End to end encrypted chat application with secured backup

Dr. Raghavendra C K
Professor, Dept. of CSE
BNM Institute of Technology,
Bengaluru

Panchami N S
Dept. of CSE
BNM Institute of Technology,
Bengaluru

Prabhat Kumar Verma
Dept. of CSE
BNM Institute of Technology,
Bengaluru

Rushil Sati
Dept. of CSE
BNM Institute of Technology,
Bengaluru

Abstract - This paper introduces a cutting-edge chat application leveraging blockchain technology for data storage, aiming to address the escalating concerns surrounding online privacy and security. With the exponential growth of digital platforms and the escalating sophistication of cyber threats, safeguarding sensitive information has become paramount. Our solution offers a seamless and secure communication platform by harnessing the immutable and decentralized nature of blockchain. Through advanced encryption protocols and distributed ledger technology, our chat application ensures end-to-end encryption, data integrity, and resistance against unauthorized access. The user-friendly interface caters to individuals with diverse technical proficiencies, providing features such as encrypted messaging, secure file sharing, and decentralized storage. By combining the convenience of traditional messaging applications with the robust security afforded by blockchain, our project strives to redefine the landscape of secure digital communication.

Index Terms – Chat application, Blockchain technology, ,Immutable,Decentralized,End-to-end encryption,,Unauthorized access,Secure communicationplatform,Sensitiveinformation.

I. INTRODUCTION

In today's digital landscape, communication stands as the cornerstone of connectivity, facilitating interactions across vast distances. However, amidst the convenience of instant messaging and the ubiquity of online conversations, concerns regarding privacy and security loom large. It's within this backdrop that our project emerges, introducing a novel chat application poised to revolutionize digital communication.

Harnessing the power of Ethereum blockchain for storage, our chat application ensures the immutability and decentralization of data, fostering a secure environment where user conversations remain safeguarded from unauthorized access. Moreover, by integrating the x3DH protocol, our platform guarantees robust forward secrecy, enhancing confidentiality by generating unique session keys for each conversation.

But security doesn't end there. Leveraging RSA encryption, our chat application employs industry-leading cryptographic techniques to fortify message integrity and authenticity. Through asymmetric encryption, messages are secured with public keys, ensuring that only intended recipients possess the private key necessary for decryption.

As students passionate about technology and driven by a desire to innovate, our project represents a culmination of research, experimentation, and dedication. We recognize the significance of privacy in today's digital age and are committed to providing users with a

communication platform that prioritizes security without compromising on usability.

In the subsequent sections of this paper, we will delve deeper into the architecture, functionalities, and security measures employed in our chat application. Through a comprehensive analysis, we aim to elucidate the efficacy of our solution in addressing contemporary challenges surrounding digital communication. Join us on this journey as we explore the intersection of blockchain, encryption protocols, and user privacy in shaping the future of online conversations.

II. LITERATURE SURVEY

In reviewing the existing literature pertaining to chat applications leveraging Ethereum blockchain, x3DH protocol, and RSA encryption, several key themes emerge. Research highlights the growing importance of decentralized storage solutions, such as blockchain, in safeguarding user data and ensuring privacy. Additionally, studies emphasize the significance of cryptographic protocols like x3DH and RSA in securing communication channels and preventing unauthorized access. While there is a wealth of literature exploring each component individually, there is a gap in research that comprehensively evaluates the integration of these technologies in chat applications. Our project seeks to bridge this gap by implementing a holistic approach to secure digital communication.

