Asia-Pacific Journal of Information Technology and Multimedia 15(1) 2026: 60 – 83
https://doi.org/10.17576/apjitm-2026-1501-04

Web3 Digital Identity Authentication: Challenges, Opportunities, and a Proposed Secure Framework

Pengesahan Identiti Digital Web3: Cabaran, Peluang, dan Kerangka Keselamatan

*Liu XiaoYu, Khairul Akram Zainol Ariffin**

Center for Cyber Security, Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia

**Corresponding author: k.akram@ukm.edu.my*

Received 31 July 2025
Accepted 22 April 2026, Available online 30 June 2026

ABSTRACT

The advent of Web3 technologies has revolutionized the digital identity management landscape by introducing a decentralized framework that prioritizes user autonomy, privacy, and security of digital identity. This paradigm shift addresses the limitations of traditional centralized systems, which are vulnerable to cyberattacks and often compromise user control over personal data. Web3 digital identity authentication systems that leverage blockchain technology and decentralized identifiers (DIDs) offer a transformative approach that empowers users to manage their identities independently and securely. However, these systems also present unique challenges, including the complexities of managing cryptographic keys and the potential for irreversible data modifications on the blockchain. Furthermore, the decentralized nature of Web3 systems complicates regulatory compliance and interoperability across diverse platforms. Despite these challenges, Web3 digital identity systems are promising. They use verifiable credentials and smart contracts to enhance trust and automate identity verification processes, thereby reducing the risk of fraud. The integration of interoperability protocols facilitates seamless identity management across blockchain platforms and ensures a consistent user experience. However, the implementation of these systems requires addressing critical issues, such as user privacy, security vulnerabilities, and regulatory adherence. The global regulatory environment, characterized by diverse and evolving standards such as the GDPR and CCPA, poses significant compliance challenges for entities operating internationally. This paper addresses the critical gap in the existing literature by proposing a structured, multilayered secure framework for Web3 digital identity authentication that systematically integrates decentralized identifiers, verifiable credentials, smart contracts, interoperability protocols, and robust security mechanisms into a cohesive architectural model. The proposed framework is organized into seven interdependent components: DIDs, verifiable credentials, smart

contracts, interoperability protocols, user control, security mechanisms, and privacy enhancements. Each is mapped to specific functional requirements derived from the Self-Sovereign Identity (SSI) paradigm and the W3C standards ecosystem. By focusing on user-centric design and scalability, this framework aims to overcome the limitations of existing centralized systems while fostering a more secure and trustworthy digital identity ecosystem. Ultimately, the success of Web3 digital identity systems depends on addressing the interplay between technological innovation, regulatory compliance, and user education, ensuring that these systems enhance privacy, security, and user control in digital environments.

Keywords: Web3, privacy, digital identifiers, blockchain, verification.

ABSTRAK

Kemunculan teknologi Web3 telah merevolusikan landskap pengurusan identiti digital dengan memperkenalkan kerangka terdesentralisasi yang mengutamakan autonomi pengguna, privasi dan keselamatan identiti digital. Perubahan paradigma ini menangani keterbatasan sistem berpusat tradisional yang terdedah kepada serangan siber dan sering menjejaskan kawalan pengguna terhadap data peribadi. Sistem pengesahan identiti digital Web3 yang memanfaatkan teknologi rantaian blok dan pengenal terdesentralisasi (DID) menawarkan pendekatan transformatif yang memberi kuasa kepada pengguna untuk menguruskan identiti mereka secara bebas dan selamat. Namun begitu, sistem ini juga menimbulkan cabaran tersendiri, termasuk kerumitan pengurusan kunci kriptografi dan potensi pengubahsuaian data yang tidak boleh dipulihkan pada rantaian blok. Selain itu, sifat terdesentralisasi sistem Web3 menyukarkan pematuhan peraturan serta interoperabiliti merentas pelbagai platform.Walaupun terdapat cabaran ini, sistem identiti digital Web3 mempunyai potensi yang besar. Ia menggunakan kelayakan boleh disahkan (verifiable credentials) dan kontrak pintar untuk meningkatkan kepercayaan dan mengautomasi proses pengesahan identiti, sekali gus mengurangkan risiko penipuan. Integrasi protokol interoperabiliti memudahkan pengurusan identiti yang lancar merentas platform rantaian blok dan memastikan pengalaman pengguna yang konsisten. Walau bagaimanapun, pelaksanaan sistem ini memerlukan perhatian terhadap isu kritikal seperti privasi pengguna, kelemahan keselamatan dan pematuhan peraturan. Persekitaran regulatori global yang dicirikan oleh piawaian yang pelbagai dan sentiasa berkembang seperti GDPR dan CCPA menimbulkan cabaran pematuhan yang ketara bagi entiti yang beroperasi di peringkat antarabangsa. Kertas kerja ini menangani jurang kritikal dalam literatur sedia ada dengan mencadangkan kerangka keselamatan Web3 bagi pengesahan identiti digital yang berstruktur dan berbilang lapisan, yang secara sistematik mengintegrasikan pengenal terdesentralisasi, kelayakan boleh disahkan, kontrak pintar, protokol interoperabiliti dan mekanisme keselamatan yang kukuh ke dalam model seni bina yang padu. Kerangka yang dicadangkan disusun kepada tujuh komponen saling bergantungan: DID, kelayakan boleh disahkan, kontrak pintar, protokol interoperabiliti, kawalan pengguna, mekanisme keselamatan dan penambahbaikan privasi. Setiap komponen dipetakan kepada keperluan fungsi khusus yang diperoleh daripada paradigma Self-Sovereign Identity (SSI) dan ekosistem piawaian W3C. Dengan menumpukan pada reka bentuk berpusatkan pengguna dan kebolehskalaan, kerangka ini bertujuan mengatasi keterbatasan sistem berpusat sedia ada sambil memupuk ekosistem identiti digital yang lebih selamat dan boleh dipercayai. Akhirnya, kejayaan sistem identiti digital Web3 bergantung pada bagaimana interaksi antara inovasi teknologi, pematuhan regulatori dan

pendidikan pengguna dapat ditangani, bagi memastikan sistem ini benar-benar meningkatkan privasi, keselamatan dan kawalan pengguna dalam persekitaran digital.

Kata kunci: Web3, Privasi, Identiti digital, Rantaian blok, Pengesahan

INTRODUCTION

With the widespread adoption of Internet technology and rapid digitalization, users are increasingly dependent on digital identification for various online endeavors, including online banking and e-commerce. The issue of privacy protection in digital identity authentication systems has become a major research topic in recent years. Conventional centralized digital identity systems, such as social and bank account verification, offer convenient services; however, their centralized management and storage methodologies render them high-risk targets for cyberattacks.

The domain of digital identity management is undergoing a significant transformation with the advent of Web3 technology. In contrast to traditional centralized systems, Web3 introduces a decentralized framework that fundamentally redefines the creation, management, and utilization of identities across digital environments (Ghosh et al. 2024). This transformative shift is propelled by the growing demand for enhanced security, privacy, and user control—attributes that are frequently compromised under the centralized paradigms characteristic of Web2 (Ragab et al., 2024)

Web3 digital identity authentication systems that employ blockchain technology and decentralized identifiers (DIDs) signify a revolutionary change in identity management. However, despite their innovative frameworks, these systems are not exempt from security concerns. For instance, the decentralized nature of the blockchain may complicate prompt responses to unauthorized access or fraudulent activities. Once data are inscribed on a blockchain, it becomes challenging to modify them, implying that any initial unauthorized alterations are permanently recorded and are potentially irreversible (Xu et al. 2023).

Furthermore, while augmenting user autonomy over personal data, the implementation of DIDs concurrently imposes a substantial responsibility on users to manage their digital identities securely. There have been instances in which users have lost access to their cryptographic keys, rendering them incapable of accessing their digital identities without any means of recovery. Such instances highlight the user-dependent risks that are intrinsic to Web3 identity systems (Li et al., 2021).

The security of Web3 technologies is challenged by the increasingly sophisticated nature of cyber threats. A notable incident transpired in 2022, involving a prominent decentralized application (dApp) that managed digital identities, which were exploited through vulnerabilities in smart contracts. This breach resulted in unauthorized access to and theft of user identity data, illustrating that the complexity of Web3 systems can expose them to distinct attack vectors that are not present in conventional digital identity frameworks (Si et al., 2024).

