

Secure Sphere: A Blockchain-Based Social Media Platform with Verifiable Token Identity for Enhanced Security and Authentication

A Sheerin¹, E Rubesh², K Sasidharan³, S.K. Sukundan⁴

¹Assistant Professor Department of CSE (Internet of Things and Cyber Security including Blockchain Technology),

^{2,3,4,5} Department of CSE (Internet of Things and Cyber Security including Blockchain Technology)

¹Email ID: sheerinasoodulla@gmail.com ²Email ID: rubeshrubesh533@gmail.com

³Email ID: ksasidharan2152@gmail.com ⁴Email ID: sugucud28april2004@gmail.com

Cite this paper as: A Sheerin, E Rubesh, K Sasidharan, S.K. Sukundan, (2025) Secure Sphere: A Blockchain-Based Social Media Platform with Verifiable Token Identity for Enhanced Security and Authentication. *Journal of Neonatal Surgery*, 14 (23s), 959-971.

ABSTRACT

To counteract the emerging difficulties regarding user authentication details, falsehoods, and the facilitated spread of deceptive messages, this project proposes a blockchain-based social media platform. Many existing centralized systems are susceptible to identity theft and cyberattacks, and they also allow the widespread creation of false profiles that promote misleading content. Moreover, these systems can damage an online business's standing and trigger financial downturns. This project aims to improve user authentication, enhance security, and prevent online harassment. The blockchain model, in conjunction with the Verhoeff algorithm, evaluates relevant metrics to effectively distinguish between real and fake accounts. This project collects user data associated with Aadhaar credentials and then generates a token key and a secret key for secure authentication by using Verifiable Token Identity Algorithm (VTIA). Thus the secret key acts as a public key, shown on the user's personal profile, and the token key is sent to the registered email ID. The success of this model is completely dependent on the quality of detection over time and the token ID remains permanent for future authentication and creating another account. Furthermore, this system also provides a transparent and secure social media experience.

Keywords: User authentication, Cyber Attacks, Verhoeff algorithm, Verifiable Token Identity Algorithm (VTIA), token key, secret key.

1. INTRODUCTION

1.1 Background

The evolution of online networking tools has significantly eased human interaction, connecting neighbors to people worldwide and transforming everything from personal communication to public business. This growth has also fueled the expansion of e-commerce by connecting millions across geographical boundaries, creating opportunities for collaboration on complex challenges. However, this potential growth brings both advantages and disadvantages to users who rely on social networking platforms. Moreover, these online spaces have become integral to our daily lives, influencing everything from users' personal data to social development. Most of the Social networks helps people to engage their business promotion activities such as branding their product, targeting audience, building some social communities which driving online stores and influence the user-generated content for increasing their sales.

Instagram is a powerful social network platform that helps users to allow communication among the world, sharing their personal or informative thoughts, commercial ideas, cultures via photos and videos. Although it plays a vital role in establishing e-commerce channels to impress customers and some other product dealers for making e-business. To improve their business growth, people can arrange or circulate their schedule, agenda and post some forms to collect users' opinions. This leads to a major flaw for the Instagram / Facebook user as without knowing proper belief/ knowledge on that link, they submit their personal details. These social network platforms have not limited to share their events also producing shopping tool in some cases. Fraudulent users try to open an account in the name of the reputed (or) Posting some misinformation regarding health, lifestyle, politics or banking details to make. The enormous fake account activities on social networks presents a major threat to normal users. To prevent this, the creation of online accounts is a case procedure, so that a fraction of second users cultivating their activities easily. To create a secure account verification, blockchain technology gives their hands in preventing account creation on the account of anonymous users and some secured private algorithms to block third party accesses to hack that account details.

1.2 Problem Statement

The aim of this project is to develop a system that can efficiently detect and remove fake users to ensure the integrity of the platform as well as its users. False accounts are manipulated in the matrix for interaction, and it's hard to discern genuine from bogus users. Cyber criminals evade detection using advanced methods. Centralized platforms don't have an open mechanism to allow public users to authenticate multiple connected accounts.

