Decentragram: A New Era of Decentralized Photo Sharing

[1]Rahul Sharma, [2]Ankit Aggarwal, [3]Aniket Kumar, [4]Ritesh Pal, [5]Ritik Gupta

[1]ASSISTANT PROFESSOR, [2,3,4,5]STUDENT

[1,2,3,4,5]CSE DEPARTMENT

[1]RKGIT GHAZIABAD, UP, [2,3,4,5]RKGITM GHAZIABAD, UP

Abstract - In the current world, social networking sites like Instagram, Facebook, and Google+, among others, have been a benefit to our humanitarian society. With these social media platforms comes a tremendous deal of responsibility for safeguarding customer privacy and data. Most of these websites save data on a centralized system known as the server. If the server crashes, the entire system fails. Using a decentralized system is one solution to this challenge. Blockchain is used to power decentralized apps. Blockchains are meant to keep transactions immutable, or unchangeable, which gives security.

Index Terms - Blockchain, decentralized, DOSNs, framework.

I. INTRODUCTION

The aim of this study is to analyze and compare the various methods in which contemporary Decentralized Online Social Networks (DOSNs) secure users' privacy. We choose a diverse set of DOSNs from the literature, rather than focusing just on those that are being implemented and actively being developed, such as Diaspora, Friend Ica, and Retro Share. Also analyze the architecture model utilized to ensure independence from a centralized provider for each selected DOSN, followed by the ways developed to allow users to set their privacy choices and focus on each DOSN's privacy model and privacy policy administration and utilize an attribute-based taxonomy to classify the various privacy models to help the reader understand their properties. Furthermore, explored the ways provided for privacy policy administration, with an emphasis on solutions that ensure that the privacy rules generated by users are appropriately implemented on each piece of information by utilizing suitable security mechanisms and access the projected managing the privacy policy in terms of number of keys generated and cryptographic operations required. Finally, investigate whether modifications in privacy policies provide backward secrecy. The purpose of this article is to provide a detailed analysis of the privacy techniques employed by existing DOSNs and to assist readers in understanding the primary privacy needs of DOSNs and how they affect the performance of current DOSN implementations.

II. LITERATURE SURVEY

Qi Xia et al. [1] presents “MeDshare: Trust-less Medical Data Exchanging Across Cloud Service Providers Via Blockchain" have suggested a new model for sharing medical data among cloud service providers that makes use of blockchain technology. This architecture involves the use of smart contracts and access control methods to effectively track data transfer and revoke access to any party that breaches the data's rules and permissions. The system's performance was evaluated and compared to existing methods for data exchange among cloud service providers. The suggested blockchain-based system provides a safe and dependable means for untrusted parties to communicate electronic medical information while protecting sensitive medical data.

Stanciu. et al. [2] present the problem of privacy in edge computing devices in their study "Blockchain-based Distributed Control System for Edge Computing," notably in IoT applications where several devices are connected in a network and there is a possibility of data theft. They suggest a method called the Hierarchical Distributed Control System Model for Edge Computing to solve this. They investigate the use of the IEC 61499 standard for distributed control systems and present ongoing research on the supervision level. implementation of function blocks as smart contracts executed by blockchain technology, as well as their integration with edge nodes that perform the executive level responsible for process control. The authors suggest that the adoption of blockchain technology enables the establishment of a distributed peer-to-peer network in which non-trusting users can communicate with each other in a verifiable and safe manner without the need for a trusted intermediary.

Elena Karafiloski and Mishev et al. [3] presented Blockchain Solutions for Big Data Challenges It proposes unique solutions related with some of the Big Data domains such as private data management and digital property resolution that can be enabled by Blockchain technology. It operates on a peer-to-peer network, with each complete node storing a copy of the Blockchain ledger. When a new transaction is made, the sender broadcasts it to all other nodes in the P2P network. It may play an important part in data security by allowing user authentication, restricting access depending on a user's needs, tracking data access histories, and ensuring effective data encryption. The author has conducted research on how blockchain may be used in many applications, such as personal data.

