International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 11 | Nov 2024 www.irjet.net p-ISSN: 2395-0072

Blockchain-Enabled Authentication for Social Media Platforms

[1]Nagesh Sarade, [2]Abhijit Chorade, [3]Prathamesh Patil, [4]Laxman Alashetti , [5]Digvijay Jadhav , [6]P.A.Satarkar

[1,2,3,4,5]UG Students, Department of Computer Science and Engineering, SVERI's College of Engineering Pandharpur, Maharashtra, India
[6]Assistant Professor, Department of Computer Science and Engineering, SVERI's College of Engineering Pandharpur, Maharashtra, India

---

Abstract—Social media platforms are widely used for sharing ideas and content globally. However, they face challenges such as the spread of misinformation, which poses a threat to democracy. One major issue is the presence of fake accounts and inadequate regulation. To address these problems, it's proposed to verify social media accounts using real identities. Blockchain technology offers a solution by securely storing digital identities. When creating a social media account, users would need to verify their identity with a database. This database would then share a unique identifier with the social media platform, preventing the creation of multiple accounts by a single person.

Keywords—Fake news, Social media, Blockchain, Digital identity.

I. INTRODUCTION

In the realm of digital communication, social media stands as a transformative force, offering internet-based platforms for mass personal interaction and content generation, as defined by Carr and Rebecca [1]. Early precursors such as Usenet, crafted in 1979 by Tom Truscott and Jim Ellis, paved the way for online idea sharing. However, these platforms faced limited adoption due to factors like restricted internet access and low literacy rates.

The advent of Web 2.0 in 2005 heralded a new era of internet innovation, ushering in a diverse array of social media platforms that empowered users to create and disseminate content [2]. Web 2.0 introduced groundbreaking technologies like Adobe Flash, RSS, and AJAX, fueling the development of more dynamic and engaging social media experiences [5].

Today, social media has become an integral facet of contemporary life, particularly for younger generations raised in a digital milieu replete with electronic devices and online networking platforms [3].Despite a stabilization in growth rates observed since 2013, the global tally of social media users surged to an estimated 3.81 billion in 2020, representing a 45% upsurge from 2015 and a remarkable 95% leap from 2008. This consistent growth trajectory, averaging an annual increase of 9.8%, underscores the enduring relevance and impact of social media in modern society.

II. Literature Survey

The rapid evolution of social media platforms has transformed how individuals communicate and share information. However, this shift has introduced significant challenges, particularly regarding misinformation, identity theft, and the proliferation of fake accounts. Numerous studies have explored these issues and proposed solutions, emphasizing the need for robust digital identity verification mechanisms.

1. Carr, Caleb T., and Rebecca [1] Social Media and Misinformation

The rise of social media has facilitated the spread of misinformation, which can undermine public trust and democratic processes. Carr and Rebecca (2015) highlight that social media, while empowering users to share content, has become a breeding ground for false information ,particularly during significant events such as elections. The dissemination of fake news through social media can skew public perception and influence decision-making (Fieseler et al., 2010).The role of social media bots in manipulating online discourse has been documented, with studies showing extensive bot intervention during the 2016 U.S. elections (Kwon et al., 2016).

2. Fieseler, C., Fleck, M., Meckel, M [2]. Digital Identity Verification

To combat the challenges posed by fake accounts and misinformation, researchers have proposed various digital identity verification solutions. One prominent approach is the use of bio metric data, such as fingerprints, to authenticate users. This method ensures that each account corresponds to a verified individual, thereby reducing the potential for fake accounts (Yu et al.,2018). The integration of blockchain technology into digital identity verification systems has garnered attention due to its decentralized nature and security features. Blockchain can store digital identities securely, making it difficult for unauthorized users to manipulate or create false identities (Can Kaya, 2016).

3. Anderson, Monica, and Jingjing Jiang.[3] Blockchain Technology Blockchain technology offers a promising solution for digital identity verification. Its immutable nature ensures data integrity, while cryptographic hashing enhances security (Shabir etal., 2016). Various studies have explored the potential of blockchain in identity management ,arguing that it can provide a secure, decentralized framework for verifying users' identities (Griffiths, 1999). By leveraging a blockchain-based system, social media platforms can enhance user trust and reduce the risks associated with identity theft and fraud.