1.3 Research Objectives

To address these issues, this paper aims to improve the decentralized social platform via blockchain technology. Its aim is to protect users' data, address the proliferation of fake accounts, and improve overall transparency of the platform. The main goals of this study are as follows:

- Building a blockchain-based social media network where user data is stored safely in an unchangeable and decentralized ledger.
- A new false account identification mechanism through the token -ID and secret system, which allows public users to confirm multiple related accounts.
- Strengthen security and privacy through cryptographic hashing to safely lock user information in various blockchain blocks.
- Providing transparency and user responsibility through a public search option, allowing users to check associated accounts with a secret key.

This paper introduces a decentralized social media platform that leverages blockchain technology to address these issues. By utilizing a peer-to-peer network, Decentagram ensures data ownership remains with the users, eliminating the need for intermediaries. The platform employs smart contracts to facilitate transparent interactions and incorporates cryptocurrency mechanisms to reward user engagement. This approach aims to mitigate challenges such as data breaches, censorship, and unauthorized data manipulation, thereby offering a more secure and user-centric social media experience.

2. LITERATURE REVIEW

Each day use of the Internet generates as a minimum a few megabytes of facts. Nowadays, social media has enabled everybody with a cellphone and net get the right of entry to perform as a writer, writer, marketer, or content material author. It is hard to provide copyright and safety for social media content material together with images, movies, and audio [7]. Copyright infringement is ordinary; for this reason, it ought to be easier to ensure content validity and distinctiveness. A personal and steady on the spot messaging gadget primarily based on blockchain era to enhance the records protection and privateness of social media platforms. The solution reduces the dangers associated with centralized servers and unauthorized facts [11] gain admission by using a personal blockchain structure to make end-to-end encryption and decentralized information management. The reason for this approach is to handle more about their communication and personal facts. The centralization of records on conventional social media structures has caused several challenges, together with content restriction, facts breaches, and privateness worries. To cope with these demanding situations, this essay appears at how blockchain generation can decentralize social networking systems. SARS can maintain the occupation of their personal information by spreading it in a blockchain network, ensuring safety and openness [4]. Look at it, I support a secretary sharing mechanism to protect a blockchain structure, a current day decentralized filling system and social media information. [14]. Because of its immutability and decentralization, this architecture has numerous applications for defensive copyright rights of material on decentralized social media platforms. The record [20] examines new systems that have adopted a decentralized method to spotlight the benefits and potential issues of transitioning from centralized to decentralized social media ecosystems.

Blockchain's decentralized and immutable ledger appears to be a viable solution for preserving user data in social networks. Smart contracts enable users' privacy preferences to be securely stored and enforced without the need for central authorities [10]. This paper has ensured that any changes to privacy settings are both explicit and tamper proof, in line with regulations such as the General Data Protection Regulation. These systems give consumers complete control over their data, minimizing the risks associated with centralized data management. The study discusses how blockchain technology might increase security in decentralized storage systems. It underlines how blockchain's decentralized, impermeable structure ensures anonymity and integrity, making it ideal for distributed environments. To improve security and access control in these systems, the authors propose an adaptive encryption approach. This solution addresses data breaches and illegal access by leveraging blockchain technology's peer-to-peer design to create a secure framework for data sharing [7]. Decentralized social networking apps aim to address issues such as censorship, single points of failure, and data privacy associated with traditional centralized platforms [12]. These apps distribute data management and storage across a network of nodes by leveraging decentralized storage systems and blockchain technology, eliminating the need for central authorities. This strategy allows users greater control over their content, protects their privacy, and ensures data immutability. To address these issues, the paper [14] introduced "Decentagram," a decentralized social networking platform based on blockchain technology. Decentagram ensures that users keep ownership of their data by using a peer-to-peer network, which eliminates

the need for middlemen. The site incentivizes user participation with bitcoin ways, and smart contracts allow for transparent interactions. This method aims to make social media more secure and user-friendly by eliminating data breaches, censorship, and illicit data manipulation.