The E2EE [1] Overview underscores the critical role of E2EE in safeguarding online communications, particularly in the face of government surveillance and potential man-in-the-middle attacks. It establishes the context for the subsequent analysis. Authentication Ceremonies receive meticulous scrutiny. The study evaluates various E2EE applications, focusing on their authentication processes. A notable finding emerges: existing ceremonies often fall short in effectively countering ongoing MitM attacks. Turning to Security & Usability, the document dissects the security features and user-friendliness of E2EE programs. Limitations: MitM attacks, Poor User Experience

The document[2] discusses a Blockchain-enabled End-to-End Encryption (E2EE) framework for instant messaging services, which addresses the privacy concerns raised by current messaging apps. It examines the flaws in current E2EE implementations, where service providers control critical portions of the encryption process and keep decryption keys, resulting in decreased user confidence. The study suggests a novel solution to addressing these challenges that employs blockchain technology to ensure true anonymity without allowing third parties access to secret keys. The architecture requires users to generate public/private key pairs during app installation, with mobile network providers (MNOs) issuing digital certificates stored on a public blockchain. This enables secure communication through a ratchet forward encryption technique. Limitations: Group messaging

This[3] a thorough examination of the building of a Decentralised Chat Application (DCA) using blockchain technology. The Decentralised Chat Application (DCA) uses blockchain technology to provide a safe and private chat platform. Decentralising infrastructure minimises centralised weaknesses, increasing security and resilience against network outages. Users have complete control over their information, which promotes trust and anonymity. The DCA is designed with encryption methods, blockchain connectivity, and a user-friendly interface, giving it a dependable alternative for safe communication. This study paves the way for future advancements in decentralised communication technologies. Limitations: Relatively high costs

Decentralized Communication[4] the document discusses "bChat," a decentralised chat programme meant to overcome security problems for message transmission across insecure channels.It identifies flaws in existing messaging systems, such as eavesdropping and man-in-the-middle (MITM) attacks, and suggests a blockchain-based alternative. bChat offers data confidentiality, immutability, and censorship resistance by storing user data directly on the blockchain, making it available only to authenticate users via private keys. This removes the need for middlemen and central databases, making the system more secure and less prone to failure. Limitations:Slower confirmation times, high network traffic.

The paper[5] presents a comprehensive approach to addressing the growing threat of denial-of-service (DoS) attacks on Internet of Things (IoT) devices. The paper introduces a hybrid Intrusion Detection System (IDS) that combines signature-based and anomaly-based detection techniques to enhance the accuracy and efficiency of DoS attack detection in IoT environments. By leveraging the strengths of both

detection methods, the proposed system effectively identifies malicious traffic patterns and abnormal behaviour indicative of DoS attacks while minimizing false positives. Additionally, the paper outlines a proactive prevention mechanism that dynamically adjusts network configurations to mitigate the impact of detected attacks in real-time.

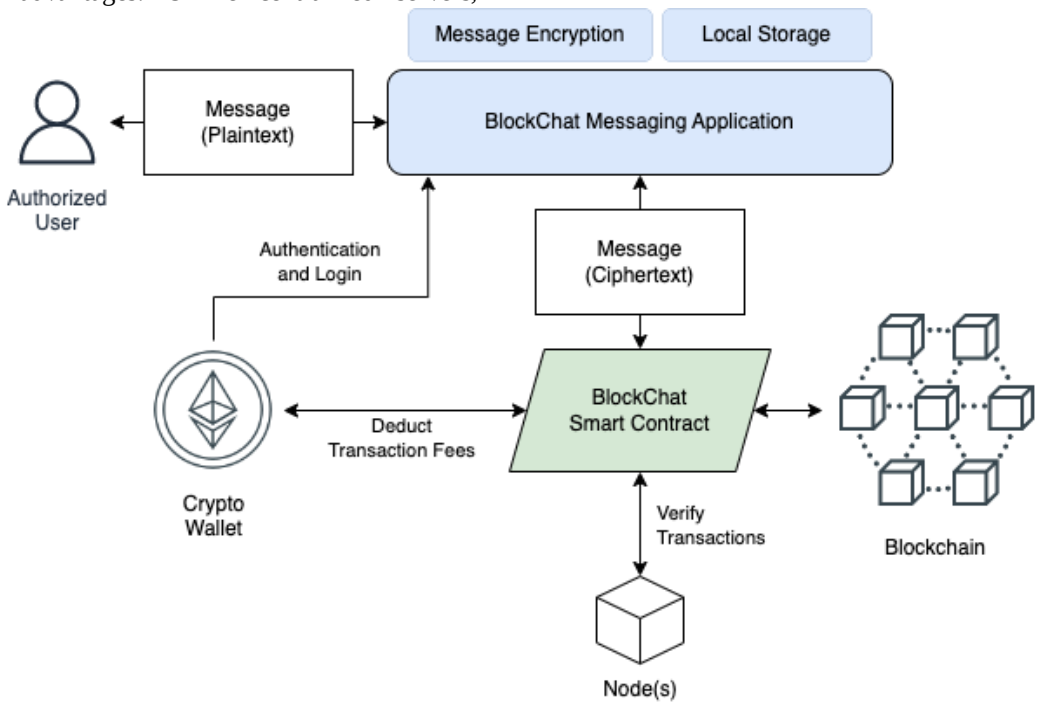
Limitationlack of media support,Lack of private chat features