Despite the proliferating body of literature on blockchain-based identity management and self-sovereign identity architectures, a critical research gap persists: the absence of a unified, theoretically grounded framework that systematically integrates the core architectural components of Web3 digital identity authentication, including decentralized identifiers, verifiable credentials, smart contracts, interoperability protocols, user control mechanisms, security infrastructure, and privacy-enhancing technologies, into a single, cohesive model that addresses the concurrent demands of security, privacy, scalability, regulatory compliance, and user-centricity (Schardong & Custódio, 2022). Existing studies, while valuable in addressing individual components or specific technological aspects, tend to operate in isolation, examining DIDs, verifiable credentials, or smart contracts as discrete elements without elucidating their architectural interdependencies or their collective contribution to a holistic identity authentication ecosystem (Sedlmeir et al., 2021). Moreover, several proposed systems prioritize technical feasibility over the equally imperative dimensions of regulatory alignment and user accessibility, resulting in frameworks that, although technologically sound, remain inadequately positioned for real-world deployment across heterogeneous jurisdictions and user populations (Soltani et al. 2021). This paper directly addresses this gap by formulating a comprehensive, multi-layered framework that delineates the architectural roles and interdependencies of each component and maps them against established theoretical constructs, including the SSI paradigm, Cameron's Seven Laws of Identity, and the W3C standards for DIDs and Verifiable Credentials, thereby contributing a structured knowledge synthesis that is both theoretically rigorous and practically actionable.

In this study, we investigated and proposed a secure framework for Web3 digital identity authentication. Through rigorous empirical research and comprehensive analysis, it is anticipated that a digital identity solution that is both secure and user-friendly can be established to address the myriad issues inherent in the existing centralized system, thereby fostering the advancement of digital identity authentication technology in a more secure and trustworthy manner. This study examines the essential components of Web3 digital identity authentication based on previous studies. A secure Web3 digital identity authentication framework was formulated based on the collected data. This framework not only considers the feasibility of technical implementation but also places significant emphasis on the ease of operation for users and the scalability of the system.

The remainder of this paper is organized as follows. The next section describes the development trends of Web3 digital identity authentication. This is followed by a discussion of the challenges and limitations of current digital authentication application. Next, the key elements of Web3 digital identity authentication are explained, followed by the framework development. Finally, the conclusions are presented.

DEVELOPMENT TRENDS OF WEB3 DIGITAL IDENTITY AUTHENTICATION

As the digital landscape has grown, the evaluation of digital identity has changed substantially. Advancing from the traditional, centralized network of Web1 to the interactive, user-focused realm of Web2, it now enters the exceptionally decentralized setup of Web3. This evolution signifies not only technological advancement but also a fundamental shift, namely, the enhancement of user autonomy, privacy, and security within the realm of digital authentication (Gadge, 2024).

Web 1.0 represents the Internet's first iteration. This period signifies the inception of the Internet, characterized primarily by users who are predominantly content consumers, whereas content creators are mostly the developers. Websites generated during this timeframe predominantly feature textual or visual material. The Web 1.0 era spanned approximately 1990–2000. A defining characteristic of this phase is the provision of static content by websites, in contrast to dynamic Hypertext Markup Language (HTML) content. Data and content are derived from static file systems, as opposed to databases, resulting in limited interactivity on web pages (Panchekha, 2024). In this era, the authentication of digital identities is rudimentary and entirely reliant on centralized servers. Users predominantly engage with the Internet through web browsers to access web pages that exhibit infrequent alterations.

The digital identity authentication mechanisms associated with Web 1.0 remain nascent, characterized by simplistic username and password frameworks that afford minimal security and nearly nonexistent data encryption. The governance of personal data predominantly resides with website administrators, thereby presenting considerable risks related to data privacy and security vulnerabilities (Nita and Mihailescu 2024).

With advancements in technology, the notion of Web 2.0 surfaced around the year 2000, originally introduced by Dale Dougherty. Web 2.0 enables users to transition from ordinary observers to active participants. The Web has grown into an interactive environment that aids in the transfer of information among people at opposite ends, culminating in the formation of what is termed social networks.

In this era, characterized by interactive networks, users can disseminate their information to a global audience. Users can upload videos for the consumption, engagement, and commentary of all network participants. As shown in Table 1, the extent of user engagement has undergone qualitative enhancement. The process of data transmission, which encompasses the transfer of various forms of data, such as videos, comments, and other user-generated content across the network, is instrumental in fostering these interactions. Commercial activities have become more efficient due to advancements in the capacity to exchange ideas, enhance communication technologies, and reduce travel and operational expenditures. The efficacy and reliability of data transmission not only expedite the pace of information sharing but also extend team collaboration and market responsiveness. The emergence of Web2 has profoundly altered the marketing landscape by significantly reducing the time required to implement marketing campaigns while simultaneously expanding the potential reach of such endeavors (Belostecinic, 2023). This technological advancement allows for a more rapid distribution of marketing content, thereby enabling businesses to respond promptly to fluctuations in the market and consumer feedback. Furthermore, Web2 has facilitated the extensive enlargement of the audience, rendering it feasible for marketing strategies to exert global influence and transcend conventional geographical and demographic constraints (Sridhar, 2019). This simplifies the process by which companies disseminate their products. Most importantly, acquiring customer feedback through online commerce is essential. Currently, a host of distinguished online business platforms and social media channels are related to Web2, including YouTube, Facebook, Instagram, Twitter, and other social networking sites.

In Web2, digital identities are predominantly governed by centralized authorities. Although this centralization permits efficient administration and fluid user experiences, it simultaneously engenders significant apprehensions regarding privacy, security, and ownership of data. Centralized frameworks frequently establish singular points of failure, rendering them appealing targets for cyberattacks that may culminate in extensive data breaches. Furthermore, such frameworks generally offer users restricted authority over their personal information, thereby raising critical issues regarding data privacy and potential misuse. Consequently, there is a growing demand for paradigms that guarantee enhanced user autonomy and legal structures to safeguard personal data (Abbas et al. 2024). As Web2 progressed, user data retained within expansive centralized repositories became a primary target for leakage and exploitation. This era witnessed the advent of the federated identity model, which endeavored to provide convenience to users by enabling single sign-on functionalities across diverse platforms. Notwithstanding its advantages, this model has proven largely ineffective in addressing the more profound concerns surrounding privacy and data sovereignty. While the federated model promotes ease of access and interconnectivity among various systems, it continues to depend on centralized data management, thereby failing to empower users with authoritative control over their information. The concept of privacy involves an individual's right to manage their own information, while data sovereignty emphasizes that data are accountable to the laws and governance structures of the place where they were obtained. The significance of these concepts became increasingly evident during this period, as public awareness and regulatory discourse underscored the vulnerabilities and potential misappropriation of personal information (Zheng et al., 2018).

The concept of Web3 was initially expressed by Berners-Lee. He envisaged an Internet in which data are interconnected in a significant manner, facilitating machines to comprehend human-like inquiries and process data with contextual awareness (Cao et al., 2023). The principal elements of Web3 predominantly encompass Financial Transactions, Privacy and Security, Transfer Speed, Technology, Ownership and Control.

Web3 introduced a fundamentally distinct paradigm regarding digital identity, marked by the decentralization and empowerment of users. In contrast to Web2, where identities are bound to services and governed by central authorities, Web3 endows users with self-sovereign identity (SSIs). These identities are overseen by individuals using blockchain and decentralized technologies, thereby facilitating enhanced control over personal data and interactions (Buterin, 2014; Abou et al., 2023).

The launch of Web3 and its repercussions on digital identity signal a change in direction towards a more decentralized digital realm, utilizing innovations such as blockchain and peer-to-peer architecture (Bashir, 2020). In this technology, digital identity advances towards self-sovereignty, whereby individuals possess augmented control and ownership over their digital identities, independent of central authorities (Popa, 2023). Technologies such as blockchain facilitate the establishment of secure and verifiable digital identities, thereby enhancing privacy and mitigating the risk of identity theft (Liu et al. 2024). Constructs such as decentralized identifiers (DIDs) and verifiable credentials are emerging as new standards for self-managed, interoperable digital identities (Huh et al., 2023). Furthermore, Web3 can facilitate interoperable digital identities that can traverse different platforms and services while upholding user privacy and security (Gebre et al., 2024). However, in Web3, digital identity continues to face multiple challenges.