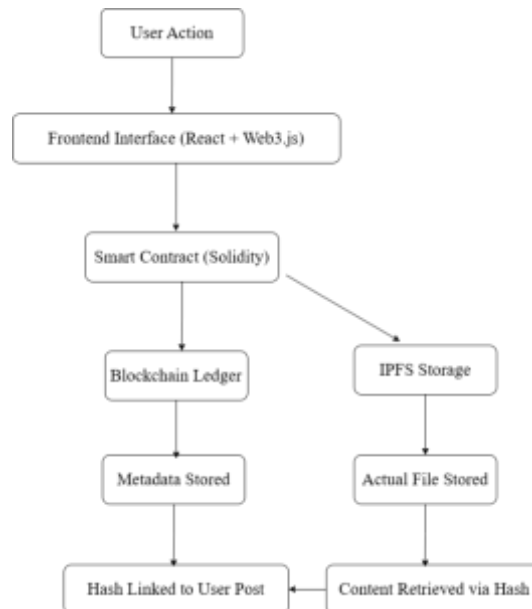
3. EXISTING METHODOLOGY

The DeGram research paper outlines a decentralized social media network that uses blockchain technology and Interplanetary File System (IPFS) to provide secure, transparent, and censorship-free social networking. Conventional social media sites such as Facebook and Instagram rely on centralized servers where control over data, moderation, and user privacy is determined by a central authority. The centralized model makes such platforms susceptible to data theft, censorship, unauthorized surveillance, and identity hijacking. DeGram, however, aims to change this paradigm through the integration of a peer-to-peer (P2P) model where content ownership, data ownership, and user authentication are decentralized across a blockchain network. User-generated content (posts, pictures, videos, etc.) within DeGram isn't stored in one server but uploaded to IPFS, an open-source file system that relies on content-addressing to define files in a unique way. Metadata and hashes of these types of files are stored on a blockchain ledger with the provision of immutability and traceability. This provision ensures that the moment content goes live, it cannot be tampered with or deleted without a consensus on the network. Members sign in using a decentralized identity scheme—cryptographic keys instead of the standard username/password combination—to gain access to the more secure and privacy-conscious sign-in. DeGram applies smart contracts to orchestrate actions such as posting, following, likes on posts, and commenting. The contracts are open, transparent, and automated with no requirement for a third party, imbuing an amount of trust as well as automation. The site also offers token-based incentives, where users receive cryptocurrency tokens for contributing quality content or acting as network moderators, to encourage participation and system coherence. This helps to cut spam, abuse and misinformation, and promote real interactions. However, although the setup of DeGram offers a decent level of decentralization, it does not address the challenges of real-world identity or prevent false accounts. Usually, cryptography is used for authentication, which protects access, but does not always connect accounts with the real-world identity. Blockchain became added in 2008 by using Satoshi Nakamoto as the muse for Bitcoin. It is a distributed, decentralized ledger that stores records in blocks related together chronologically and cryptographically. Each block incorporates a hash of the previous block, making the facts tamper resistant. Blockchain is used as the core infrastructure to report User identification hashes, Smart agreement transactions and IPFS file hashes (not the actual content) It ensures that everyone's social interactions (like posting, liking, and commenting) are transparent, traceable, and immutable, preventing records manipulation or unauthorized editing. DeGram most probably uses Ethereum or a comparable platform for imposing these blockchain functions due to its aid for smart contracts and extensive adoption. The idea of clever contracts was first added through Nick Szabo within the Nineties, but it became realistic with the launch of Ethereum in 2015. A smart contract is a self-executing program saved on the blockchain that routinely enforces policies while predefined situations are met. DeGram makes use of clever contracts (likely written in Solidity) to automate Posting content, Commenting or liking, Following or unfollowing users and Token-based rewards for engagement. These contracts get rid of the want for a principal moderator or administrator. For example, when a consumer likes a put up, the smart settlement updates the like rely without delay on the blockchain with no need approval from any centralized machine. IPFS turned into created with the aid of Juan Benet in 2015 through Protocol Labs. It is a peer-to-peer distributed record storage system that shops documents across more than one node and retrieves them the use of content-primarily based addressing (a completely unique hash of the report's content), unlike conventional systems that use area-primarily based URLs. In DeGram, IPFS is used to store actual consumer-generated content material including Images, Videos, Text posts Only the hash of each document is stored on the blockchain. This aggregate of IPFS and blockchain keeps storage green while maintaining report integrity and decentralization. For instance, if a consumer uploads a image, IPFS shops it, and the blockchain shops the IPFS hash which can continually be used to retrieve or confirm the content material.

