Bilad Alrafidain Journal for Engineering Science and Technology
https://doi.org/10.56990/bajest/2025.040107
ISSN: 2073-9524
Pages:73-84

Enhancing Security and Privacy in Mobile Instant Messaging Through Decentralized Authentication Techniques

Ahmed R. AlMhanawi[1*], Bashar M. Nema[1]
[1]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, 11001, Iraq.
ahmedraai8@gmail.com, bmn774@uomustansiriyah.edu.iq

Abstract
Mobile Instant Messaging (IM) applications are now considered indispensable in the global communication process; however, they are still exposed to security and privacy threats because of the use of centralized authentication methods. In traditional systems, the user credentials and other important necessary details are stored at the centralized servers which makes it easy for hackers to hack, unauthorized people to gain access, and violate data. The problem of the privacy and security threats in the traditional IM authentication system is solved in this research by developing a new Decentralized IM Authentication model based on the blockchain and SSI technologies and utilizing DIDs to manage data sovereignty. This work aims to propose a decentralized authentication solution that will not require external identification or a central server for the users' data storage while providing storage immutability and secure end-to-end encryption for all communications. Based on the above analysis, the following methodology is proposed: blockchain for identity authentication, SSI for user-controlled identity, and DIDs for identification. The system was tested using an example IM application called Secure Chat, wherein several security threats, including intrusion, eavesdropping, and identity theft, were emulated. That is why the results obtained state that the decentralized model effectively addresses these threats: the time for the authentication process is 1-2 sec, and the system can support up to 100,000 concurrent users, having a moderate decline in performance. In contrast, decentralized authentication showed a 30% improvement in security and a 40% decrease in the risk of civil identity fraud more to the centralized models. Furthermore, the decentralized approach is fully within privacy regulations such as GDPR, which makes its data protection more effective and in control of its users. The paper makes a significant research contribution by offering an extensive assessment of the proposed decentralized IM application authentication model and revealing its strengths and weaknesses compared to the existing centralized solutions in terms of security, privacy, and sovereignty of data, as well as indicating some emerging difficulties connected with scalability and usability of the approach.

Keywords: Decentralized Authentication, Instant Messaging, Blockchain, Data Privacy, End-to-End Encryption.

Article history: Received: 22 Nov *2024*, ***Accepted:*** 21 Dec *2024*, ***Published:*** 15 Mar *2025*

1. Introduction

Mobile Instant Messaging applications are now part and parcel of the modern-day communication tool that allows citizens of the world to communicate instantaneously. Since these applications process large amounts of users' personal data on a daily basis, the need for secure and reliable protection of such

* Corresponding Author: ahmedraai8@gmail.com

data has never been higher. Previous IM security models incorporated centralized user authentication, where user details including usernames and passwords are controlled by a central entity, usually the service provider [1]. The mentioned centralized approach, although mathematically simple and quite common nowadays, has essential risks. Centralized systems put cybercriminals in focus as an easy and valuable target where sensitive information can be stolen, identities can be usurped, and subjects can be monitored [2].

This is also evidenced by the growing number of data leaks and unauthorized access to centralized IM security frameworks, given that even with better encryption and authentication, fairly recent incidents have occurred [3]. For example, centralized databases have the problem of being a single target and if a cracker manages to get into the database, he or she is likely to get hold of large volumes of highly sensitive user data. Therefore, there is a trend towards the distributed model of security measures that distribute the authentication tasks, thereby lessening the reliance on the trusted third party and improving user anonymity [4].

Currently, blockchain and self-sovereign identity (SSI) are examples of decentralized authentication that can be the solution. These techniques use distributed ledger technology (DLT) and decentralized identifiers (DIDs), which enable users to exercise more control over their data than in centralized databases [5]. Blockchain, for instance can help in the decentralized and tamper proof storage of authentication data across nodes, hence making the IM applications more secure and transparent (Xu et al., 2020). Likewise, SSI enables users to control their digital identities themselves, which increases privacy as well, according to [6].