Abdullah et al. [4] presents the study of "Blockchain based Approach to Enhance Big Data Authentication in Distributed Environment" investigated the usage of authentication protocols in big data systems, concentrating primarily on the widely used Kerberos protocol and highlighting its security weaknesses. To overcome these restrictions, the authors propose using blockchain technology to improve large data security in distributed situations. The study examines how blockchain may be used to address typical security challenges in big data systems, as well as the authentication requirements required to increase security in distributed big data settings.

Yong Yuan and Wang et al. [5] "A decentralized social networking architecture enhanced by blockchain" provides decentralized social networking architecture enhanced by blockchain technology which use a sharing framework to increase the system scalability, a blockchain system to ensure the data integrity and consistency, a reputation-based authority control method to improve the system security at IEEE International Conference on Service Operations and Logistics, and Informatics.

III. TECHNOLOGY USED

(1) METAMASK: MetaMask is a browser plugin that allows users to interact with Ethereum blockchain-based decentralized apps (dApps). When a user accesses a dApp website, the MetaMask extension injects a JavaScript library into the page, allowing the dApp to connect with the MetaMask extension and the Ethereum blockchain. The MetaMask plugin allows the user to interact with the dApp in a safe manner, such as creating and maintaining Ethereum accounts, signing transactions, and accessing the user's Ethereum address. MetaMask also enables users to interact with the dApp in a private and secure way. The extension stores the user's private keys and seed phrase locally, so the user has full control over their private keys and their funds. This eliminates the need for users to trust a third party with their private keys and ensures that only the user has access to their Ethereum account.

(2) BLOCKCHAIN: Decentralized web apps (dApps) employ blockchain technology to create a secure and decentralized platform for storing and exchanging data and assets. There is no central authority directing the network in a decentralized web application, and all data is saved on a distributed ledger maintained by a network of nodes. Blockchain enables the establishment of a decentralized network in which all nodes are equal, and no centralized authority controls the network. This eliminates the requirement for a trusted third party while also making the network immune to censorship and sabotage. To safeguard the data and assets held on the blockchain network, cryptography is used. Each transaction is recorded on the blockchain and connected to the preceding one, resulting in an immutable and transparent record of all transactions. These contracts are recorded on the blockchain and can be executed automatically if specific criteria are satisfied. This removes the need for middlemen and guarantees that the agreement's conditions are carried out automatically and openly. Blockchain enables the construction of a transparent and verifiable system in which all transactions are recorded on the blockchain and visible to anyone.

(3) NGROK: Ngrok is a program that allows developers to connect to the internet via a local web server. It is often used in decentralized web apps since it allows developers to test and showcase their dApp without having to deploy it to a live server. When a developer installs Ngrok on their local system, it generates a public URL that redirects incoming traffic to the developer's local web server. This enables the developer to distribute their dApp to others, test it on many devices, and even connect it with other services that require a live URL. Ngrok also allows developers to view all incoming and outgoing traffic, which is important for debugging and resolving dApp difficulties. It also offers a secure tunnel to the local host and may be encrypted using SSL/TLS certificates. Ngrok is a valuable tool for decentralized web application developers since it allows them to test and showcase their dApp on a live, publicly available URL without deploying it to a live server, examine all incoming and outgoing traffic, and offer secure tunnel and encryption.

(4) ETHEREUM: Ethereum is a blockchain platform that allows the development of decentralized apps (dApps) and smart contracts. The Ethereum Virtual Computer (EVM) is a decentralized virtual machine that runs the code of smart contracts and dApps. Ethereum enables the development of decentralized apps that are not controlled by a single body. This reduces the need for confidence in a centralized organization and provides for a more transparent and safe system.