Table I. Related Findings for Non-centralized Platforms

Title	Year	Ideas
Lens Protocol	2022	Decentralized social graph protocol for building diverse social apps
Farcaster	2022	Decentralized social networks emphasizing identity and ownership
Mirror	2021	Platform for writers and creators to publish and monetize content
Bluesky	2023	New social network aiming for a more open and decentralized platform
Lenster	2023	Decentralized social media app built on Lens Protocol, offering user-friendly experience

Table-1 summarizes a top-level view of new decentralized social media structures developed between 2021 and 2023, highlighting their center thoughts and contributions. Lens Protocol (2022) serves as a foundational framework that lets build decentralized social apps using a shared social graph. Farcaster (2022) emphasizes decentralized consumer ownership and identity, with the aim of individuals being the owner of their own profiles and data through the Blockchain certification protocol. Mirror (2021) is for writers and manufacturers of materials, enables them to publish and take advantage of their work using blockchain techniques. Lastly, Lenster (2023) is a person-friendly social media app built on the Lens Protocol, supplying a acquainted enjoy even as ensuring decentralized manage over identity and content material. Together, those systems showcase the developing fashion towards consumer empowerment, information privateness, and censorship resistance within the evolving panorama of decentralized social media.



Existing System Architecture: The overall process of a decentralized social media platform like DeGram kicks off when a user creates a post or uploads content via a web interface. This content gets stored on IPFS, which is a distributed file system that assigns a unique hash to each file. At the equal time, a clever settlement is activated to verify the movement, file the content material of cannabis, person facts and time stamp on blockchain. This setup guarantees that the facts is secure and cannot be tampered with. Blockchain acts as a reliable account ebook for all interactions, while the IPFs take care of storing huge files. When someone wants to use the material, the system reflects it from IPF using hash on blockchain. The whole process allows for safe, transparent and decentralized content, and ensures that users retain ownership and that trust is unstable is the code rather.

4. PROPOSED SYSTEM ARCHITECTURE:

4.1 Overview:

VTIA Algorithm is a standardized algorithm specifically named for "fake user detection". With the support of VTIA Algorithm to prevent anonymous user for creating account on the name of verifiable user. This VTIA algorithm works like:

1. Verification:

Checking the validity of contact information such as E-mail and phone number and Adhaar number. The details provided are to be verified in this method. It Links and detects multiple accounts with the same username using the same secret key.

2. Transactions:

This principle focuses on analyzing financial transactions and interactions to detect fraudulent activity.

3. Identity:

This principle focuses on analyzing user profiles and information to assess their genuineness. Requiring users to complete their profiles with relevant information (e.g., bio, interests, profile picture). Analyzing profile completeness and consistency to identify suspicious profiles with minimal information.

4. Activity:

This principle focuses on analyzing user behavior and interactions to detect patterns that deviate from genuine activity. Monitoring posting frequency, interaction patterns (e.g., likes, comments, shares), and engagement levels. Analyzing the time of account creation, posting times, and interaction patterns to detect suspicious activity.