TABLE 1. Comparative Analysis of Web1, Web2, and Web3

Category	Web1	Web2	Web3
Interaction	Static content	Dynamic, interactive content	Decentralized, interactive, real-time exchanges
User Role	Information consumer	Information participants; content creators	Information control by users; decentralized participation
Data Management	Centralized on servers	Centralized, with dynamic content delivery	Decentralized data across a distributed network
Technology	Basic HTML, static webpages	Rich Internet applications, AJAX	Blockchain, AI, machine learning
Management Model	Managed by website administrators	User-generated content, community management	Autonomous, user-controlled through smart contracts
Usability	Simple, limited user interaction	Enhanced usability, user-centric design	Advanced, with emphasis on security and user empowerment

CHALLENGES AND LIMITATIONS OF CURRENT DIGITAL IDENTITY AUTHENTICATION APPLICATIONS

As we transition into the Web3 era, the evolution of digital identity has introduced not only transformative advantages but also considerable challenges (Bashir, I. 2020). This includes concerns regarding user privacy and the security of identity frameworks. These challenges arise from the underlying factors associated with the management and knowledge of digital identities within a decentralized architecture, which may deter users and complicate their usability. Furthermore, adherence to regulatory standards has emerged as a significant impediment, as decentralized systems frequently lack explicit regulatory supervision, resulting in potential exploitation and complications pertaining to legal liability.

Beyond these challenges, obstacles to the implementation of digital identity systems are recognized within the Web3 landscape. These encompass the absence of a standardized framework to facilitate interoperability among diverse systems, as well as resistance from novel decentralized paradigms. These recognized hindrances may obstruct the extensive adoption and efficient operation of digital identity systems in various domains. As emphasized by Bashir (2020), it is imperative to address these challenges and surmount the recognized barriers to fully realize the potential of digital identity in Web3.

The primary challenge is the user's privacy. In an era where identity information holds substantial significance, concerns regarding user privacy have escalated to a critical level. As digital interactions and transactions have become increasingly fundamental to daily existence, safeguarding personally identifiable information has transitioned from a luxury to an essential requirement. The complexities surrounding user privacy issues in digital identity systems are multifaceted and profoundly influenced by the architecture of the implemented system. In conventional systems, the centralization of user data engenders inherent vulnerabilities. These centralized repositories serve as enticing targets for malicious entities because a single breach can compromise sensitive information pertaining to millions of users (Lin et al., 2022). These incidents

can result in serious fallout, including identity theft, monetary loss, and even the lasting impairment of someone's physical and psychological wellness. Moreover, the ramifications of a compromised digital identity extend beyond personal losses, potentially undermining social trust and the overall integrity of the digital ecosystem (Golladay and Holtfreter, 2017).

While blockchain establishes a secure infrastructure by facilitating the detection of data modifications, it does not, in and of itself, provide encryption for the data. This occurs when the need for encryption becomes apparent. Encryption transforms intelligible data into a secure format that can be reverted to its original form by an authorized entity using a cryptographic key. In a decentralized identity (DID) setup based on blockchain technology, every portion of user data can be encrypted before being recorded on the blockchain. This guarantees that, even in instances of data access, the data remain confidential and safeguarded against unauthorized scrutiny.

Nonetheless, the security and privacy advantages of the combination of blockchain technology and encryption concurrently introduce new challenges, particularly in the administration of encryption keys. Users are obliged to manage their keys with utmost security, as the loss of access to a key translates to the loss of access to the encrypted data that it secures. This prompts usability challenges that must be resolved to ensure that users can manage their keys without jeopardizing security (Guo et al., 2023).

To ensure that decentralized systems uphold user privacy, implementing robust encryption protocols and strict access controls is essential. Encryption algorithms require persistent updates to protect against cryptographic attacks. Likewise, access controls must be sufficiently sophisticated to accommodate intricate permissions and sharing configurations that empower users to disseminate various components of their digital identity in distinct contexts without unveiling unrelated personal information (Song et al., 2025).

Users have the duty to handle their keys, and the inability to access a cryptographic key could lead to leaving behind one's digital self. This not only presents considerable usability challenges but also raises concerns regarding the user's ability to manage keys securely without compromising the integrity and accessibility of their data (Fröhlich et al., 2020). This constitutes a significant obstacle to Web3 digital identity authentication.

The subsequent challenge pertains to the security of identity systems. Safeguarding identity frameworks is of immense significance, as these frameworks store and oversee vast amounts of personal data across diverse industries, such as finance, medical care, and public sector services. Considering their critical nature, digital identity systems are targets for cybercriminals and require continuous innovation in security strategies to safeguard sensitive data from increasingly sophisticated threats (Jena et al. 2024).

Digital identity systems are confronted with a multitude of cyberattacks, each meticulously crafted to exploit specific vulnerabilities (Alenezi, 2020):

1. Phishing attacks: These incidents arise when cybercriminals masquerade as legitimate entities through electronic communication with the intent of deceiving users into disclosing sensitive information. Such attacks are becoming increasingly sophisticated and frequently circumvent traditional security measures.

2. Malware attacks: Malware is employed to disrupt operations, expropriate sensitive data, or obtain unauthorized access to computer systems. The diversity and complexity of malware, including ransomware and spyware, present significant challenges to identity security systems.
3. Man-in-the-middle (MitM) attacks: These attacks involve an attacker intercepting communications between two parties to expropriate or manipulate data. The growing prevalence of insecure IoT devices in identity systems has broadened the scope of these vulnerabilities.
4. SQL injection: These attacks introduce malicious SQL code into a database via a web form or query parameter, thereby enabling an attacker to gain unauthorized access and manipulate sensitive information stored within the database.
5. Distributed denial of service (DDoS) attacks: These attacks utilize traffic to overwhelm a system, network, or service, exploit capacity constraints, and severely disrupt service availability and functionality.

To effectively mitigate these vulnerabilities, it is imperative to adopt a layered security strategy that encompasses the most advanced encryption methodologies, stringent access controls, and ongoing surveillance of security infrastructures. Advanced systems for detecting threats using AI and machine learning can help identify and eliminate dangers before they affect a system (Cao et al. 2023).

Moreover, the evolution of blockchain technology presents a promising pathway for enhancing digital identity security. By decentralizing the storage and management of identity-related data, blockchain technology can diminish the risks inherent in centralized data breaches and bolster resilience to potential attacks (Buterin, 2014; Liu et al., 2024).

The security of digital identity systems is a paramount concern that necessitates sustained focus and innovation. As the cyber threat landscape undergoes transformation, characterized by increasingly sophisticated assaults such as deepfakes and AI-driven phishing schemes, the methodologies and technologies employed to safeguard these systems must progress. The incorporation of biometric authentication, machine learning algorithms aimed at anomaly detection, and blockchain-based authentication exemplifies some of the most recent initiatives to fortify the integrity of digital identity systems.

Biometric recognition technologies, including facial recognition and fingerprint scanning, provide a level of security that makes it difficult to replicate or counterfeit, thereby enhancing the user authentication process. However, as these technologies have gained prevalence, they have concurrently become targets for more advanced attacks. For instance, studies have demonstrated that facial recognition systems can be deceived using sophisticated image processing techniques (Wu et al., 2022). This vulnerability necessitates ongoing advancements in biometric sensor technology and the formulation of more refined detection algorithms to differentiate between authentic and counterfeit biometric data.

Furthermore, the use of machine learning within security frameworks facilitates the assimilation of new data, augmenting the ability to identify irregular patterns that may signify security infringement. For instance, machine learning algorithms can scrutinize access logs and user

conduct to detect potentially nefarious activities that diverge from conventional patterns (Ali et al., 2024). This anticipatory methodology towards security serves to mitigate threats before they can inflict substantial harm.