4. Kwon, H.E., So, H., Han, S.P., Oh, W.[4] Social Media Addiction and User Behavior

The addictive nature of social media is another critical area of research. Studies indicate that excessive use of social media platforms can lead to detrimental effects on mental health, particularly among younger users (Kuss Griffiths, 2017). The design of social media platforms often exploits users' psychological vulnerabilities, leading to increased screen time and diminished real-life interactions. This phenomenon highlights the need for responsible design practices and regulatory oversight to protect users from potential harm.

III. OBJECTIVES

The primary objective of implementing blockchain technology for social media authentication is to create a more secure, reliable, and user-centric authentication system that enhances user privacy while minimizing the risk of fraud and identity theft. The specific objectives of this project include:

1. To Enhancing Security and Privacy
2. To Empowering Users
3. To Reducing Fraud and Misinformation
4. To Decentralizing Identity Management
5. To Streamlining User Experience
6. To Promoting Interoperability

IV. PROBLEMS IN SOCIAL MEDIA

While social media platforms offer avenues for sharing photos and videos, they also serve as conduits for disseminating content containing violence and negativity, which can significantly impact the behaviour of children growing up in a mobile phone-centric environment. Additionally, users spend an average of 2.5 hours per day on social media, diverting their attention from specific activities and potentially leading to addiction [8].

A. Addiction

Griffiths (1999) distinguishes internet addictions as being about addictions on the internet rather than being addicted to the internet itself [9]. Individuals can become addicted to various internet activities such as gaming, content sharing, shopping, and social networking. While social media serves communication and educational purposes for most users, a subset develops problematic, uncontrollable, and addictive behaviour

B. Fake news

While social media facilitates information sharing, some users exploit it to disseminate fake news. Individuals create and spread fake news to boost views, likes, and shares, while others use fake accounts and groups to influence society. Many malicious accounts, including fake accounts, are operated by social media bots, cyborg users, and trolls [4]. Social media bots, driven by computer algorithms, engage in negative activities like targeted digital bullying and spreading fake news. Studies have shown extensive bot intervention in online debates, such as during the 2016 U.S. election, where millions of Twitter bots were used to manipulate polls and spread fake news, potentially impacting public sentiment and decision-making [2].

C. Echo Chamber Effect

The echo chamber effect occurs when individuals seek information that aligns with their existing beliefs, reinforcing their viewpoints without exposure to counterarguments[7]. Like-minded individuals form groups and are exposed to similar news feeds on social media, leading to homogeneous communities. Cyborgs and social bots exploit these groups to propagate fake news, leveraging psychological factors like social credibility and frequency heuristic to influence belief in fake news. Homogeneous communities contribute to social polarization and the widespread dissemination of fake news [1].

D. Social Media Companies

Social media companies profit by selling targeted advertisements based on user data and engagement metrics. To increase profits, tech companies employ machine learning models to optimize news feeds and increase user engagement. Recommendation systems play a significant role in social media addiction by tailoring content to users' interests [1].

However, these systems can also facilitate the spread of fake news by targeting users with similar interests.[4] While various methods and technologies can detect fake news, robust solutions to prevent its spread remain elusive. A blockchain-based digital identity verification

system is proposed as a potential solution to address this challenge [5].

V. DIGITAL IDENTITY VERIFICATION

Digital identity verification involves authenticating the identity of individuals registering for social media platforms[9]. The implementation of this system is contingent upon government policies regarding social media and identity verification. By verifying users' real identities stored in government databases, social media companies can enhance security and trust[3].

A. Elements of Digital Identity

Distinct elements are employed for digital identification to bolster system robustness. These elements include identifiers (e.g., passport numbers), attributes (e.g., height, weight), and personal identifiers (e.g., date of birth), which remain unchanged over time. Identifying elements may vary based on government policies. Examples of identifiers include fingerprint raw data, photos, and passport numbers, while attributes encompass details like date of birth, height, and address. Fingerprint data, being unique to individuals, serves as a primary identifier.