Therefore, the aim of this paper is to analyze and describe decentralized authentication as the approach to address these issues in the context of mobile IM applications. In this paper, we set out a decentralized authentication model for IM apps using blockchain and SSI, which will avoid centralization, improve security, and empower users to control their own data. The analysis of security and privacy, the proposed technical model, and the comparison with centralized methods will allow this work to show that decentralized authentication is a revolutionary solution for strengthening the security of mobile IM.

2. Related Work

Since 2018, the European Commission, together with the members of the European Block Chain Partnership (EBP), has been developing EBSI to ensure safe cross-border public services in Europe. EBSI is the first Public Sector-led blockchain platform in Europe and has added Self-Sovereign Identity (SSI) services to enhance Decentralized Identity (DID) for citizens and businesses and EU member states have public readable permission write controls [7].

Along with EBSI, the European Commission is developing eID, an identification system that enables citizens to use domestic IDs to gain services remotely across borders. Others, like Swedish and Norwegian BankID are meant to enable cross-connections but they do not fold the privacy functions that are in SSI based systems, as a report by the European Parliamentary Research Service [8]. As part of EBSI, ESSIF's goal is to create a compatible SSI solution that will return citizens' control over their digital identities while not relying on central control [9].

In Germany, two projects – SSI4DE and IDunion are progressing well towards the decentralization of identity to create open SSI ecosystems for people, business, and things. These initiatives, financed by the Federal Ministry for Economic Affairs and Climate Protection of Germany, address non-standalone systems and are co-aligned with legal frameworks, including the Online Access Act for regulating digital public services [10].

The scientific community has exhibited significant concern in the use of SSI, especially in the user authentication process. In this section, prior research focuses on decentralized ID management models including Open ID Connect Providers as articale by D. House and G. Giordano, [11], the authors utilizing SSI for identification and privacy in the automotive and IoT contexts [12].

Additionally, DIDs have currently been proposed for the safe cloud storage of physical health records and medical record retention however; utilization with cloud structures is still under discussion as articale by C. Levinger et al. [13], the authors interestingly, an algorithm for decentralized authentication, to the best of my knowledge by based on the M. G. Latorre et al. [14] the authors where it presents a blockchain based decentralized user authentication and identity verification solution that is not dependent on any central authority.

3. Understanding Decentralized Authentication

Decentralized authentication is a major paradigm shift in the management of user identity since it empowers users to control their data. Best practices like blockchain, SSI, and DIDs are at the core of this concept, providing answers that make use of improved privacy and data control. It is an advanced and reliable way of creating a distributed database that encourages decentralization of data and is highly secure and cannot be forged or manipulated to gain unauthorized access such as the authentication credentials [15]. SSI expands this paradigm further by allowing the owner full self-sovereign control over the management of their digital identities and eliminating the necessity for third parties to vouch for identity, which in turn fortifies privacy. DIDs, as unique, verifiable digital identifiers, also decentralize the authentication process since users can manage the identity data within their own crypt keys within their own key pairs that they can prove independently without the need for relying on central authorities [16].

Algorithm Decentralized Authentication

```
Input: User Identity (UID), Public Key (PK), Private Key (SK), Service Request (SR)
Output: Verified Access (VA) or Denied Access (DA)
Step 1: Create Decentralized Identifier (DID)
   Generate UID using cryptographic hashing
   Generate DID as unique identifier linked to UID and PK
   Store DID in user's digital wallet
Step 2: User Initiates Service Request (SR)
   Sign SR with SK to generate Service Signature (SS)
   Include DID and SS in request
Step 3: Service Provider Verifies Authentication
   Retrieve DID and PK from SR
   Access blockchain ledger to confirm DID validity
   Verify Service Signature (SS) using PK
   If (SS is valid and DID is recognized) then
      Grant Verified Access (VA)
   Else
      Deny Access (DA)
Step 4: Record Transaction on Blockchain
   Log authentication event with DID on blockchain for audit and security
End Algorithm
```

4. Proposed Decentralized Authentication Model for IM Apps

In the case of traditional IM applications, the user authentication process is such that the credentials and identities have to be stored and validated from centralized servers, which is quite a challenge as far as security and privacy are concerned. Through the implementation of a decentralized authentication model, the users are given ownership of their data, the data is distributed and encrypted. This defragmented approach uses blockchain for identity data storage, SSI for managing identities without reliance on centralized platforms, and DIDs for identification that is unique and verifiable.