The implementation of robust security protocols presents a formidable challenge that entails not only the adoption of innovative technologies but also the assurance that all elements of a digital identity framework function in harmony. This necessitates a comprehensive strategy that encompasses not only technological remedies but also legal and regulatory structures that endorse ethical utilization of these technologies. As these systems become increasingly vital to sectors such as finance, healthcare, and government services, preserving trust in digital identities has become paramount. Consequently, there must be unwavering dedication to enhancing security protocols, adapting to emerging threats, and accepting innovations that fortify the integrity of the digital infrastructure (European Commission, 2022).

The third significant challenge that digital identity systems face is regulatory adherence. The global regulatory environment governing data protection and privacy is fragmented and is perpetually evolving. Adhering to these diverse regulations is essential for enterprises to operate legally across various jurisdictions and maintain the trust of their clientele.

European Union (EU) General Data Protection Regulation (GDPR): The GDPR constitutes one of the most rigorous privacy and security statutes globally, mandating substantial safeguards for personal data. It endows individuals with a broad spectrum of rights, including access to data, the right to erasure, and data portability. The study discourse suggests that the GDPR's all-encompassing approach has profoundly influenced how businesses manage and process personal data, compelling them to guarantee lawful, transparent processing, and eliminate data when it is no longer a requisite (Tan et al., 2023).

United States - California Consumer Privacy Act (CCPA): The CCPA bears a resemblance, in principle, to the GDPR, emphasizing the provision of specific rights to consumers over their personal data. It applies to any enterprise operating in California and encompasses the right to be informed, access, and opt for the sale of personal data. The study observes that the CCPA’s focus on consumer rights reflects the burgeoning trend towards enhanced data protection in the United States, albeit with an emphasis on the commercial applications of personal data (Stallings, 2020).

APAC - Personal Data Protection Act (PDPA) of Singapore: The PDPA of Singapore establishes a framework for personal data protection similar to that of the GDPR, with a pronounced emphasis on consent and the practices of organizations. In contrast to the GDPR, the PDPA does not require data portability, thereby underscoring regional disparities in data protection priorities. Research indicates that the PDPA bolsters consumer trust by prioritizing consent and security measures; however, it does not confer as many rights to individuals as the GDPR does (Liu et al., 2024).

These distinct regulatory frameworks exemplify the various methodologies for data protection. The GDPR is recognized for its rigor and extensive scope, accentuating individual rights and imposing severe penalties for noncompliance. Conversely, the California Consumer Privacy Act (CCPA) places greater emphasis on consumer rights concerning the sale of commercial data,

whereas Singapore's PDPA underscores organizational accountability and consent, lacking the breadth of individual rights afforded by the European Union (Ke et al., 2022; Tan et al., 2023).

Entities operating on an international scale are compelled to navigate this intricate regulatory terrain by modifying their practices to align with the legal stipulations of each jurisdiction. This process requires not only the implementation of robust security measures but also continuous monitoring and adaptation to ensure compliance with evolving legal standards.

The establishment and management of international digital identity solutions can prove exceedingly challenging because of the imperative to comply with multiple, and at times contradictory, regulatory frameworks. Companies must possess the acumen to adeptly maneuver through these complexities to avert significant repercussions, including substantial financial penalties and reputational damage.

The European Commission (2016) emphasizes that failure to comply with the GDPR could incur fines amounting to 4% of the global annual revenue or €20 million, whichever is greater. This underscores the financial risks associated with noncompliance.

Compliance transcends legal adherence to laws and regulations. This necessitates vigilance regarding new regulatory developments and the implementation of requisite adjustments. As new privacy concerns or technological advancements have arisen, exemplified by the advent of blockchain technology and its implications for data security and anonymity, regulations have been frequently revised to accommodate such changes. The persistent challenge for companies lies in remaining apprised of these developments, comprehending them, and expeditiously executing the necessary modifications.

Digital identity systems face a multifaceted array of regulatory challenges across various jurisdictions, each demanding adherence to its own legal framework. This regulatory milieu substantially influences the execution and operation of technology within these systems. However, it is not only external regulations that pose challenges; internal technical constraints also play a pivotal role.

The initial limitation pertains to the constraints of technology related to digital identity authentication. Despite the remarkable technological progress that heralds have made in enhancing security and efficiency in digital identity systems, these advancements may not fully realize their potential because of intrinsic limitations.

Digital identity systems increasingly incorporate biometric technologies, including voice identification, iris recognition, facial recognition, and fingerprint scanning, owing to their exceptional security and distinct identification advantages. However, these methods have their limitations. Unlike passwords or PINs, biometric characteristics are fundamentally static; thus, once compromised, biometric data present a unique challenge. If these data are exposed or appropriated, an individual's biometric identification may be irreparably compromised (Sasada et al., 2024). Moreover, biometric systems are susceptible to accuracy challenges that can undermine their reliability. Environmental factors, the aging process, and alterations in physical conditions may modify biometric traits, resulting in elevated false rejection rates. For example, minor injuries

to the fingers can hinder fingerprint recognition, and facial recognition systems may encounter difficulties under inadequate lighting or variations in facial hair. Furthermore, sophisticated threats, such as spoofing, in which deceitful biometric traits are introduced (e.g., counterfeit fingerprints or masks), represent a considerable security hazard. These challenges necessitate continuous enhancements in sensor technology and algorithmic resilience to maintain the integrity and security of biometric systems in the future.

Blockchain technology has the potential to provide a transparent and decentralized framework for managing digital identities is frequently lauded. The qualities of blockchain—clarity, permanence, and removal of middlemen—offer significant benefits in creating trustworthy and authentic digital identities. However, blockchain technology is burdened by multiple issues, especially those related to energy consumption and scalability. Considering the decentralized characteristics of blockchain, an increase in transaction volume could result in substantial delays and elevated costs, as each transaction necessitates authentication from multiple nodes throughout the network. This scalability represents a substantial barrier to the widespread adoption of blockchain technology in digital identity systems, where prompt and efficient processing is crucial (Zheng et al., 2017).

Although advancements in biometric and blockchain technologies have significantly influenced digital identification systems, their inherent limitations underscore the challenges associated with their successful implementation. To address these challenges effectively, it is essential to embrace a holistic strategy that evaluates the technological, practical, ethical, and environmental aspects of digital identity systems. Further research and development are required to overcome these hurdles and unlock the full potential of these technologies for enhancing digital identity management.

The second constraint pertains to institutional barriers to the implementation of Digital Identity Systems. The effective implementation of digital identity systems is frequently obstructed by substantial institutional barriers that exhibit considerable variability across regions, thereby affecting the accessibility and efficacy of these technologies. Tan et al. (2023) highlighted that disparities in technological infrastructure are pivotal, particularly in developing nations where contemporary digital frameworks may be deficient. This inequality directly affects the capacity to integrate and operate advanced digital identity systems.

A robust technological infrastructure that facilitates the seamless integration and functionality of sophisticated digital identity systems is typically advantageous to developed nations. Conversely, the comparatively underdeveloped technological frameworks in emerging economies impede the efficacy and reliability of such systems. The imperative for real-time processing and verification capabilities in digital identification systems can be significantly compromised by antiquated telecommunications and insufficient high-speed Internet connectivity, thereby diminishing the overall effectiveness of the systems (Tan et al., 2023).

The population’s digital literacy levelis another critical factor that influences the extent to which digital identification technologies are embraced and their overall success. Sullivan et al. (2023) observes that higher levels of digital literacy correlate with more straightforward adoption and more efficient utilization of these technologies. Conversely, individuals residing in regions characterized by low digital literacy levels may encounter difficulties when attempting to utilize digital identity systems and may even exhibit reluctance to adopt them. Authorities must launch

programs focused on improving digital skills to enable individuals to navigate online spaces safely and efficiently.

The thriving use of digital identity systems relies on essential financial and logistical support from the government, together with the development of legislative and regulatory frameworks. Degen et al. (2024) posited that the absence of political will or governmental resources may significantly impede the advancement and implementation of these systems in certain areas. A contributing factor to this dilemma is the lack of straightforward regulatory guidelines, leading to legal vagueness that could discourage involvement and funding from both the government and private organizations.

