Study of Implementing Blockchain for Enhanced Authentication in Web Portals

Vidhi Mehta; Shruti Patil; Pranaya Pounikar
Dept of MCA, GHRCEM, Nagpur, RTMNU, India

Abstract

Authentication is a fundamental component of web security, enabling users to safely access online websites. The Authentication is one of the major elements of web security that facilitates users to secure access to internet websites. Traditional methods of authentication are based on password entry, multi-factor authentication (MFA), and single sign-on (SSO). Even though the methods are often followed in these times, the methods are never foolproof Passwords can be hijacked, MFA can be circumvented, and SSO depends on centralized infrastructure that can be compromised. Millions of user accounts have been exposed due to data breaches and phishing attacks, and there is a growing demand for a safer alternative.

This paper discusses ways blockchain technology improves authentication in web portals. Blockchain provides decentralization, immutability, and cryptographic security that makes it difficult for hackers to steal credentials or tamper with login systems. We present why decentralized identity (DID), smart contracts, and Web3 authentication are preferable to conventional alternatives. Besides, the real-world applications and case studies will be examined to demonstrate how blockchain technology can build a more secure and user-managed authentication system. This paper aims to offer a clear picture of how blockchain technology can enhance authentication, minimize hacking threats, and build a safer online environment.

Keywords: blockchain, authentication, security, data protection, web portals.

1. Introduction

Web portals are now commonplace for almost every service ranging from e-commerce and banking to social media and healthcare. Such web portals mandate secure verifications to confirm users' identities and safeguard their personal information. Authentication has always relied on passwords, multi-factor authentication (MFA), and Single Sign- On (SSO) systems. Passwords can be stolen through phishing or data breaches, MFA can be bypassed, and SSO depends on centralized systems that hackers cantarget. Because blockchain offers decentralized and secure identity verification, it's authentication methods are much more challenging to interfere with and represent an improvement over the existing measures. Unlike the traditional methods, passwords do not need to be stored centrally using blockchain-based authentication, so there is less chance of large-scale hacking. With the use of smart contracts and decentralized identity (DID) blockchain, users can assert their identity without any third- party service interference [1]. This paper focuses on the issues surrounding authentication and how Blockchain technology can help resolve security concerns in web portals. It highlights the important aspects of web portals like login systems, decentralized identity, cryptography security, and other postulated functionalities along with their real-world applications and obstacles in the deployment. It attempts

DOI: https://doi.org/10.5281/zenodo.15567584

to explore these innovative and secure forms of identity authentication and their implementation in web portals.

1.1. About Authentication

Organizations often face challenges in managing IT assets efficiently which reduces the efficiency of software and it might lead to issues in the development phase, particularly when dealing with large numbers of workstations spread across multiple teams. Manual tracking methods are difficult to use and prone to inconsistencies, security risks, and resources mismanagement. Moreover, existing inventory tools often lack real-time system updates, seamless Linux integration, and team-based connectivity, making them inadequate for modern IT environments. This research addresses these challenges by developing an automated, real-time workstation inventory system that improves monitoring, optimizes resource allocation, and enhances security [3] .

1.2. Traditional Authentication Methods

Traditional authentication methods in web portals have been generally used for decades to verify user identities and allow access to online services. These methods depend on established techniques to ensure thatonly authorizedusers can access sensitive information or perform specific actions.However, they have some weaknesses especially when dealing with new and changing online security threats. Below are the most common traditional authentication methods:

1.2.1. Password-Based Authentication

Password-Based Authentication is the most common approach where username and password are entered to login to an account. The system checks if the password provided is equal to the hash that is stored in the database. When a password is input by a user, the system never stores the password itself for security reasons. It stores a hashed version of the password.

Limitations of Password-Based Authentication

Phishing whereby Hackers will trick users to type in their passwords on sites that are pretending to be sites they trust, Brute-force attacks Hackers utilize automated systems to guess at passwords by using millions of variations,

Database breaches If a database of a company is compromised, stored password hashes can be released.

Most individuals employ the same password across several websites (e.g., email, social media, banking). If a single website is hacked, attackers can attempt the same password on other websites.

With every site demanding a password, users find it difficult to have unique and complicated passwords. This results in using weak password which is easy to crack, noting down passwords which is susceptible to theft and losing passwords and trusting password resets, which can be taken advantage of by attackers.