Working of vtia Algorithm for Generating TOKEN ID:

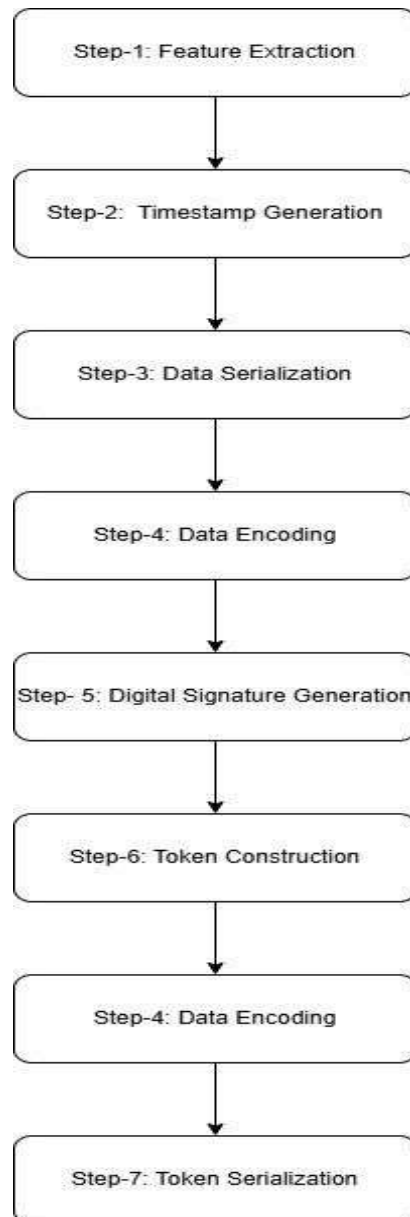


Fig.3.1 Workflow diagram for working VTIA Algorithm

The above given Fig.3.1 explains the flowchart for working VTIA Algorithm, where the user credentials are featuring extraction and generates timestamp as one time generation that is not get back again. After that, Data serialization and Data Encoding performs and produces output as hash value in form of token key and secret key. This supports secure registration in social media accounts. In step 5, Digital signature Generation executes only if there is a missing key or the user's account. Following that Combine encoded data and signature into a token as token construction in step 7.