Furthermore, the requirement for legal adherence in worldwide activities relies on the synchronization of domestic laws with global data safeguarding benchmarks, such as the GDPR. In their analysis of misalignments, Cao et al. (2023) explained how such discrepancies can engender legal complications and inhibit multinational corporations from implementing their systems in non-compliant jurisdictions, thereby further isolating them from technological advancements.

To address the institutional obstacles to deploying digital identity systems, it is vital for governmental organizations, global entities, and local stakeholders to join forces. This collaboration should focus on enhancing technological infrastructure, advancing digital literacy, and harmonizing legal frameworks. These initiatives are crucial for ensuring that the benefits of technology are distributed fairly, while also enhancing inclusive growth and participation in the international digital economy.

The challenges and constraints associated with digital identity systems highlight the complexity of realizing their full potential. Table 2 presents these challenges and their implications. The development of a fair, inclusive, and efficient global digital identity management system requires the resolution of these concerns. Progress in education, infrastructure, and regulatory frameworks is essential to overcome institutional obstacles; however, technological limitations, such as blockchain and biometrics, demand ongoing innovation.

TABLE 2. Summary of Challenges and Constraints in Digital Identity Systems

Challenge/Constraint	Description	Key Implications
Regulatory Compliance	Varying data protection and privacy laws across regions require strict compliance with them.	Legal barriers, need for adaptation to diverse laws.
Technological Limitations	Biometric inaccuracies and blockchain scalability issues limit effectiveness.	Need for advanced sensor technology and improved scalability.
Security Threats	Phishing, malware, MitM, SQL injection, and DDoS attacks.	Continuous innovation in security strategies is required.
Institutional Barriers	Differences in technological infrastructure and digital literacy across regions.	Challenges in adoption and operation in less developed areas.

Privacy Concerns	Centralized systems pose the risk of massive data breaches. Decentralization can help address these issues.	Management of encryption keys and secure data handling.

KEY ELEMENTS OF WEB3 DIGITAL IDENTITY AUTHENTICATION.

Petcu et al. (2023) proposed a framework for managing decentralized digital identities using Ethereum blockchain technology. The fundamental components are listed in Table 3. This framework guarantees that digital identities are resilient and maintained under personal jurisdiction in accordance with the foundational principles of Web3. Thus, this approach aligns with the broader Self-Sovereign Identity (SSI) paradigm, which suggests that a digital identity must be user-centric, portable, and independent of any single centralized authority. As Mühle et al. (2018) emphasized, SSI is governed by ten principles: existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and protection. Together, these principles outline a vision in which the identity holder maintains the ultimate authority over their digital presence. This mechanism not only bolsters security and privacy but also enhances interoperability and user convenience, thereby rendering the management of digital identities across various platforms and services more efficient and accessible. The theoretical foundation of these objectives can be traced back to Cameron's Seven Laws of Identity, which assert that users must have control over how their identity information is shared, that only the minimum necessary data should be disclosed, and that interoperability across diverse architectures must be a fundamental system property (Soltani et al., 2021). Furthermore, Soltani et al. (2021) elaborate that these laws have served as the philosophical precursor to the SSI paradigm and continue to guide the design criteria for modern, decentralized identity systems.

Bambacht and Pouwelse (2022) have introduced a framework that fundamentally seeks to challenge and transform the conventional centralized system that presently governs digital identities, financial transactions, and data exchanges. The transition to Web3 infrastructure is propelled by the necessity for increased transparency, security, and user autonomy, addressing enduring concerns such as data privacy, trust in the financial system, and identity security. The transformation is best comprehended through the identity management evolution model, which maps the shift from isolated and centralized identity systems to federated and user-centric models, culminating in the self-sovereign identity paradigm (Čučko & Turkanović, 2021). Each phase in this sequence addresses the specific shortcomings of its predecessor. For instance, isolated models compel users to maintain distinct credentials for each service provider, whereas centralized models introduce single points of failure, making them vulnerable to extensive data breaches. Federated models, such as SAML and OpenID Connect, facilitate cross-domain authentication but still depend on intermediary identity providers (Sedlmeir et al., 2021). Bambacht and Pouwelse's (2022) initiative acts as a powerful appeal for society to move towards a decentralized digital landscape, where power and control are shared among all members rather than being concentrated in the hands of a few. This vision encompasses not only the implementation of innovative technologies but also advocacy for cultural and philosophical transformation towards enhanced equality, transparency, and collaboration in digital engagement. According to Giannopoulou (2023), the transition to self-sovereign identity is not just a technological change but a societal one, demanding a fundamental reimagining of how individuals, institutions, and the digital infrastructure interact to mediate trust.

The framework devised by Lai et al. (2023) regarding Web3 technology emphasizes a decentralized architecture comprising essential components aimed at addressing challenges related to limited user permissions and privacy. As articulated in their study, the fundamental principle of Web3 is to establish a user-centric, secure, and interoperable Internet environment. The framework posits that this represents a significant departure from the traditional centralized web architecture, which is anticipated to augment user control, enhance privacy, and strengthen the security. The authors aspired to empower users by reinstating their control and ownership of their data and interactions. From a theoretical standpoint, this empowerment is closely tied to the concept of the identity lifecycle, which encompasses the entire trajectory of a digital identity—from its initial provisioning and credential issuance, through active authentication and management, to its eventual revocation or decommissioning (Ma et al., 2022). Soltani et al. (2021) outlined the critical operations of this lifecycle as identification, verification, authentication, and authorization, each representing a distinct yet interconnected phase that must be integrated into a cohesive framework. In the SSI paradigm, the identity holder, rather than an external authority, controls each phase of this lifecycle, thereby fundamentally shifting the power dynamics inherent in digital identity management (Ferdous et al., 2019). This comprehensive approach to Web3 development encompasses technical, operational, and strategic dimensions, thereby offering a holistic roadmap for the future of decentralized digital interactions.

By synthesizing the existing studies, the fundamental elements of Web3 digital identity authentication encompass decentralized identifiers (DIDs), Verifiable Credentials (VCs), Smart Contracts, Interoperability Protocols, User Control, Security Mechanisms, and Privacy Enhancements. These elements are not isolated; they operate as interconnected parts within a unified system. The W3C Verifiable Credentials Data Model formalizes this interconnectedness through a trust triangle involving three key participants: the Issuer, who generates and cryptographically signs credentials to verify specific attributes; the Holder, who manages, stores, and selectively shares these credentials; and the Verifier, who confirms the credential's validity and the issuer's reliability without the need for a centralized authority (Schardong & Custódio, 2022; Mühle et al., 2018). This tripartite framework underpins the Web3 digital identity ecosystem, ensuring that trust is built on cryptographic validation rather than traditional institutional authority (Sedlmeir et al., 2021).

Decentralized Identifiers (DIDs) are imperative for establishing user-governed digital identities, eliminating dependence on centralized authorities, and mitigating the risks associated with centralized data management. DIDs bolster privacy and empower users to regulate the disclosure of their identity information, which is essential for preserving user autonomy during digital engagement. The W3C Decentralized Identifiers specification introduced DIDs as a novel form of globally unique identifier, which is generated, owned, and managed independently by the identity subject, without the need for authorization from any centralized registry or certificate authority (Mühle et al., 2018). Theoretically, DIDs embody the principles of Self-Sovereign Identity (SSI), namely existence, control, and persistence, by allowing individuals to create self-authenticating identifiers linked to a distributed ledger. This ensures that the identifier remains under the subject's control throughout its entire life cycle (Schardong and Custódio, 2022). Nevertheless, the deployment of DIDs encounters obstacles concerning interoperability and user education, necessitating a resolution to facilitate broader acceptance. Mühle et al. (2018) emphasize that DIDs

must contend with Zooko's Triangle, which involves the challenge of creating identifiers that are secure, decentralized, and human meaningful. Blockchain technology offers a potential solution by enabling decentralized verification without compromising cryptographic security.