1.2.2. MultifactorAuthentication

Multifactor Authentication works where users provide two or more verification factors, like OTPs, Authenticator apps and fingerprints or face recognition which greatly improves security by using multiple ways to verify identity, making it harder for unauthorized people to gain access.

LimitationsofMultifactor Authentication

It can be complicated and expensive to set up or implement.

Users can find it frustrating to use the system, making them less likely to adopt it. There is risk of data breach, if the data like facial recognition or fingerprints is hacked it is hard to change like password

1.2.3. Single Sign-on

In this, users log in once using a single set of credentials (e.g., Google or Facebook account) to access multiple web portals or services without needing to log in

DOI: https://doi.org/10.5281/zenodo.15567584

separately for each one. This simplifies the login process for users and reduces the number of passwords they need to remember.

If the Single Sign-On (SSO) provider is hacked, all connected accounts will be vulnerable to attacks.

The security of the entire system relies heavily on the SSO provider's ability to protect user data and prevent breaches.

When using SSO, individual websites have limited control over user data, which can make it harder to manage and protect that data.

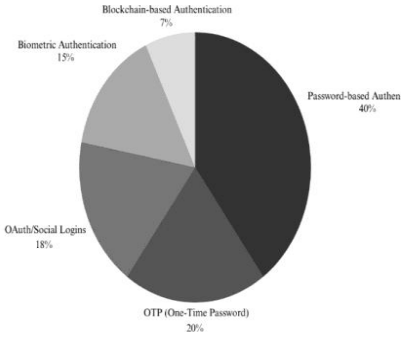

Fig. 1 Comparison of Authentication Methods Usage

2. Introduction to Blockchain Technology

Blockchain is a decentralized, distributed Logbook technology that records transactions or data across multiple computers in a way that ensures the data is secure, transparent, and tamper-proof. Each "block" in the blockchain contains a list of transactions, and these blocks are linked together in a Sequential "chain" using cryptographic principles. Once data is added to the blockchain, it cannot be modified or removed, making it immutable means cannot changed. Blockchain is a decentralized, digital logbook that records transactions across multiple computers in a secure and Protected manner. Instead of depending on a central authority, it ensures trust through cryptography and Coordination techniques [5] .

Suppose a bunch of friends share a shared digital notebook to record payments for a vacation. Rather than having one bookkeeper keep track, each friend has a copy of the book. When someone makes a payment (say, food or transportation), the payment is added to a "block" and broadcast to everyone. Each block connects to the last one, creating a chain. If an individual attempts to change a transaction, the group can quickly check the alteration since all have a copy of the ledger. This is to ensure transparency and avoid fraud.

A practical application of blockchain is the use of Bitcoin, a form of cryptocurrency that employs the use of blockchain to track financial transactions. Each Bitcoin transaction is deposited in a block, and blocks are combined to create a public ledger [4]

. The ledger is kept by a worldwide network of computers (nodes) to prevent any entity from possessing the data.

2.1 .Implementation and Working Of Blockchain –

Blockchain is used by first determining a particular challenge it may address, e.g., authentication, supply chain tracking, etc. After a use case has been defined, the type of blockchain, public, private, or consortium, is selected based on the degree of access and control needed. A consensus mechanism (e.g., Proof of Work or Proof of Stake) is chosen, as a way to authenticate transactions and achieve consensus amongst network nodes. The architecture of the blockchain is subsequently designed, specifically defining how blocks are generated, connected, and secured. Where necessary, smart contracts are created to process context on the blockchain, e.g., checking user identity for authentication purposes. Nodes/computers are configured so as to create the decentralized network, so that no single entity can control the system.

The blockchain is then put through the paces of security, scalability and performance and deployed. Live the

DOI: https://doi.org/10.5281/zenodo.15567584

system is the target of continuous monitoring and evolution, to combat security flaws or enhance the behaviour. Blockchain works by recording transactions in a secure, transparent, and immutable manner. If a user starts a transaction it is transmitted to a node network with the goal of verification. Confirmed transactions are aggregated in blocks that include a list of transactions, a pointer to the block prior, and an identity. The network nodes, based on a consensus mechanism, will agree the validity of the block and then will include that block in the blockchain. After its introduction, the block is chained to the current one, in that it inherits the identity of the previous one. Due to the decentralized structure of the network, the collected data is not controlled by any one party, and thanks to cryptography, data is tampered evident. This decentralization, transparency and immutability provide blockchain with the potential for use in secure authentication, finance, and supply chain management, etc.