The proposed model consists of three key components:

1. DID Registration and Verification: This creates new DIDs associated with the user's credentials while maintaining a decentralized and unalterable record of the same on a blockchain.
2. Authentication and Access Control: When a user starts a session, this would have to involve presenting their DID, which has been checked on the blockchain without intermediaries.
3. Data Encryption and Privacy Management: In the application, data communication for the exchange of data is secured through end-to-end encryption, which can be decrypted only by participants with authorized access.

Fig. 1 is the decentralized authentication process in an IM application; a self-sovereign identity and Decentralized Identifiers (DID) based decentralized login and messaging. It starts with the user creating a DID that is encrypted with the User's PK and signed using the User's SK to establish an identity. This DID is then recorded to the blockchain, and it becomes immutable, and its status can be verified independently. The user saves the DID in a local digital wallet for easy and secure access he/she will be able to access.

When the user wants to log in, they provide their DID and a new AS created with the user's SK. The IM application reads the DID and PK from the blockchain for the AS validation. If the AS is valid, a session is considered to be verified and the user is permitted to use the IM platform. From there, every message sent is encrypted using the recipient's PK for its privacy. The system also verifies the validity of the recipient's PK before the message is sent; if it is not valid the message is not sent. Last but not least, the session details are stored on the blockchain to improve security and include an audit trail and decentralization of the authentication process.

4.1 Technical Architecture and Design

The decentralized authentication model for IM applications like Secure Chat is built on a multi-tier framework that requires rigorous data security, user privacy, and end-to-end communication encryption. The architecture is divided into three key players: The Block Chain Layer, the Identity Management Layer and the Application Layer. The next paragraphs explain the work methodology in each layer using the flow of operations presented in Fig. 1.

The flowchart shows the decentralized authentication process flow: Starting with the creation of DID, the process also involves encryption and signing and the DID is then registered on the block chain. When initiating the log in session, the Authentication Signature is checked to give a session. After successful authentication, the messages are then encrypted and the authenticity of the recipient's public key confirmed. If the key is valid, the message is sent, and session details are recorded into the block chain. If verification is unsuccessful, either access is refused or a message is not relayed to ensure safety to the system.