Verifiable Credentials (VCs) serve as a mechanism for augmenting trust and optimizing identity verification procedures across decentralized networks. VCs provide users with the capability to present proof of identity without disclosing any underlying personal data, thereby enhancing privacy and security (Gunasinghe et al., 2019). These credentials are digitally signed by reputable issuers and can be verified throughout the network without requiring a central verification authority, thereby promoting user autonomy and reducing fraud risk. The operational logic of VCs is based on the W3C Verifiable Credentials Data Model, which defines a credential as a collection of tamper-evident claims accompanied by cryptographic metadata. This setup allows any relying party to verify both the integrity of the credential and the identity of the issuer (Schardong & Custódio, 2022). A significant advancement within this model is the concept of Verifiable Presentations (VPs), which enables holders to create selective disclosures. This means that they can share only the claims necessary for a specific transaction, often using Zero-Knowledge Proofs (ZKPs) to validate attribute predicates without revealing the underlying data (Ma et al., 2022). This mechanism directly implements SSI principles of minimal disclosure and data minimization, thereby embedding privacy preservation into the framework of credential exchange (Sedlmeir et al. 2021).

Smart contracts facilitate the automation of interactions and agreements directly on the blockchain, offering a transparent and tamper-resistant mechanism for managing digital identities (Liu et al., 2024). They play a crucial role in automating identity verification processes, minimizing the potential for human error, and enhancing transaction efficiency. Despite their advantages, smart contracts remain vulnerable to threats arising from coding errors, necessitating thorough testing and auditing to ensure security. Within the SSI ecosystem, smart contracts function as a programmable trust layer, facilitating the registration, resolution, and revocation of decentralized identifiers and credentials without the need for administrative intermediaries (Mühle et al., 2018). Mühle et al. (2018) specifically identify two primary architectural approaches: the Identifier Registry Model and its extension, the Claim Registry Model. Both approaches employ smart contracts to maintain immutable mappings between identifiers and authentication keys, as well as the cryptographic fingerprints of the issued credentials on the blockchain. This architecture ensures that the lifecycle operations of digital identities, including creation, modification, and revocation, are executed transparently and can be audited by all network participants (Dunphy & Petitcolas, 2018).

Interoperability protocols are vital for seamlessly integrating Web3 identities across diverse blockchain platforms, thereby facilitating a consistent and cohesive user experience (Lv et al., 2024). These protocols help overcome the fragmentation inherent in blockchain ecosystems, permitting the recognition and utilization of digital identities across various systems and applications. However, the development of these protocols presents substantial technical challenges that require further research and standardization. The theoretical foundation for interoperability lies in the SSI principle, which asserts that self-sovereign identities should be broadly applicable across various boundaries, jurisdictions and architectures (Soltani et al., 2021). To address this challenge, the W3C Decentralized Identifier specification established a universal

DID resolution mechanism. This mechanism abstracts the underlying blockchain or distributed ledger, allowing identifiers from diverse systems to be resolved through a common protocol layer (Mühle et al., 2018; Čučko and Turkanović, 2021). As demonstrated by Čučko and Turkanović (2021), the widespread adoption of DID methods across platforms such as Sovrin, Ethereum, and Hyperledger highlights the urgent need for standardized resolution and interoperability frameworks to prevent ecosystem fragmentation.

User control over personal data is a fundamental principle of Web3 identity systems that empowers individuals to oversee their digital footprints (Gebre et al., 2024). This empowerment fosters compliance with global privacy regulations and cultivates trust in the digital services. Nonetheless, enhanced control requires users to possess or acquire a certain degree of digital literacy to manage their identity effectively. The emphasis on user control in Web3 identity architectures is directly influenced by the SSI property taxonomy outlined by Ferdous et al. (2019). This taxonomy categorizes the fundamental attributes of self-sovereign systems into systematically organized groups, including security, control, and portability issues. Within this framework, controllability includes the properties of optionality, selective disclosure, and informed consent, each requiring that the identity holder maintain decision-making authority over which attributes are shared, with whom, and under what conditions (Ma et al., 2022; Ferdous et al., 2019). This classification refines and extends the original SSI principles by offering a more detailed analytical framework for assessing the extent to which a given Web3 identity system achieves true user sovereignty (Schardong & Custódio, 2022).

The security mechanisms in Web3 structures are designed to safeguard the integrity and confidentiality of digital identities, thus shielding them from unauthorized intrusions and cyber threats. Advanced encryption methodologies and consensus algorithms have been utilized to bolster security; however, they must evolve continuously to address emerging and novel security threats. From a theoretical perspective, the security framework of Web3 identity systems is shaped by the classic information security triad of confidentiality, integrity, and availability, which is enhanced by the specific demands of decentralized environments (Dunphy & Petitcolas, 2018). Dunphy and Petitcolas (2018) illustrate that blockchain-based identity systems present unique security trade-offs, where the immutability of recorded transactions must be weighed against the practical need for credential revocation and identity lifecycle management. Furthermore, the implementation of decentralized public key infrastructure (DPKI) in SSI systems replaces traditional Certificate Authorities with blockchain-anchored key management, thus eliminating the single point of trust failure inherent in conventional PKI models while maintaining the cryptographic rigor essential for secure authentication (Mühle et al., 2018; Soltani et al., 2021). Soltani et al. (2021) observed that in DPKI, the blockchain ledger acts as a tamper-evident registry of public keys and authentication metadata, distributing the trust establishment process across the network rather than concentrating it within a single issuing authority.

Privacy-focused technologies, such as zero-knowledge proofs, are used in Web3 ecosystems to help users validate their identity assertions without revealing sensitive personal information (Liu et al., 2024). These technologies offer robust privacy safeguards; however, they may introduce complexities and performance overheads that require careful management. The integration of Zero-Knowledge Proofs (ZKPs) into Web3 identity systems exemplifies a sophisticated application of the privacy-by-design principle, allowing for the selective disclosure of verifiable

claims without revealing any information beyond the assertion's validity (Schardong & Custódio, 2022). Ma et al. (2022) formalize this concept through a Policy Verifiable Claim (PVC) model, where verifiable credentials are encapsulated within policy-controlled signatures. These signatures enforce fine-grained access control over identity attributes, ensuring that only verifiers who meet the holder's predefined access policy can complete the verification. This approach enhances the privacy mechanisms of Web3 identity systems beyond basic anonymization, offering a formally verified framework for privacy-preserving authentication that meets the controllability, security, and flexibility criteria outlined in the SSI taxonomy.

TABLE 3. Architecture Comparison

Component	Petcu's Framework (2023)	Bambacht and Pouwelse's Framework (2022)	Yiwei Lai's Framework (2023)
Decentralized Identifiers (DIDs)	Described as fundamental for decentralized digital identity, facilitating anonymous authentication and transactions.	Utilized for ensuring user autonomy and privacy, essential for self-sovereign identity.	Employs DIDs for secure, tamper-proof identity verification without centralized authorities.
Verifiable Credentials (VC)	Not explicitly detailed in framework, potential for integration into the system for enhanced trust and credential verification.	Utilizes VC for reinforcing the security and authenticity of identity claims, crucial for maintaining a trusted digital environment.	Emphasizes the role of VCs in enabling secure and privacy-preserving verification processes across decentralized networks.
Smart Contracts	Smart contracts enable immutable and transparent operations on the blockchain, crucial for trust and automation in Web 3.0 environments.	Applied in self-sovereign identity systems to automate identity verification and reduce reliance on central authorities.	Used to automate and secure transactions and agreements, integral to maintaining decentralized storage and operations.
Interoperability Protocols	Not explicitly discussed in the context of interoperability but emphasized decentralized operation across various blockchain applications.	Stressed the need for interoperable frameworks to ensure seamless operations across different blockchain platforms.	Highlights the use of standard protocols to enhance cross-platform communication and verification.
User Control	User control is a primary focus, enabling users to manage their identities and transactions directly without intermediaries.	Emphasizes user empowerment through control over identity verification processes and data sharing.	Individuals have complete control over their identity data, deciding when and where to share their information.
Security Mechanisms	Prioritizes robust encryption and security protocols to protect user data and transactions from unauthorized access.	Incorporates advanced cryptographic methods to safeguard user data and ensure privacy in digital interactions.	Uses decentralized security measures to protect against breaches and ensure data integrity.

Privacy Enhancements	Emphasizes privacy through anonymous interactions and reducing traceability on the blockchain.	Privacy by design; minimizes data exposure and enhances user privacy through decentralized architectures.	Strong focus on protecting personal privacy with mechanisms that allow for secure, private data exchanges without revealing underlying personal data.