III. PROPOSED SYSTEM

In today's interconnected world, where digital communication is omnipresent, ensuring the security and privacy of our conversations has become paramount. Traditional messaging platforms often lack robust security measures, leaving users vulnerable to data breaches and privacy violations. Recognizing this pressing need, our project aims to develop a cutting-edge chat application that integrates Ethereum blockchain for storage, the x3DH protocol for key exchange, and RSA encryption for message security.

The use of Ethereum blockchain for storage offers several advantages. Unlike centralized servers, which are vulnerable to hacking and data breaches, blockchain technology ensures decentralization and immutability. Each message and piece of data is cryptographically linked and stored across a distributed network of nodes, making it extremely difficult for malicious actors to tamper with or access sensitive information. Additionally, the use of smart contracts on the Ethereum blockchain enables the implementation of secure access control mechanisms, allowing users to control who can view and interact with their messages.

The x3DH (Extended Triple Diffie-Hellman) protocol plays a crucial role in ensuring forward secrecy and secure key exchange in our chat application. Unlike traditional key exchange protocols, which rely on a single exchange of keys, x3DH employs multiple rounds of Diffie-Hellman key exchanges to establish a shared secret key between users. This shared secret key is used to derive session keys for encrypting and decrypting messages, ensuring that even if one set of keys is compromised, past and future communications remain secure. Moreover, the x3DH protocol supports asynchronous communication, allowing users to exchange keys and messages even when one party is offline.



General Proposed System

RSA encryption, a cornerstone of modern cryptography, is utilized to secure the content of messages exchanged on our chat application. RSA encryption relies on the mathematical complexity of factoring large prime numbers to ensure the confidentiality and integrity of data. Each user

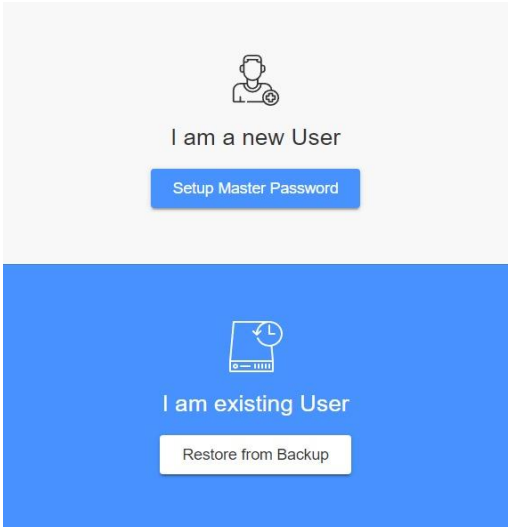
possesses a public-private key pair, with the public key used for encryption and the private key used for decryption. This asymmetric encryption scheme ensures that only the intended recipient can decrypt and read the contents of a message, even if it is intercepted during transmission.

By combining these advanced technologies, our chat application offers users a secure and private platform for communication. Messages are encrypted end-to-end using RSA encryption, ensuring that only the sender and recipient can access the content. The x3DH protocol facilitates secure key exchange, protecting against eavesdropping and man-in-the-middle attacks. And with Ethereum blockchain providing decentralized storage, users can rest assured that their data is safe from tampering and unauthorized access.