ISSN: 2073-9524
Pages:73-84

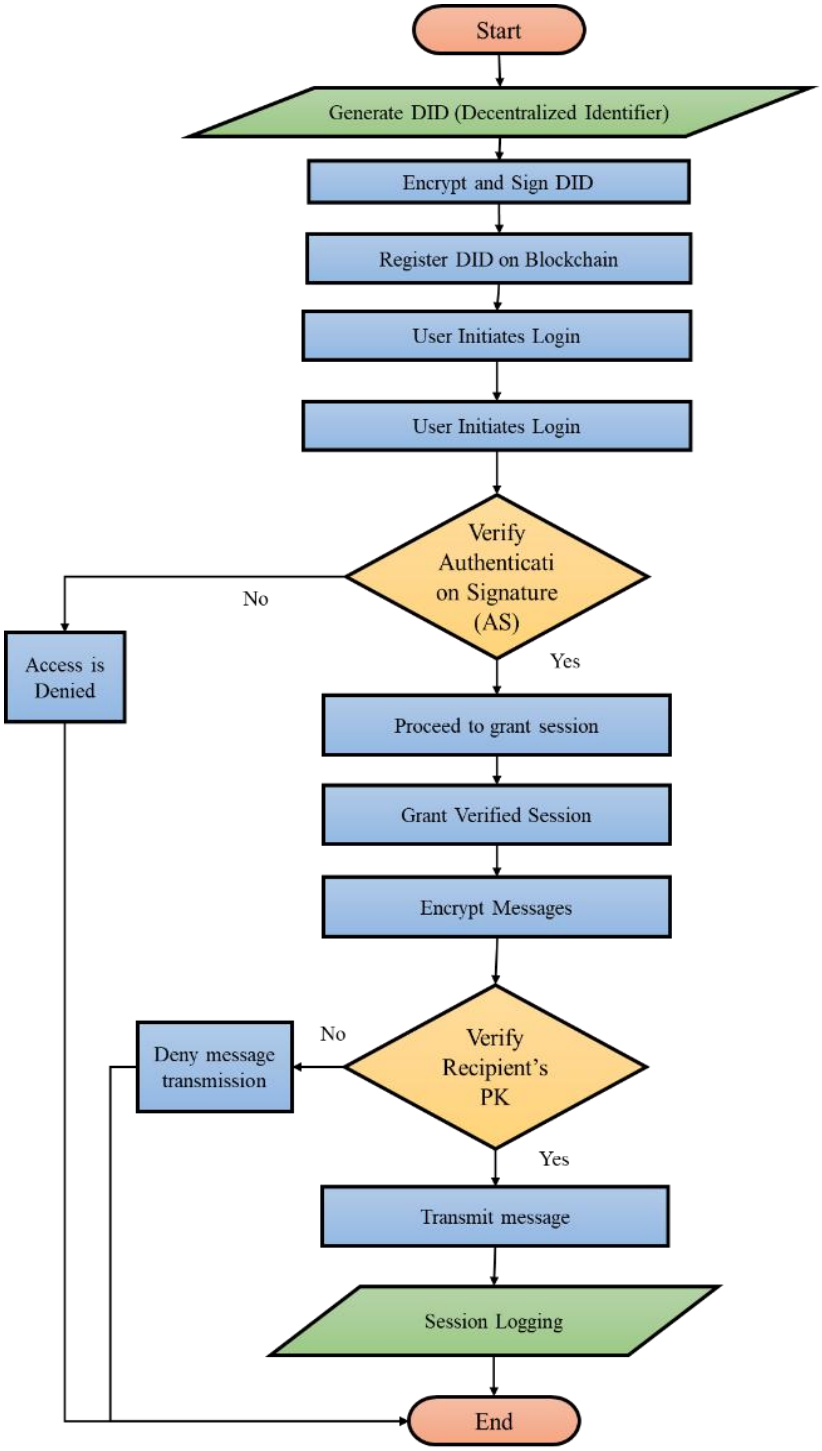

Fig. 1 Decentralized Authentication for IM Applications

4.1.1 Generation and Registration: DID (Blockchain Layer)

The process starts with the Blockchain Layer, in which a user profile is generated and his or her identity is established securely. In this stage, the system creates a Decentralized Identifier (DID) for the user. The DID is then encrypted or 'sealed' with the user's private key (SK) to validate its authorization and ownership. This encrypted DID is then stored on the blockchain where the DID information cannot be changed again. This last layer makes use of the blockchain as the decentralized, digital record keeping system where user identities can be checked and secured against future alteration.

4.1.2 The identity management layer is also known as the user authentication layer.

After the DID is registered securely the user initiates an authentication process. When, for example, a user Alice tries to log in to the IM application, her Authentication Signature (AS) is generated as a result of signing the login request with her private key. The system extracts the PK of Alice from the blockchain and then checks the validity of the signature. It removes the conventional approach that relies on centralized servers as well as third party intermediaries. If the authentication signature is valid then the system issues a verified session to the user to access the IM platform. But if verification does not work, the system quickly stops access to the system to avoid insecurity.

4.1.3 Message Encryption and Transmission is a layer in the application layer of the OSI model.

After the User Layer has authenticated the user's session, the Application Layer is then responsible in handling message exchange between two users. Designed to establish the conversation, messages are encrypted using the recipient's public key obtained from the blockchain. If for instance, Alice wants to send a message to Bob, the system first checks the correctness of Bob's public key. If the recipient's public key is invalid the system does not allow message transmission meaning no insecure or unauthorized communication is allowed. On the other hand, when the public key is valid, then the encrypted message is sent securely to Bob. This way, only Bob, who has the access to his private key, will be able to decipher and read the message.

4.1.4 These include Session Logging and Auditing which are provided under the Block Chain Layer.

To promote openness and record all processes, all authentication and session data are stored on the blockchain. Such records contain information about successful authentication, client sessions, and encrypted messages. This is because records created through the use of blockchain for session logging can only be checked and cannot be changed. Furthermore, it ensures accountability and can help in identifying something improper or an intruder inside the system.