FRAMEWORK FOR WEB3 DIGITAL IDENTITY AUTHENTICATION SYSTEMS

This section delineates the conceptual framework meticulously crafted to enhance the efficacy of Web3 digital identity authentication systems. The framework is based on insights derived from existing studies and incorporates decentralized identifiers (DIDs), verifiable credentials (VCs), smart contracts, and user-centric security mechanisms as the fundamental elements of its construction. Through the integration of these pivotal components, this model aims to tackle fundamental issues such as privacy, security, and user autonomy within existing systems, thereby fostering digital identity management towards a more secure, transparent, and user-directed paradigm.

Current digital identity authentication methodologies, particularly those based on centralized management, provide a modicum of security. However, their centralized storage attributes render users' personal information susceptible to cyberattacks. Furthermore, these systems typically lack adequate transparency, and users experience restricted control over their data. To address these challenges, this conceptual framework advocates a decentralized solution grounded in blockchain technology that can offer an elevated level of security and complete user autonomy. Figure 1 illustrates the critical core of the proposed framework.

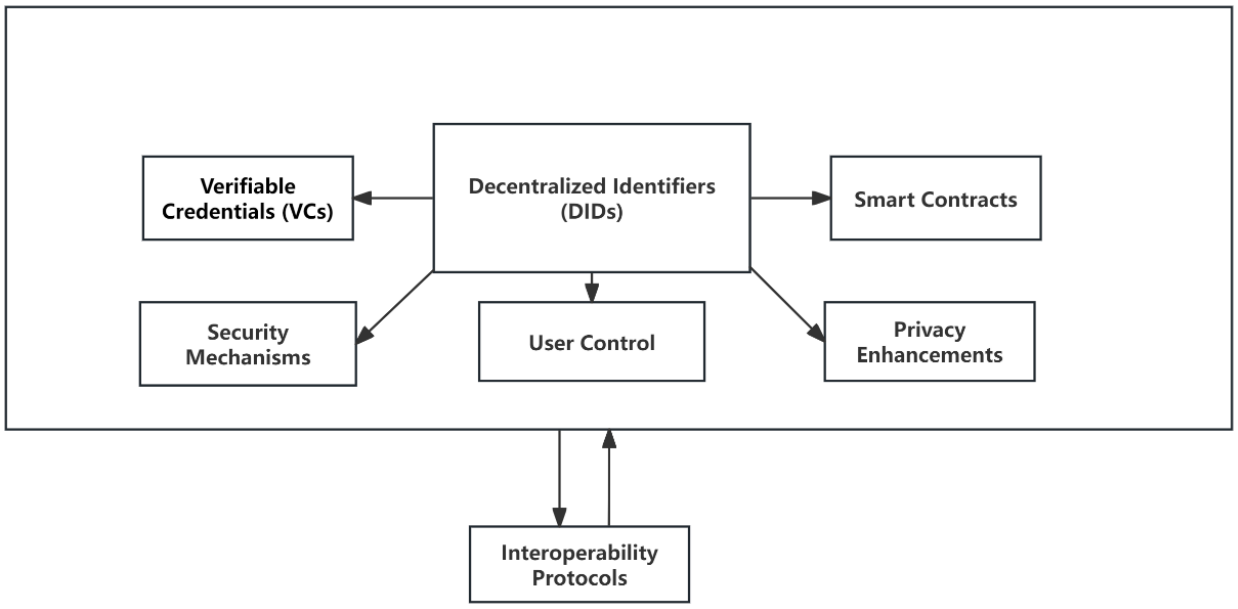

FIGURE 1. Framework for web3 digital identity authentication systems

The centralized identifier (DIDS) is positioned at the center of the diagram, signifying its pivotal function within the identity authentication framework. The Decentralized Identifier (DID) serves as a distinctive and enduring identifier for individuals across diverse Web3 services, acting as the nexus that links all other elements. The placement of a centralized identifier (DIDS) at the center plays a fundamental role in upholding the consistency and security of user identities.

Verifiable credentials (VCs) and smart contracts are situated on the left and right flanks of the centralized identifier (DIDS), indicating that they represent the principal technologies that directly engage with the centralized identifier (DIDS). Verifiable credentials are employed to substantiate the attributes or identities of users, whereas smart contracts facilitate the automation of the verification procedure for these proofs. This configuration underscores the direct involvement of VCs and smart contracts in the execution of centralized identifier (DIDS) authentication.

The user control component is positioned beneath the centralized identifier (DIDS) and is directly linked, illustrating the significance of users exercising control over their identity. This design layout indicates that the empowerment of users regarding their identity information is reinforced by a centralized identifier (DIDS), accentuating the principle of user sovereignty, wherein users are regarded as legitimate proprietors of their identity data.

The security mechanism and privacy enhancement components are in the lower left and right corners of the diagram, corresponding to the VCs and smart contracts, respectively. This arrangement accentuates the notion that security and privacy measures are essential supporting elements of the identity authentication system, which ensures the integrity of the authentication process and the confidentiality of user data.

Finally, the interoperability protocol component is situated at the base of the entire configuration and provides support for all elements. This positioning illustrates that interoperability serves as the foundation for the comprehensive functionality of an identity authentication system across various networks and services, functioning as a conduit that connects all components. This framework diagram effectively delineates the relationships and interactions among the components, as well as the role and significance of each component in the identity authentication process.

CONCLUSIONS

In conclusion, the advent of Web3 technologies has led to a transformative era in digital identity management, marked by a paradigm shift towards decentralization, user autonomy, and enhanced security. This evolution is a direct response to the limitations of traditional centralized systems, which are inherently vulnerable to cyber threats and often compromise user control over personal data ownership. Web3 digital identity authentication systems, which leverage blockchain technology and decentralized identifiers (DIDs), empower users to manage their identities independently, thereby fostering a more secure and trustworthy digital landscape. However, these systems also present unique challenges, including the complexities of managing cryptographic keys and the potential for irreversible data modifications on the blockchain. Furthermore, regulatory compliance and interoperability across diverse platforms remain significant challenges. Despite these challenges, Web3 digital identity systems hold immense promise. They utilize verifiable credentials and smart contracts to enhance trust and automate identity verification processes, thereby reducing fraud risk. The integration of interoperability protocols ensures

seamless identity management across blockchain platforms, providing consistent user experience. To fully realize the potential of these systems, it is crucial to address critical issues such as user privacy, security vulnerabilities, and regulatory adherence. The global regulatory environment, characterized by diverse and evolving standards, poses significant compliance challenges for entities operating internationally. By focusing on user-centric design and scalability, a secure Web3 digital identity authentication framework can overcome the limitations of existing centralized systems, ultimately enhancing privacy, security, and user control in the digital space. The success of Web3 digital identity systems hinges on the interplay between technological innovation, regulatory compliance, and user education, ensuring that these systems contribute to a more secure and trustworthy digital identity ecosystem. To transition the proposed framework from its current conceptual formulation to operational deployment, it will be validated through simulations, expert reviews, or comparative studies. While the present study contributes a comprehensive conceptual framework grounded in established theoretical constructs and a critical synthesis of the extant literature, the framework has not yet been subjected to empirical validation. For future work, the proposed framework should be rigorously evaluated using multiple complementary methodologies to establish its practical efficacy and generalizability.

ACKNOWLEDGEMENT

The authors would like to thank the Ministry of Higher Education for their support through grant FRGS/1/2023/ICT07/UKM/02/3 Finally, we show gratitude to Universiti Kebangsaan Malaysia and the Faculty of Information Science and Technology.

REFERENCES

Abbas, E., van Velzen, T., Ofe, H. A., Kaa, G. V. de, Zuiderwijk, A., & Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electronic Markets*, *34*, 20.

Abou-Tair, D. el D. I., Haddad, R., Khalifeh, A., Alouneh, S., & Obermaisser, R. (2023). A Distributed and Secure Self-Sovereign-Based Framework for Systems of Systems. *Sensors*, *23*(17), 7617.