Some of the advantages of employing blockchain in identity management have already been suggested:

Decentralized: The data maintained by the blockchain has no centralized authority controlling. This means blockchain is distributed across multiple nodes, meaning no single entity controls the entire network.

Tamper Resistant: The data committed to the blockchain cannot be removed. Therefore, historical actions on the blockchain cannot be modified and all the modifications performed are traceable.

Cost saving: Shared identity data can result in a cost reduction for relying parties. In addition, the size of replicated data in database is minimized.

User control: User never loses control of his digital identity even when he loses access to any specific service. All the above-mentioned points sum up to utilize blockchain network for authentication.

2.1. How Blockchain Can Improve Authentication

With the rapid growth of web service usage in the world, the blockchain technology can conveniently enable better user authentication in web portals. Unlike traditional methods of passwords and two-factor authentication, which can be easily hacked, phishing-ed or breached, blockchain can eliminate these problems with its unique features of decentralization, cryptography and immutability. Here are some of the ways which blockchain can enables better user authentication in web services portals.

2.1.1. Blockchain Technology And Strong User Verification Systems

Blockchains utilize computers which are referred to as nodes and the data is not stored centrally. This means that it can eliminate the need for hackers to target user credentials stored on a singular server that is prone to attacks. Therefore, Blockchains can enhance cyber security by enabling the control of sensitive information to only authorized personnel. For instance, instead of a standard password, a blockchain system could replace it with a set of cryptographic sets. There is a private key that the user only knows and a public key which the web portal can share. This way whenever the user wants to log in into the system, their identity is verified using these keys making the process much more secure and user friendly while eliminating the risk of password hacking.

2.1.2. Methods In Which Blockchain Technology Has Helped Reduce Attacks

Web Portal phishing and other cyber-attacks can be efficiently minimized with the use of blockchain technology. Here's how these systems can be secure integrated:

Data Breaches: One of the primary advantages of blockchain technology is the decentralization of its nature. Information is spread around a network with multiple nodes, therefore in the unreal instance a hacker manages to break

DOI: https://doi.org/10.5281/zenodo.15567584

into one node, there is no central hub of information to target. Each node operates in a network, meaning you are always going to be secured.

Man-in-the-Middle Attacks: When using a blockchain system, information is encrypted making it almost impossible for attackers to intercept crucial and confidential information.

Password Reuse: Risks of weak or easily guessable passwords are something that no user should worry about when using blockchain, because it rids the need of passwords entirely.

2.1.3. ExamplesofBlockchain-BasedAuthentication Models

In order to facilitate better web system security and user privacy, several blockchain-based authentication models have been developed. A few of them are listed below:

Self-Sovereign Identity (SSI)

A Self-Sovereign Identity model allows users to have full control of their identity information. Instead of a government or larger body validating their identity, users themselves store their credentials in a blockchain. Users can then provide only required information to the services without exposing their identity. For example, a user can prove they are an adult without revealing their actual date of birth.

Decentralized Identifiers (DIDs)

DIDs, Decentralized Identifiers, are new kinds of identifiers that users can create and manage on a blockchain. This can be useful to login into web portals without the need for a password and account username. Since DIDs are recorded on a blockchain, they are safe, unalterable, and impossible to replicate.

Blockchain-Based Single Sign-On (SSO)

SSO is a service that allows a user to access multiple applications with one single account. Instead of using a centralized service like Google or Facebook, it is possible to use SSO on blockchain to decentralize identity verification.

Password reuse is not one of the more worrying aspects when it comes to security, but paired with cyber-attacks makes it a serious threat that can be eliminated through the implementation of blockchain technology [9].

2.2. Challenges and Limitations of Using Blockchain for Web Portal Authentication

Even though blockchain technology can enhance the web portal's authentication, it has its challenges and shortcomings. There are certain issues that need special attention in order to allow successful execution and greater acceptance of the technology. Let's analyze these concerns one by one:

The Limits of Scalability

Difficulty: Most public blockchain networks, like Bitcoin and Ethereum, are restricted to a low allowance of transactions per second, making their efficiency very low for large-scale web portals. This is particularly true for web portals that have millions of users.

Remedy: Utilize private or consortium blockchains, which in addition to solving the scalability problem, are also quicker. Alternatively, one could implement Layer-2 solutions, like sidechains or off-chain transactions.