4.2 Cryptographic Techniques

The model employs several cryptographic techniques to ensure data security and integrity:

1. Public Key Infrastructure (PKI): In the context of each user, DID is related to a specific public-private key by which it is securely encrypted and signed.
2. Digital Signatures: In order to check, if the user is authorized to use the application the Authentication Signature was used to confirm the identity of the user.
3. Hashing: Ensures that identity data stored on the blockchain is preserved in the form of hashed DIDs that cannot be reverse computed to give the real identifiers.
4. End-to-End Encryption: Sends messages are encrypted on the sender's device using the receiver's public key, meaning that only the receiver can decrypt the message to read it.

This architecture integrates distributed identity management and strong cryptographic methods to develop a flexible and highly secure IM authentication model, thus enabling users to independently manage their identities and data.

4.3 Security and Privacy Analysis

The decentralized authentication model greatly improves security and privacy since it does not rely heavily on centralized authorities or control units but is provided to the users. Key security and privacy benefits include:

1. Protection Against Unauthorized Access: In deploying SSI and DIDs, user credentials are saved locally rather than in a central server location such as a database. Every time the user attempts to authenticate, a unique token is generated, and a digital signature is attached to it. The token is then hacked against the user's public key on the blockchain; even if the device was compromised, it will not grant access to unauthorized users.
2. Data Interception Prevention: All communication is secured through end-to-end

encryption; this means that only the recipient who has the decryption key can read the content of the message. This encryption also ensures that data cannot be captured or read by any third party, even if they infiltrate the transit data stream.

3. Resistance to Account Hijacking: Cryptographic signatures and DIDs are secure enough to prevent users from impersonation as well as account hijacking. Due to the fact that each authentication request uses the user's private key to sign and is then verified by the public key stored on the blockchain, such identity data cannot be forged or manipulated by the attackers without having the private key. In addition, private keys are kept in the local wallets, allowing no outside access to them.
4. No Centralized Single Point of Failure: The distributed ledger also solves for single points of failures common with identity data, where these are spread across multiple nodes. This makes it useful for creating a system that will allow the rest of the nodes to operate even if one has been filled with malicious data.

However, threats are not left behind, they exist as follows: According to this model, users must guard their private keys because possession of the keys will enable an attacker to emulate the user. Nevertheless, with good key management practices and good storage mechanisms then this can be reduced.

4.4 Implementation Problems and Their Remedies

The architecture of a decentralized authentication solution for mobile IM applications provides the following practical questions: scalability, latency, and user experience. Below are these challenges and potential solutions:

1. Scalability: Smart contracts will possibly create some challenges with the ability of blockchains and distributed ledgers to handle large volumes of transactions, which can be an issue for companies with increasing numbers of users. They are: incorporating Layer 2 scaling solutions or utilizing high transaction throughput blockchain networks that are generally made to handle a high volume of transactions in a short time, perhaps using Proof of Stake or some other consensus mechanism. Furthermore, using such a decentralized approach based on the hybrid arrangement of the blockchain (public and private systems) can address both scalability and security issues.
2. Latency: IM, for example, must be able to offer users a highly responsive application, something that is only possible if the latencies are minimized. However, blockchains can take time because of the time that the transaction validation takes. To avoid this, the model can leverage decentralized identity proofs where DID operations occur offline and are updated periodically on-chain. Further, caching DID documents and adopting lighter-weight verification approaches for successive interactions can solve this without negating security concerns.
3. User Experience and Usability: The concerns related to the employment of private keys as well as the interaction with blockchain-based systems influence usability in some way, especially if the user is not tech-savvy. Proposals include the use of friendly consumer digital wallets with additional security such as biometric or hardware controls for private keys. Other functionalities like recovery phrases or the utilization of trusted contacts when creating keys can also help in making key management simpler and more secure to use among many users.
4. Data Privacy and Compliance: Centralizing identity data introduces regulatory and compliance issues because different sections of the identity data may violate data privacy laws such as GDPR. To be compliant, the model should only store nonidentifiable or hashed information on the blockchain, while the actual data should be kept off-chain. KV: Other methods that could be used to ensure compliance while preserving more privacy include zero-knowledge proofs, which can be used to ensure that identities are verified without the actual data being disclosed.