IV. RESULT

The goal of this study was to better understand the different approaches and procedures employed by current decentralized online social networks (DOSNs) to preserve the privacy of their members' material. To do this, we evaluated a variety of popular DOSNs' architectural designs as well as how they handle user privacy. According to our findings, the bulk of these networks use unstructured peer-to-peer (P2P) architecture for routing and content exchange. and investigated how each network allows users to express their privacy choices and restrict access to their material and discovered that social networks' privacy rules are often restricted and straightforward, enabling users to select from predetermined alternatives based on friendship or relationship type. Also, recognize that these simplistic models may have flaws, such as a lack of consideration for relationship qualities or features, and the possibility of including other forms of relationships, such as owner and co-owner, into privacy rules.

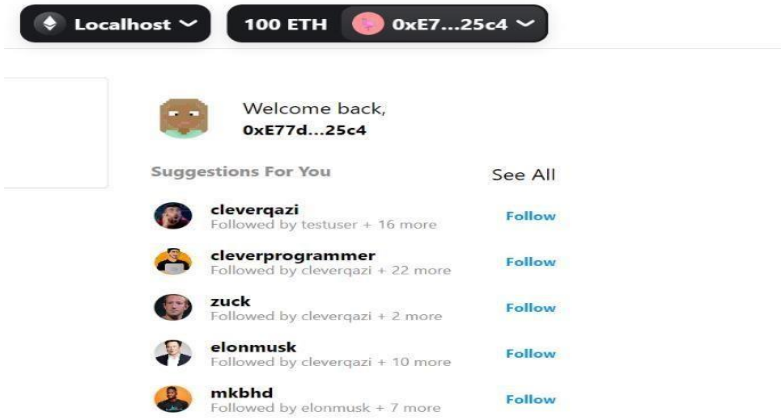

Fig 1: Follow Users

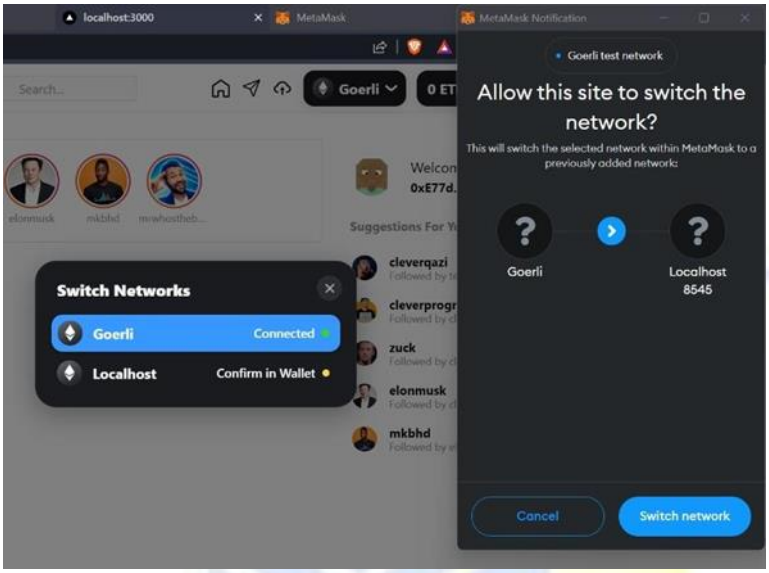

Fig 2: MetaMask connection

As shown in fig 1 The figure illustrates the "Follow User" functionality in Decentragram, showcasing the key elements and actions associated with this feature. The interface consists of various components that facilitate users in establishing and maintaining connections with other Decentragram accounts.

At the center of the figure, a user profile is displayed, showcasing the essential information about the account being followed. This includes the account holder's profile picture and username. Additionally, relevant statistics such as the number of followers and following may also be displayed.

Adjacent to the user profile, a prominent "Follow" button is presented. This button acts as the primary means of initiating a connection with the displayed user. By clicking the "Follow" button, users express their interest in following the account and receiving updates on their activities.

The figure 2 illustrates the integration of MetaMask functionality within the Decentragram platform, showcasing key elements and actions associated with this feature. The interface incorporates components that enable users to engage in decentralized interactions, securely manage cryptocurrency transactions, and leverage blockchain-based functionalities.
At the center of the figure, a section dedicated to MetaMask integration is depicted. This section showcases the presence of MetaMask within the Instagram interface, allowing users to interact with decentralized applications seamlessly.