B. Digital Identity Database

Databases play a crucial role in managing stored data and its purpose. Database Management Systems (DBMS) have evolved to accommodate vast amounts of data, with factors such as data model, consistency, security, and access influencing DBMS selection. While data models may vary, relational databases are commonly utilized, with SQL databases accounting for a significant portion of global data storage [6].

C. Limitations of SQL Database

Despite its advantages such as normalization and data integration, SQL databases are susceptible to vulnerabilities like SQL injection and administrative weaknesses. Data security is paramount for protecting records and resources from cyber threats. While encryption and administrative controls mitigate risks, SQL databases may not be suitable for digital identity verification systems due to centralized vulnerabilities and limitations in handling big data [10].

D. Blockchain for Digital Identity Verification

Blockchain technology offers a decentralized solution for storing digital identities, mitigating concerns associated with centralized databases. Its immutable nature ensures data integrity, while cryptographic hashing enhances security.

Private blockchains, despite vulnerabilities, offer advantages such as reduced power consumption and enhanced security through cryptographic algorithms. The decentralized and encrypted nature of blockchain technology makes it an ideal solution for securing digital identities, with its growing network size bolstering data immunity against security breaches [3].

VI. WORKING MODEL

1.User Creation of Social Media ID:

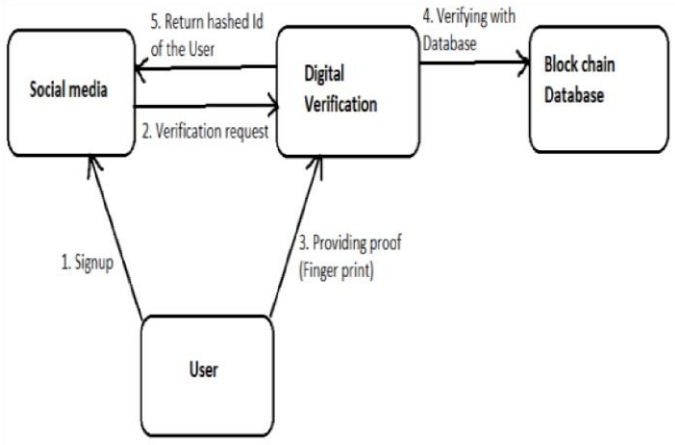
The process begins when a user decides to create a new social media account. This could be on any platform such as Facebook, Twitter, or Instagram.

1. Verification Request from Social Media

Platform: Once the user initiates the account creation process, the social media platform requests verification from the government's digital verification system. This step ensures that the user's identity is authenticated using reliable sources [6].

2. User Identification: The user is directed to the verification system portal, where they are required to provide their identifier, which in this case is their fingerprint [2].

1 System Design



3. Fingerprint Verification with Blockchain Database: The system then verifies the provided fingerprint data with the blockchain database. The blockchain database contains encrypted records of users' identities, ensuring their integrity and security [9].

4. Return of Encrypted ID: If the system finds a match between the provided fingerprint data and the records in the blockchain database, it generates a hashed (encrypted) ID for the user. This encrypted ID is then returned to the social media platform. [4]

Overall, this working model ensures that users' identities are securely verified using biometric data and stored in a tamperproof blockchain database. This enhances security, reduces the risk of identity theft, and helps in maintaining the authenticity of user accounts on social media platforms. [10].

Algorithms

1.Secure Shell (SSH) Algorithm

Steps:

1. Key Exchange:

The client and server exchange a session key using a key exchange protocol like Diffie-Hellman or ECDH.

2. Data Encryption:

All subsequent communication is encrypted using symmetric encryption (e.g., AES) with the session key.

3. Integrity Verification:

Message integrity is ensured using HMAC (Hash-based Message Authentication Code).

2.Digital Identity Verification with Zero-Knowledge Proofs (ZKP)

Steps:

1.Generate Identity Parameters:

The user generates a private identity parameter (e.g., a secret SSS) that will not be shared.

Compute a public identity parameter PPP, derived using a cryptographic function P=f(S)P = f(S)P=f(S).

2.Store Public Identity on Blockchain:

The computed PPP is recorded securely on the blockchain.