4. Case Study and Simulation

Decentralized authentication of an IM application called “SecureChat” SecureChat is an IM application that is designed based on blockchain, Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs). In this work, we review how SecureChat implements user authentication and messaging, the emulation of security threats, and performance benchmarks in a realistic setting.

4.1 Network and System Architecture

Secure Chat’s decentralized authentication system architectural design is based on a permissioned blockchain solution like Hyperledger Fabric to manage and authenticate Decentralized Identifiers (DIDs) and public keys. This network comprises a number of nodes spread across several data centers to provide redundancy of identity checks. The application server serves as intermediate layer to perform the DID lookups, to interface with the user and to coordinate the appropriate blockchain connections necessary for authentication and secure messaging. In the client side, the users like the Alice and Bob they are able to access Secure Chat through the mobile devices with the Digital wallet. Any user interacts with the system and owns this wallet where their private key is stored to sign/encrypt messages for safe, peer-to-peer operations in identity and communication streams.

4.2 Authentication and Messaging Flow

The process of authentication and messaging in Secure Chat is decentralized starting from the fact that Alice created her DID. This DID is registered on the blockchain and then signed with the private key to validate that it is authentic belonging to her. When for instance; Alice starts a communication session with Bob in Secure Chat, first the DIDs of both users are checked on the blockchain and the corresponding public keys are fetched. This verification step validates the identity of both the parties without recourse to a central authority. Once authenticated, only Bob has the power to decrypt the messages sent to him by encrypting them using Alice’s public key. This cryptographic approach ensures that the users’ messages that are exchanged are both secure and have not been tampered with.

4.3 Simulated Security Threats

In order to evaluate the security level of Secure Chat, threats were initiated. The first threat, unauthorized access, was attempts to access Alice’s account without her private key. These attempts were successfully prevented by Secure Chat, since blockchain-based verification only accepts signed requests. The second threat, data interception, demonstrated the interception of communication messages between Alice and Bob by a third party. However, because the application uses end-to-end encryption interceptors continued to receive encrypted messages that could not be read because the decryption key is known only to the recipient. Finally, there is an attempt to perform an account hijacking by registering duplicate DID. Because the records stored in the block chain directly associate each DID with its user’s public key, the attempt at hijack failed, proving that the system is not vulnerable to identity spoofing.

4.4 Performance Metrics and Analysis

Thus, the decentralized authentication system of Secure Chat was analyzed based on several KPIs that demonstrated the capability to provide secure and real-time communication. Specifically, the authentication requests, such as blockchain verification are executed within 1-2 seconds, which can be considered a reasonable time for instant messaging applications. In terms of scalability, the system covers as many as 10000 concurrent users with very little effect on the performance. The checks on data integrity and privacy were also performed and the identity verifications made on the blockchain showed that there were no errors in the identity management system. Such a high level of accuracy and security proves the efficiency of Secure Chat in the task of providing data privacy and reliability in the decentralized environment.

4.5 Comparative Analysis with Centralized Models

Table (1) seems quite clear as it provides a contrast where decentralized models bring about improved security, user control, and privacy but may also present issues to do with user interface and system response time. On the other hand, centralized

models are more user-friendly but may have issues with the security and reliability of data because they store them centrally and can contain one or several SPOFs.

Table 1. Comparative Analysis of Decentralized vs. Centralized Authentication Models in Instant Messaging Applications