V. CONCLUSIONS

The goal of this study was to better understand the different approaches and procedures employed by current decentralized online social networks (DOSNs) to preserve the privacy of their members' material. To do this, we evaluated a variety of popular DOSNs' architectural designs as well as how they handle user privacy. According to our findings, the bulk of these networks use unstructured peer-to-peer (P2P) architecture for routing and content exchange. and investigated how each network allows users to express their privacy choices and restrict access to their material and discovered that social networks' privacy rules are often restricted and straightforward, enabling users to select from predetermined alternatives based on friendship or relationship type. Also, recognize that these simplistic models may have flaws, such as a lack of consideration for relationship qualities or features, and the possibility of including other forms of relationships, such as owner and co-owner, into privacy rules.

VI. REFERENCES

[1] MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain IEEE Access published on 24 July 2017.

[2] Alexandru Stanciu. (2017). Blockchain Based Distributed Control System for Edge Computing.IEEE at 21st International Conference on Control Systems and Computer Science (CSCS).

[3] Elena Karafiloski and Anastas Mishev (2017). Blockchain solutions for big data challenges: A literature review. IEEE Access, 17103072.

[4] Nazri Abdullah, Anne håkansson and Esmiralda Moradian (2017) Ninth International Conference on Ubiquitous and Future Networks.

[5] Shuai Zeng, Yong Yuan and Fei-Yue Wang A decentralized social networking architecture enhanced by blockchain (2020), IEEE Access, 8, 19260875.

[6] Barbara Guidi (2021). An Overview of Blockchain Online social media from the Technical Point of View.

[7] Ching-man Au Yeung, Ilaria Liccardi, Kanghao Lu and Oshani Seneviratne (2011). Decentralization: The Future of Online Social Networking.

[8] Manoj Kumar, Mukunthan K, R. Reena, S. Bhuvaneswari. (2022). Decentralized Social Media Platform using Blockchain, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT).

[9] Renita Murimi. (2019). A Blockchain Enhanced Framework for Social Networking, 10.5195/ledger.2019.178.

[10] Cornelius C. Agbo and Qusay H. Mahmoud (2020) Blockchain- Based E-Health Consent Management Framework, Conference: (2020) IEEE International Conference on Systems, Man, and Cybernetics.

[11] K. Makar, S. Goel, P. Kaur, M. Singh, P. Jain, and P. K. Aggarwal, "Reliability of Mobile Applications: A Review and Some Perspectives," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2021, pp. 1-4, Doi: 10.1109/ICRITO51393.2021.9596350.

[12] P. Chaudhary, S. Goel, P. Jain, M. Singh, P. K. Aggarwal, and Anupam, "The Astounding Relationship: Middleware, Frameworks, and API," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2021, pp. 1-4, doi: 10.1109/ICRITO51393.2021.9596088.

[13] S. Mishra, A. Shukla, S. Arora, H. Kathuria, and M. Singh, "Controlling Weather Dependent Tasks Using Random Forest Algorithm," 2020 Third International Conference on Advances in Electronics, Computers and Communications (ICAECC), 2020, pp. 1-8, doi: 10.1109/ICAECC50550.2020. 9339508.

[14] Sharma, A., Singh, M., Gupta, M., Sukhija, N., & Aggarwal, P. K. (2022). IoT and blockchain technology in 5G smart healthcare. Blockchain Applications for Healthcare Informatics, 137–161.

[15] H. Garg, M. Singh, V. Sharma, and M. Agarwal, "Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936413.

[16] Jiang, X., Liu, S., & Sun, Y. (2021). A survey on the application of blockchain technology in the logistics industry. Journal of Ambient Intelligence and Humanized Computing, 12(9), 8759-8774.

[17] Kim, J., & Kim, Y. (2021). Design and implementation of a blockchain-based electronic document management system. Journal of Ambient Intelligence and Humanized Computing, 12(8), 75317542.