali, M., Jaharadak, A., & Al-Shekly, M. (2019). An Investigate on the Critical Factors that can Affect the Implementation of E-government in Oman.2019 IEEE 15Th International Colloquium On Signal Processing & Its Applications (CSPA). doi: 10.1109/cspa.2019.8695988

[11] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Draft NISTIR 8202: Blockchain Technology Overview [Ebook

[12] Mahendran, D., Jamal, A., Helmi, R., & Fatima, M. (2018). Trusted computing and security for computer folders. International Journal Of Medical Toxicology & Legal Medicine, 21(3and4), 83. doi: 10.5958/0974-4614.2018.00036.0