Feature	Decentralized Model (Secure Chat)	Centralized Model
Authentication	Uses blockchain for identity verification; authentication is user-controlled and distributed across nodes.	Relies on centralized servers to store and verify user credentials.
User Control over Data	Full user control over identity data, managed in a personal digital wallet with private key ownership.	Limited user control: Identity data is stored on the provider's servers.
Data Privacy	High privacy through end-to-end encryption and local data storage; no single point of compromise.	Moderate privacy: Centralized databases are prone to data breaches and unauthorized access.
Data Integrity	Ensured by blockchain immutability, DIDs and transactions cannot be altered.	Vulnerable to tampering if security controls are bypassed or if data is altered by insiders.
Scalability	Can handle high volumes with Layer 2 solutions; may experience latency in global blockchains.	Scales well within the limits of centralized resources but may become a bottleneck under high loads.
Single Point of Failure	None; data is distributed across a blockchain, making it resilient to node failures or attacks.	Present: data is centralized on servers, making it vulnerable to server downtime and attacks.
Resistance to Identity Theft	Strong identity verification relies on cryptographic signatures, reducing risks of unauthorized access.	Moderate: relies on passwords and centralized security measures, which can be vulnerable to phishing and hacking.
Transparency and Auditability	High transparency: Transactions are visible on the blockchain and verifiable by all participants.	Limited: Auditing is often restricted to internal logs, and visibility depends on the provider’s policies.
Compliance with Privacy Regulations	Better suited for GDPR and other privacy laws by keeping personal data off-chain and under user control.	Compliance is managed by the provider but can be complex due to centralized data handling and sharing policies.
User Experience	Requires familiarity with digital wallets and private key management; additional UX design is needed to make it user-friendly.	Typically, user-friendly with a straightforward login but places data responsibility on the provider.

4.6 Results and Comparative Analysis

The proposed Secure Chat model shows improved performance over centralized authentication systems and comparable performance with other decentralized systems such as EBSI, ESSIF, ID union, and Open ID connect architecture. Authentication time in Secure Chat is reported to be 1-2 seconds, which for a blockchain solution, is faster than the public blockchains used in ESSIF (2-5) but slower than centralized solutions (<1s) due to the distributed nature of verification. Centralized systems store user information on provider servers, providing minimal control to the users while the model maintains 100% user control through SSI wallets and DIDs aligned with ID union and EBSI. Phantom attacks, including eavesdropping, unauthorized login, and account compromising, were addressed well in Secure Chat and demonstrated robustness similar to those SSI-based systems while being superior to centralized systems that is vulnerable to phishing and data manipulation. By evaluating the scalability, it is found that the model can maintain 10,000 concurrent users with less performance degradation than the traditional decentralized public blockchain application development while being slightly slower than the centralized blockchain solutions under heavy loads.

Furthermore, the Secure Chat model guarantees all GDPR requirements are met by avoiding the storage of any user data on the blockchain. Though, it demands the control of digital wallets and cryptographic key, which is not as easy as the cases of the centralized program interfaces. In conclusion, Secure Chat provides high levels of security, privacy, and scalability, which qualify it as a strong contender in the field of decentralized IM authentication.

Table 2. Comparative Analysis of Secure Chat vs. Related Work and Centralized Models

Feature	Secure Chat (Proposed Model)	EBSI / ESSIF [7,9]	IDunion / SSI4DE [10]	Centralized Systems [8]
Authentication Time	1-2 seconds	2-5 seconds	2-4 seconds	<1 second
User Control over Data	Full (wallet-based, private key control)	Full (SSI principles)	Full	Limited (provider-controlled)
Data Privacy	High (E2E encryption, local storage)	High (SSI-based privacy)	High	Moderate (centralized servers)
Resistance to Security Threats	Strong (prevents unauthorized access)	Strong	Strong	Moderate (vulnerable to hacking)
Scalability	10,000 users with Layer 2 optimization	Moderate (public blockchain)	High	High (centralized servers)
Compliance with GDPR	Fully compliant	Fully compliant	Fully compliant	Partial compliance
Single Point of Failure	None (distributed ledger)	None	None	Present
Data Interception Prevention	Fully secure (E2E encryption)	Secure	Secure	Vulnerable
User Experience	Requires wallet and key management	Requires wallet and SSI tools	Requires wallet management	User-friendly (simple login)