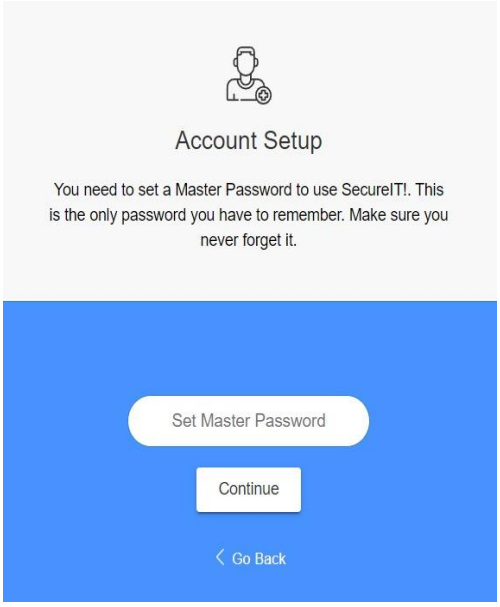
In conclusion, our proposed chat application represents a significant advancement in the field of secure digital communication. By leveraging Ethereum blockchain for storage, the x3DH protocol for key exchange, and RSA encryption for message security, we aim to provide users with a platform that prioritizes their privacy and security. Through the seamless integration of these technologies, we hope to redefine the standards of digital communication and pave the way for a safer, more secure online environment.

IV. RESULTS

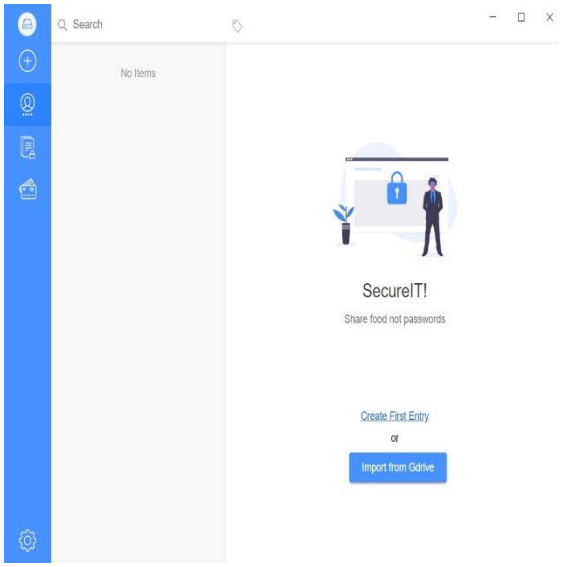
In this study, we implemented Secure It, a password manager designed to enhance security and usability. Our results demonstrate that Secure It effectively utilizes SHA-512 hashing to protect master passwords, ensuring robust resistance against brute-force attacks. Furthermore, the integration of AES 256 encryption guarantees strong key generation, bolstering the confidentiality of stored credentials. Additionally, the option to store passwords on Google Drive provides users with convenient cloud-based accessibility without compromising security. Overall, our findings underscore the effectiveness of Secure It in mitigating common password security risks while offering seamless user experience.



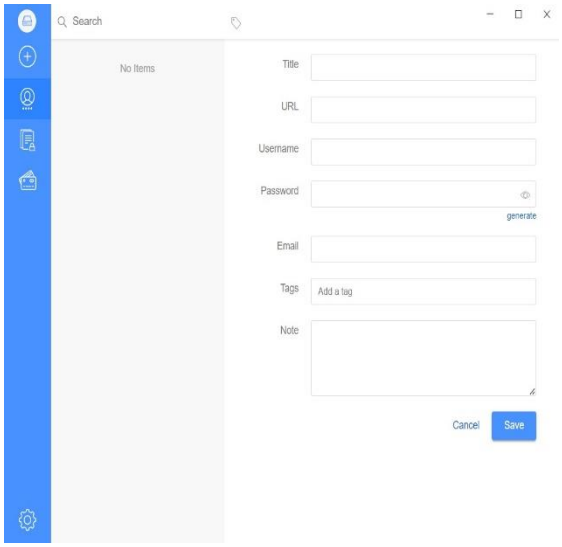
Users are presented with the option to register and log in to the application, granting them access to its features and personalized functionalities.