Proof of Work (PoW)

blockchains are slow and serve as an uncost friendly approach. For this reason, the extensive energy and computational effort required to move vast amounts of data renders them inefficient borders on crippling environmental degradation.

Difficulty: Operating any blockchain system that implements PoW takes substantial energy and didactic The energy and fossil fuel consumption required is preceded by massive data deployment. This renders it expensive and environmentally unfriendly

Remedy: The solution to this is shifting to a less demanding energy-efficient method of PoS, or making use of private blockchain systems. In addition, implementing more efficient computational power would also lend succor to the hurdle.

Challenges in Implementation

Problem: The technological barriers associated with the integration of blockchain into legacy web portals has a

DOI: https://doi.org/10.5281/zenodo.15567584

combination of high difficulty and higher effort. It needs skills in blockchain, cryptography, and networking.
Solution: Simplifying the integration process through the supply of blockchains frameworks and tools, or through affiliation with blockchain service providers.
Problems of Usability
Problem: Users in blockchain systems are often required to perform key management tasks, which includes losing their keys. In such cases, users will not have the ability to regain access to their accounts.
Solution: Developing less complex key management hardware, such as hardware wallets, greatly simplifies the processes for non-technical users.
Compliance and Governance Problems.
Problem: The decentralized structure that defines blockchain technology stands at odds with granular controls imposed by regulations, such a Europe's GDPR or CCPA in the United States.
Solution: Creating a blockchain system that is capable of satisfying compliance requirements by not storing user data on a blockchain, only encrypted data, or using a hybrid approach that incorporates blockchain and traditional databases.
Security Risks
Problem: Even though blockchain's features provide security, it can still be attacked. Some such as 51% attacks (where one entity controls most of the network) as well as issues related to smart contracts may disrupt the system [9].
Solution: Thorough security audits, the use of formal verification techniques for smart contracts, and strong encryption methods solved the problem.
Cost of Maintenance
Problem: Blockchain deals also come at a price, the upkeep of hardware, software, and networks is an endless cost, especially to novices in the business world
Solution: cloud-based blockchain as a service (BaaS) significantly cuts infrastructure and additive maintenance costs.
Lack of Awareness and Adoption
Problem: Slow adoption of blockchain technology can be traced to the lack of information and the ignorance of many users and companies, specifically for the authentication purpose on web portals.
Solution: Ease the transition by training and supporting businesses and users so that they understand the value blockchain can bring.

3. Comparison Blockchain Authentication with Traditional Authentication Methods

The discrepancies between Blockchain authentication and traditional methods of authentication are very distinct in the scope of security, user experience, expense, and execution. Passwords, two-factor authentication (2FA), and single sign-on (SSO) are traditional methods of authentication that operate on a centralized model where user credentials are kept in a single database. This means that they can easily be a victim of data breaches, hacking, and phishing. For instance, a hacker who gains access to the central database can easily extract all the stored passwords or credentials which poses user accounts at a risk [9]. Furthermore, traditional methods often employ the use of multiple passwords that users have to remember, which typically results in weaker password selection or them being re-used among different platforms which is an added security threat.
On the other hand, Blockchain authentication takes a more decentralized perspective where user data is not saved in one location but is distributed across a network of computers (nodes) [9]. This particular aspect makes it extremely challenging for hackers to compromise the system because there is no centralized point in the system that can be exploited. In addition, blockchain does not give passwords, but rather, authentication through cryptographic key. In this case, users have a private key that they know and a public
key shared with the system that helps in confirming their identity.
This method is safer since private keys are significantly less easy to be stolen or guessed

DOI: https://doi.org/10.5281/zenodo.15567584

than passwords. Additionally, blockchain's immutability guarantees that data once written can never be changed or hacked, adding another layer of protection. Another significant distinction is transparency and user control. Most traditional authentication techniques necessitate users to expose personal data, like email or phone numbers, to centralized authorities [9]. This is privacy-worrying because users lack full control over their data storage or usage. Blockchain, in contrast, gives users complete autonomy over their identity details using schemes such as Self-Sovereign Identity (SSI). Users are free to reveal just the needed details to web portals without divulging their complete identity, boosting security and privacy [7].

Blockchain authentication does come with some challenges. It is potentially more complicated and expensive to adopt than conventional approaches. For instance, cryptographic key management can be problematic for non-technical individuals, and losing a private key lead to permanent loss of account access. Moreover, blockchain networks, particularly public ones, are subject to scalability challenges, thus being slower and less efficient for extensive use. Legacy methods, although less secure, are easier, more intuitive, and less complex to implement, hence why they are still so popular.