Alenezi, M. N., Alabdulrazzaq, H. K., Alshaher, A. A., & Alkharang, M. M. (2022). Evolution of Malware Threats and Techniques: a Review. *International Journal of Communication Networks and Information Security (IJCNIS)*, 12(3).

Ali, S., Razzaque, A., Yousaf, M., & Shan, R. us. (2024). An Automated Compliance Framework for Critical Infrastructure Security through Artificial Intelligence, *IEEE Access*, 13, 4436-4459.

Bambacht, J., & Pouwelse, J. (2022). Web3: A Decentralized Societal Infrastructure for Identity, Trust, Money, and Data. arXiv:2203.00398.

Bashir, I. (2020). Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more. Birmingham, UK: Packt Publishing Ltd.

Belostecinic, G. (2023). Digital Marketing – a New Stage in the Evolution of the Modern Marketing Concept. *Economica*, 1(123), 7–22.

Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper. (Available at:

https://blockchainlab.com/pdf/Ethereum_white_paper_a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf).

Cao, B., Yan, Z., & Xia, X. (2023). Web3. *IEEE Communications Magazine*, 61(8), 18–19.

Cao, Y., Jiang, F., Xiao, J., Chen, S., Shao, X., & Wu, C. (2023). SCcheck: A Novel Graph-driven and Attention-enabled Smart Contract Vulnerability Detection Framework for Web 3.0 Ecosystem. *IEEE Transactions on Network Science and Engineering*, 11 (5), 4007-4019.

Čučko, Š., & Turkanović, M. (2021). Decentralised and self-sovereign identity: A systematic mapping study. IEEE Access, 9, 139009–139027.

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, 34(50).

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 16(4), 20–29.

European Commission. (2016). General Data Protection Regulation (GDPR). Retrieved from https://ec.europa.eu.

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. IEEE Access, 7, 103059–103079.

Fröhlich, M., Gutjahr, F., & Alt, F. (2020). Don't lose your coin! Investigating Security Practices of Cryptocurrency Users. *Designing Interactive Systems*, 1751–1763.

Gebre, D., Hadish, S., Sbhatu, A., Aloqaily, M., & Guizani, M. (2024) Establishing Trust and Security in Decentralized Metaverse: A Web 3.0 Approach. ACM Trans. Multimedia Comput. Commun. Appl. 20, 12, Article 389.

Ghadge, N. (2024). Challenges with Securing Digital Identity. *International Journal on Cybernetics & Informatics*, *13*(4), 01–08.

Ghosh, A., Lavanya, Hassija, V., Chamola, V., & A. El Saddik A. 2024. A Survey on Decentralized Metaverse Using Blockchain and Web 3.0 Technologies, Applications, and More, *IEEE Access*, 12, 146915-146948.

Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. Digital Society, 2(2), 18.

Golladay, K. A., & Holtfreter, K. (2017). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims & Offenders*, 12(5), 741–760.

Gunasinghe, H., Kundu, A., Bertino, E., Krawczyk, H., Chari, S., Singh, K., & Su, D. (2019). PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets. In The World Wide Web Conference (WWW '19). Association for Computing Machinery, New York, NY, USA, 594–604.

Guo, S., Zhang, F., Guo, S., Xu, S., & Qi, F. (2023). Blockchain-Assisted Privacy-Preserving Data Computing Architecture for Web3. *IEEE Communications Magazine*, 61(8), 28–34.

Huh, S., Shim, M., Lee, J., Woo, S., Kim, H., & Lee, H. (2023). DID We Miss Anything?: Towards Privacy-Preserving Decentralized ID Architecture. *IEEE Transactions on Dependable and Secure Computing,* 20(6), 4881-4898.

Jena, S. K., Barik, R. C., & Priyadarshini, R. (2024). A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare. *Internet of Things*, 25, 101111.

Ke, T. T., & Sudhir, K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*, 69(8):4389-4412.

Lai Y, Yang J, Liu M, Li Y, Li S. (2023). Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. *Blockchains*. 1(2), 111-131.

Lin, Y.-L., Gao, Z., Du, H., Niyato, D., Kang, J., Deng, R., & Shen, X. S. (2022). A Unified Blockchain-Semantic Framework for Wireless Edge Intelligence Enabled Web 3.0. *IEEE Wireless Communications,* 31(2), 126-133.

Liu, J., Liang, Z., & Lyu, Q. (2024). Empowering Privacy Through Peer-Supervised Self-Sovereign Identity: Integrating Zero-Knowledge Proofs, Blockchain Oversight, and Peer Review Mechanism. *Sensors*, 24(24), 8136.

Liu, Y., Zhao, Z., Liu, J., Lin, X., Wu, Q., & Susilo, W. (2024). SS-DID: A Secure and Scalable Web3 Decentralized Identity Utilizing Multi-Layer Sharding Blockchain. *IEEE Internet of Things Journal*, 11 (15), 25694-25705.

Lv, Y., Feng, R., Ma, M., Zhu, M., Wu, H. Z., & Li, X. (2024). Reinventing Multi-User Authentication Security from Cross-Chain Perspective. *IEEE Transactions on Information Forensics and Security*, 19, 8908-8923.

Ma, B., Zheng, X., Zhao, C., Wang, Y., Wang, D., & Meng, B. (2022). A secure and decentralized SSI authentication protocol with privacy protection and fine-grained access control based on federated blockchain. PLoS ONE, 17(9), e0274748.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80–86.

Nita, S. L., & Mihailescu, M. I. (2024). A Novel Authentication Scheme Based on Verifiable Credentials Using Digital Identity in the Context of Web 3.0. *Electronics*, 13, 1137.

Panchekha, P., Harrelson, C. (2024) History of the Web, *Web Browser Engineering*, Oxford Academic.

Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D.A. (2023). A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology" *Applied Sciences* 13(4), 2231.

Popa, M., & Mazumdar, S. (2023). ChainDiscipline - Towards A Blockchain-IoT-Based Self-Sovereign Identity Management Framework. *IEEE Transactions on Services Computing*, 16(5), 3238 - 3251.

Ragab, M., Savateev, Y., Oliver, H. *et al.* (2024) ESPRESSO: A Framework to Empower Search on the Decentralized Web. *Data Sci. Eng.* 9, 431–448.

Sasada, T., Taenaka, Y., Kadobayashi, Y., & Fall, D. (2024). Web-Biometrics for User Authenticity Verification in Zero Trust Access Control. *IEEE Access*, 12, 129611-129622.

Schardong, F., & Custódio, R. (2022). Self-sovereign identity: A systematic review, mapping and taxonomy. Sensors, 22(15), 5641.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. Business & Information Systems Engineering, 63(5), 603–613.

Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. Security and Communication Networks, 2021, Article 8873429

Si, J.J., Sharma, T., & Wang, K.Y. (2024) Understanding User-Perceived Security Risks and Mitigation Strategies in the Web3 Ecosystem. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24). Association for Computing Machinery, New York, NY, USA, Article 974, 1–22.

Song, X., Xu, G., Huang, Y., & Liu, Y. (2025). Decentralized Authentication Scheme Incorporating Reputation and Attribute Signature for Cross-Web3 Applications. *IEEE Internet of Things Journal.*

Sridhar, S., Fang, E., & Fang, E. (2019). New vistas for marketing strategy: digital, data-rich, and developing market (D3) environments. *Journal of the Academy of Marketing Science*, *47*(6), 977–985.

Stallings, W. (2020). Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information Under the California Consumer Privacy Act. 18(1), 61–64.

Sullivan, C., & Tyson, S. (2023). A global digital identity for all: the next evolution. *Policy Design and Practice*, 6, 433-445.

Tan, K.-L., Chi, C.-H., & Lam, K.-Y. (2023). Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. *ACM Computing Surveys*, *56*, 1–36.

Wu, Y., Weng, J., Wang, Z., Wei, K., Wen, J., Lai, J., & Li, X. (2022). Attacks and Countermeasures on Privacy-Preserving Biometric Authentication Schemes, *IEEE Transactions on Dependable and Secure Computing*, 20(2), 1744-1755.

Xu, H., Zhang, X., Cui, Q., & Tao, X. (2023). A Dynamic Blockchain-Based Mutual Authenticating Identity Management System for Next-Generation Network, *IEEE Communications Magazine*, 61(8), 116-122.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data.