During this stage, users are prompted to set up a master password, a crucial step in initializing the password manager system. This master password serves as the primary key to access and secure their sensitive information within the application.



This is the landing page of the application where users can seamlessly add and manage passwords for various websites, ensuring their digital accounts remain secure. With the ability to generate passwords, add notes, and store credit card information, our platform offers comprehensive password management solutions. Additionally, users have access to a settings icon where they can change their master password, enable Google Drive backup, and customize password generator settings according to their preferences, enhancing both security and convenience.



This page serves as the central hub for storing passwords for diverse websites and facilitates password generation, offering users comprehensive control over their digital security

V. CONCLUSION

In wrapping up we're excited about the potential of our chat application to revolutionize digital communication. By leveraging Ethereum blockchain, x3DH protocol, and RSA encryption, we've created a platform that prioritizes user privacy and security. Through decentralized storage, secure key exchange, and robust message encryption, we've built a fortified fortress for online conversations. As students passionate about technology and innovation, we're proud to contribute to the evolution of digital communication and look forward to seeing our chat application make a positive impact in the real world.

VI. REFERENCES

[1]Seoul, Hyeonhak Jeong University of et al. (2021) MonoPass: A password manager without master password authentication: Companion proceedings of the 26th International Conference on Intelligent User Interfaces, ACM Conferences

[2]Adithya Gupta *et al.* (2022), *Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021, July 6-8, 2021 - research publication.*

[3]Patel, Neel & Kalra, Aryan. (2023). "SECURE PASSWORD MANAGER".

[4]Noé Heim (2020) *Convenient password manager - ETH zürich*

[5]B, M. *et al.* (2023) *Multimedia Graphical Authentication*

[6]Skandylas, C. S. L. U. S. (2021). Paper presented at the 15th European Conference on Software Architecture: Doctoral Symposium, Sep

[7]M. Mohammadinodoushan, B. Cambou, C. R. Philabaum and N. Duan, "Resilient Password Manager Using Physical Unclonable Functions," in IEEE Access, vol. 9, pp. 17060-17070, 2021, doi: 10.1109/ACCESS.2021.3053307.

[8] Agrawal, Ekta & Pal, Parashu. (2017). A Secure and Fast Approach for Encryption and Decryption of Message Communication. International Journal of Engineering Science and Computing. 7. 5.

[9] K. I. Masud, M. R. Hasan, M. M. Hoque, U. D. Nath and M. O. Rahman, "A New Approach of Cryptography for Data Encryption and Decryption," 2022 5th International Conference on

Computing and Informatics (ICCI), New Cairo, Cairo, Egypt, 2022, pp. 234-239, doi: 10.1109/ICCI54321.2022.9756078

[10] P. Pandare, S. Uniyal, R. Vani, S. Mali and P. Rumao, "Enhanced Password Manager using Hybrid Approach," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1793-1798, doi: 10.1109/ICICT57646.2023.10134398.

[11] Jofen, P. (2020). Hashiko: a generative hybrid password manager for android : design, implementation and security analysis [Diploma Thesis, Technische Universität Wien]

[12] Maliheh Shirvanian, Christopher Robert Price, Mohammed Jubur, Nitesh Saxena, Stanislaw Jarecki, and Hugo Krawczyk. 2021. A hidden-password online password manager. In Proceedings of the 36th Annual ACM Symposium on Applied Computing (SAC '21). Association for Computing Machinery, New York, NY, USA, 1683–1686.

[13] K. Loganathan and D. Saranya, "An Extensive Web Security Through Cloud Based Double Layer Password Encryption (DLPE) Algorithm for Secured Management Systems," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India, 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526381

[14] I. Permana, M. Hardjianto, and K. Ahmad Baihaqi, “Securing the Website Login System with the SHA256 Generating Method and Time-based One-time Password (TOTP)”, Systematics Journal, vol. 2, no. 2, pp. 65–71, Aug. 2020.

[15] Setiawan Hermawan and Kesuma Rey Citra, "Design of secure electronic disposition applications by applying blowfish SHA-512 and RSA digital signature algorithms to government institution", 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). IEEE, 2018.