In cost, legacy authentication methods are cheaper to install and run, as they use known technologies and infrastructure. Blockchain, however, needs high investment in hardware, software, and human resources, particularly for private or consortium blockchains. In spite of all these challenges, blockchain provides a more secure, transparent, and user-oriented way of authentication and is a very promising solution for the future. By overcome its shortcomings, including scalability and user experience, blockchain can replace or complement existing authentication systems, offering a safer and more convenient means to check identities in web portals [7].

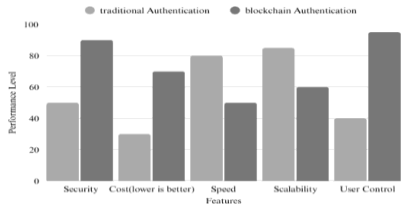

Fig. Performance Comparison of Traditional and Blockchain Authentication Across Key Criteria

3.1 Steps for Implementing Blockchain in web portals

Deploying blockchain on web portals is a series of processes to make the system secure, efficient, and user-friendly. Here's a step-by-step description of the process:

3.1.1. Define the Use Case

Begin by articulating the exact problem that you wish to address with blockchain. For web portals, it may be strengthening authentication, securing data, or facilitating decentralized identity management.

Example: Applying blockchain for safe user authentication to substitute for conventional password-based systems.

3.1.2. Select the Blockchain Type

Decide to go with a public, private, or consortium blockchain depending on your requirements:

Public Blockchain: Available to all (e.g., Ethereum, Bitcoin). Good for transparency but slow and less scalable.

Private Blockchain: Limited to certain users (e.g., Hyperledger). More scalable and faster but less decentralized.

Consortium Blockchain: Managed by a set of organizations. Achieves decentralization and control [1].

3.1.3. Select a Consensus Mechanism

Select a consensus mechanism to validate transactions and keep the blockchain secure. Popular options are:

Proof of Work (PoW): Secure but highly energy-intensive

Proof of Stake (PoS): Energy efficient

DOI: https://doi.org/10.5281/zenodo.15567584

and quicker.
Practical Byzantine Fault Tolerance (PBFT): Good for private blockchains.

3.1.4. System Architecture Design

Sketch out the system architecture of the blockchain-based authentication system
Describe how user credentials will be saved and authenticated.
Make a decision on using smart contracts for automating functions.
Design the user interface for easy integration with the web portal.

3.1.5. Create Smart Contracts

Smart contracts are programs that execute automatically on the blockchain. They can be used to automate processes such as user authentication or access management.
Example: A smart contract might authenticate user credentials and provide access to the web portal if the credentials are valid.

3.1.6. Configure the Blockchain Network

Establish the blockchain network by creating nodes (computers) that will be part of the system.
Make the network decentralized and secure by installing nodes in more than one location.

3.1.7. Web Portal Integration

Integratetheblockchain-basedauthentication system with the web portal:
Replace login forms with blockchain-based authentication (e.g., cryptographic keys or tokens).
Make sure that the integration is seamless and will not interfere with the user experience.

3.1.8. Testing of the System

Perform extensive testing to make the system secure, scalable, and user-friendly:
Test for vulnerabilities like hacking or data breaches.
Test high traffic to ensure scalability.
Get user feedback to enhance the interface and functionality.

3.1.9. Deploy the System

After testing, implement the blockchain-based authentication system on the web portal.
Keep a close eye on the system in the initial phase to fix any problems.

3.1.10. Educate Users

Provide training and assistance to assist users in understanding and transitioning to the new system:
Describe how to handle cryptographic keys or tokens.
Provide tools such as tutorials or FAQs.

3.1.11. Maintain and Upgrade

Regularly monitor the system for performance and security concerns.
Regularly update the system to handle vulnerabilities or enhance functionality.

3.1.12. Real-World Use Cases of Blockchain Authentication

Practical application of blockchain-based authentication systems is picking up pace in numerous industries because more and more customers are looking for secure, privacy-focused digital identity solutions. Many real-worluses show thecapacity of blockchain technology to transform legacy authentication mechanisms.
Civic is one such service that leverages blockchain to provide a decentralized identity verification service. Through the use of the Ethereum blockchain and its hybrid key management system, Civic enables users to confirm identities without continuously exposing sensitive personal details [2]. Its architecture keeps identity information on the user's device securely stored while the blockchain tracks status for verification, reducing the risks of data breaches and identity fraud.
Civic's methodology is commonly applied in industries that need strict Know Your Customer (KYC) compliance, like financial institutions

DOI: https://doi.org/10.5281/zenodo.15567584

and online voting platforms.