VII. COMPLICATION INVOLVED IN THE SYSTEM

A. Privacy Breaches and Law-breaking

Implementing digital identity verification to prevent digital frauds may lead digital companies to exploit personal data for their benefit. Current security laws may not adequately address such practices, posing risks of privacy breaches and potential violations of laws[2].

B. Identity Theft & Fraud and Reputation Harms

Digitalizing identity could inadvertently facilitate identity theft, resulting in issues like double identity problems. Such occurrences can adversely affect ecommerce departments and companies reliant on e-commerce platforms[4].

C. Digital Identity Invisibility & Inaccessibility

The quality of digital identity attributes is crucial. Typographical errors in digital identities, once recorded on the immutable blockchain, may persist indefinitely. This can lead to issues of inaccessibility and incorrect representation of individuals' identities.[5]

D. Machine Control and Ownership

The proliferation of machine-generated information, as highlighted by researchers, may surpass other forms of data growth. In a decentralized blockchain-based digital identity verification system, machinegenerated information is controlled by machines without human intervention, potentially raising concerns regarding control and ownership. [2]

VIII. CONCLUSION

The rise of social media has transformed the way we interact and communicate, yet its future implications were initially unclear. Over the past 15 years, social media has left both positive and negative impacts on society. Despite the challenges faced by the blockchain-based digital verification system, such as privacy concerns and potential vulnerabilities, it presents a promising solution.

Considering the growing number of social media users and the proliferation of cyborg accounts, which pose significant threats to democracy, it becomes imperative to consider innovative solutions for social media regulation. The blockchain-based digital verification system proposed in this paper represents a crucial initial step towards addressing these challenges and ensuring the integrity and security of social media platforms.

ACKNOWLEDGEMENT

Collaborating with friends and a teacher can greatly enhance the quality and depth of your conference paper. Working together allows for diverse perspectives, constructive feedback, and shared expertise, ultimately leading to a more comprehensive and polished final product.

REFERENCES

[1]. Carr, Caleb T., and Rebecca. (2015). "Social Media: Defining, Developing, and Divining Atlantic Journal of Communication." 23:46–65. ISSN: 15456870. DOI: 10.1080/15456870.2015.972282.

[2]. Fieseler, C., Fleck, M., & Meckel, M. (2010). "Corporate social responsibility in the blogosphere." Journal of Business Ethics, 91, 599–614.

[3]. Anderson, Monica, and Jingjing Jiang. (2018). "Teens, Social Media & Technology."

[4]. Kwon, H.E., So, H., Han, S.P., & Oh, W. (2016). "Excessive dependence on mobile social apps: a rational addiction perspective." Social Science Electronic Publishing. 27(4). 919-939.

[5]. Yu, L., Cao, X., Liu, Z., & Wang, J. (2018). "Excessive social media use at work: exploring the effects of social media overload on job performance." 31(6). 1091-1112.

[6]. Shabir, Ghulam, Hameed Yousef, Safdar Ghulam, & Syed Mohammed Farooq Shah Gilani. (2016). "The impact of social media on Youth: A case study of Bahawalpur City." International Journal of Computer Applications Technology and Research. 5(2). 71 – 75. ISSN: - 2319– 8656.

[7]. Perrin, Andrew. (2016). "Social Networking Usage: 2005-2015." Pew Research Center.

[8]. Can, L., & Kaya, N. (2016). "Social networking sites addiction and the effect of attitude towards social network advertising." Procedia-Social and Behavioural Sciences. 235. 484-492.

[9]. Griffiths, M. D. (1999). "Internet addiction: Fact or fiction?" The Psychologist: Bulletin of the British Psychological Society, 12, 246–250.

[10]. Kuss, D. J., & Griffiths, M. D. (2017). "Social networking sites and addiction: Ten lessons learned." International Journal of Environmental Research and Public Health, 14(3), 311. doi:10.3390/ijerph14030311.

[11] Vernekar, A. G., Phutane, M., Godase, R., Waghmode, V., & Shinde, S. M. (2020). Blockchain based E-Voting System. *International Research Journal of Engineering and Technology (IRJET)*, 7(12), 1786.