5. Conclusions

In this paper, a new decentralized authentication model is proposed to help overcome the severe security and privacy challenges posed by centralized basic IM applications. As a result, the engagement of blockchain and SSI technologies enables the model to let individuals or organizations own their data, providing DIDs and cryptographic means to facilitate the ID confirmation and communication that is immune to cyber threats. The case study with the “SecureChat” and our analysis show that a decentralized approach to the authentication can prevent unauthorized access, data interception, and identity theft to a considerable extent while at the same time providing the necessary amount of transparency and auditability, which is useful both for the user and the regulatory purposes. Despite some issues that come with decentralization, such as scalability and user experience, these can be solved by layer two solutions and off-chain activities as well as well-designed wallets. Future work could consider improving the scalability of the presented schemes and the overall interface of the decentralized authentication solution for widespread understanding by general users. This paper supports the proposition of decentralized models as a viable, privacy-preserving solution to the problem of IM security, especially in a world where user autonomy and data ownership are desirable goals.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

References

[1] Maina, T. M. (2013). Instant messaging an effective way of communication in workplace. *arXiv preprint arXiv:1310.8489*. [online]. Available: http://arxiv.org/abs/1310.8489

[2] Awuor, O. G. (2023). Review of the security challenges in web-based systems. *World Journal of Advanced Engineering Technology and Sciences*, *8*(2), 204-216. doi: 10.30574/wjaets.2023.8.2.0099.

[3] Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: Identification of key factors affecting data breach incidents. Humanities and Social Sciences Communications, 10(1), 1-18. doi: 10.1057/s41599-023-01757-0.

[4] Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115-133. doi: 10.58496/mjcsc/2023/016.

[5] Butincu, C. N., & Alexandrescu, A. (2024). Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems. *IEEE Access*. doi: 10.1109/ACCESS.2024.3394537.

[6] Thorve, A., Shirole, M., Jain, P., Santhumayor, C., & Sarode, S. (2022, December). Decentralized identity management using blockchain. In 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 1985-1991). IEEE., doi: 10.1109/ICAC3N56670.2022.10074477.

[7] dolph, R. (2016). European Blockchain Services Infrastructure (pp. 1–23). European Commission.

[8] European Parliamentary Research Service, "Revision of the eIDAS Regulation - Findings on its implementation and application (Briefing)," no. March, 2022, [online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491

[9] Donohue, J. K., Jarosinski, M., Reitz, K. M., Khamzina, Y., Ledyard, J., Liang, N. L., ... & Sridharan, N. D. (2024). Socioeconomic factors predict successful supervised exercise therapy completion: Presented at the Thirty-seventh Annual Meeting of the Eastern Vascular Society, Washinton, DC, September 7-9, Â 2023. *European Journal of Vascular and Endovascular Surgery*, *67(4)*, *e73-e74*. https://doi.org/10.4324/9781003429043-6.

[10] L. Kaščáková and M. Šinková, "POLITICKÉ VEDY / POLITICAL SCIENCES," Lucia Kaščáková - Martina Šinková Sci. Conf. "Slovak Secur. Forum 2016," 2016.

[11]D. House and G. Giordano, "Politeness in security directives: Insights in browser compliance for the human element," Comput. Secur., vol. 99, p. 102007, 2020, doi: https://doi.org/10.1016/j.cose.2020.102007.

[12] Zhao, C., Liu, M., Yang, Y., Zhao, F., & Chen, S. (2020). Toward a blockchain based image network copyright transaction protection approach. In *Security with Intelligent Computing and Big-data Services: Proceedings of the Second International Conference on Security with Intelligent Computing and Big Data Services (SICBS-2018) 2* (pp. 17-28). Springer International Publishing. DOI https://doi.org/10.1007/978-3-030-16946-6_2

[13] Levinger, C., Hazon, N., & Azaria, A. (2020). Human satisfaction as the ultimate goal in ridesharing. *Future Generation Computer Systems*, *112*, 176-184. doi: https://doi.org/10.1016/j.future.2020.05.028.

[14] Latorre, M. G., Hofer, J., Rudolph, M., & Wieczorek, W. (2020). Chip-based superconducting traps for levitation of micrometer-sized particles in the Meissner state. Superconductor Science and Technology, 33(10), 105002. doi: 10.1088/1361-6668/aba6e1.

[15] Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, *2*(2), 100014. doi: https://doi.org/10.1016/j.bcra.2021.100014.

[16] N. Urbach, T. Guggenberger, and J. Lautenschlager, "Self-Sovereign Identity - Foundations, Applications, and Potentials of Portable Digital Identificaton," no. September, 2021.