Consequently, uPort offers another substantial example of a self-sovereign identity solution based on the Ethereum blockchain. It allows users to define and control their digital identities themselves, without having to depend on a central governing body. Users are in full control of their credentials and selectively share data as desired. This decentralized approach improves privacy and blocks unauthorized access to data, thus making uPort a perfect solution for digital identity authentication across diverse web applications.

3.

Hyperledger Indy is another example of how blockchain is used in authentication. As one of the Hyperledger projects, Indy is a toolkit for building decentralized, privacy-protecting digital identities. Indy's architecture enables the issuance of verifiable credentials and DIDs, with the assurance that users maintain sole control over their digital identity. Hyperledger Indy has been implemented by enterprises, educational institutions, and government agencies to improve their identity management systems and decrease their reliance on centralized databases.

Microsoft's Identity Overlay Network (ION) is yet another great example, based on the Bitcoin blockchain. ION is designed to be a scalable decentralized identity system that dispenses with the use of third-party verifications. With it, individuals can take control and ownership of their identifiers and credentials and store them securely on decentralized networks. The system can find applications in managing digital passports, licenses, and education certificates, providing greater security and user control.

, previously known as ConsenSys Mesh, also illustrates the real-world usefulness of blockchain for authentication. Utilizing decentralized identifiers and verifiable credentials, Serto facilitates secure interactions between organizations and individuals without invading privacy. Its solutions find particular applicability in industries such as healthcare, supply chain, and finance, where identity verification must be both secure and efficient.

These real-world applications demonstrate the revolutionary effect of blockchain technology on digital verification. Through decentralizing identity management and improving privacy, these platforms overcome most of the shortcomings of conventional verification methods [4].

4.Conclusion

The authors suggest that blockchain technology presents an effective solution to augment authentication in web portals by overcoming the shortfalls of conventional methods such as passwords and two-factor authentication. Its secure, decentralized, and transparent technology renders it extremely effective in thwarting cyber threats like phishing and data breaches, with added user control over identity information. Regardless of obstacles such as scalability, expenses, and user experience, the potential of blockchain technology to change authentication is beyond question. By embracing blockchain, web portals will be able to develop a more secure, streamlined, and user-centric authentication system, opening the door for a safer digital future. More research and innovation are required to overcome current hurdles and unlock blockchain's full potential in this area.

5.References

[1] Khan, A. G., Zahid, A. H., Hussain, M., Farooq, M., Riaz, U., & Alam, T. M. (n.d.). A Journey of WEB and Blockchain towards the Industry 4.0: An Overview. Department of Software Engineering, University of Management and Technology, Lahore, Punjab.

[2] S. Patel, A. Sahoo, B. K. Mohanta, S. S. Panda, and D. Jena, "DAuth: A Decentralized Web Authentication System using Ethereum-based Blockchain," in Proc. 2019 Int. Conf. on

DOI: https://doi.org/10.5281/zenodo.15567584

Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019.

[3] D. Li, W. Deng, W. Peng, and F. Gai, "A Blockchain-based Authentication and Security Mechanism for IoT," College of Computer, National University of Defense Technology, Changsha, Hunan, China.

[4] Ahmed, M. R., Islam, A. K. M. M., Shatabda, S., & Islam, S. (n.d.). Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh.

[5] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (n.d.). Blockchain Technology Innovations. Institute for Advanced Systems Engineering, University of Central Florida, USA.

[6] Noh, H., Choi, C., Park, M., Kim, J., & Kim, S. (n.d.). Security Analysis on Password Authentication System of Web Portal. Center for Information Security Technologies (CIST), Korea University, Seoul, Korea.

[7] Asif, M., Aziz, Z., Ahmad, M. B., Khalid, A., Waris, H. A., & Gilani, A. (n.d.). Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities.

[8] J. Seo, "The Future of Digital Authentication: Blockchain-driven Decentralized Authentication in Web 3.0," Department of Computer Science and Engineering, Sogang University, Seoul, South Korea, 2024.

DOI: https://doi.org/10.5281/zenodo.15567584