3.1. System Design

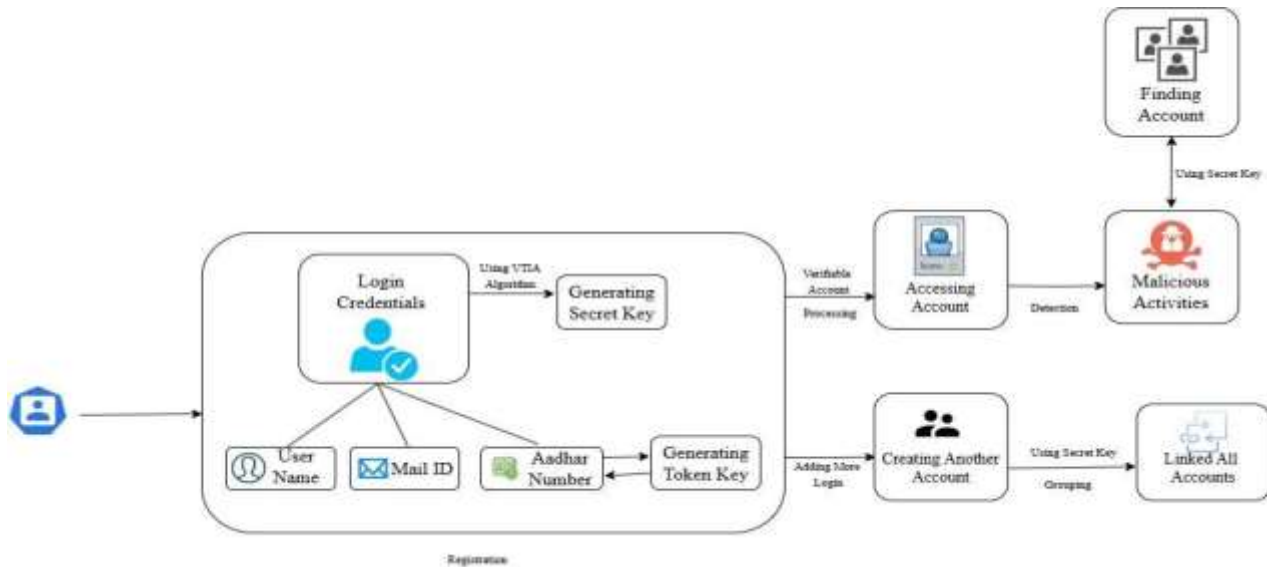


Fig.3.1. Architecture Diagram for A Blockchain-Based Social Media Platform with Verifiable Token Identity for Enhanced Security and Authentication

The above given diagram fig.3.1 illustrates the working of Social Account with safe and secure with the help of VTIA (Verifiable Token Identity Algorithm) to produce Secret key and Token key. Those keys are produced in the form of encrypted key, and its one-time generation never be created again. This Proposed model is illustrated by using flowchart in fig.3.2 given above.

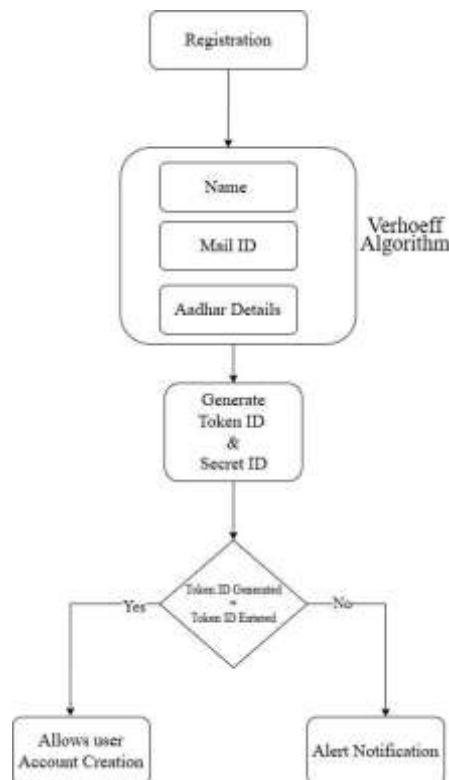


Fig.3.2 Flowchart for A Blockchain-Based Social Media Platform with Verifiable Token Identity for Enhanced Security and Authentication

Table II. Components and their Roles

Component	Roles
Client-slide view	Frontend design, user profiles, and Account creation interfaces
Application Interface	The part of the application that users interact with, usually through a web or mobile interface.
Server-Side Logic	Handle tasks that are not suitable for the blockchain, such as data storage and retrieval.
Blockchain	Provides a decentralized ledger within a private blockchain for secure and transparent transactions among authorized participants.
Digital ledger	Stores user data and content in a decentralized manner using IPFS, ensuring privacy, integrity, and security.
Identity Management Layer	Manages user identities and access control by using Aadhaar card hash values for authentication, generating a unique Token ID and Secret Key to ensure secure login and data protection.

This Table summarizes the essential components and their relative roles of our VTIA System. It describes the essential components of our system such as Client-slide view, Application Interface, Server-Side Logic, Blockchain, Digital ledger, Identity Management Layer

5. RESULTS AND IMPLICATIONS

In our efforts, we created a proper system that could detect and prevent unclean social media for the use of blockchain generation. During the trial segment, the base-based registration method worked as expected, and confirmed the identification of the buyer through the Verhof algorithm. Once proven, every consumer turned into assigned a completely unique Token ID and Secret Key, which helped in handling and identifying connected money owed securely. The information was stored in blockchain blocks, making it tamper-evidence and steady. Our public search function additionally made it viable to test if a person had more than one bills linked to the equal Aadhaar, improving transparency. Overall, the effects display that our system may be a practical approach to address the issue of faux profiles on social media systems



Fig.1 Welcome screen for a social platform named 'SECURE SPHERE,' highlighting blockchain security and featuring 'Login' and 'Create Account' buttons.

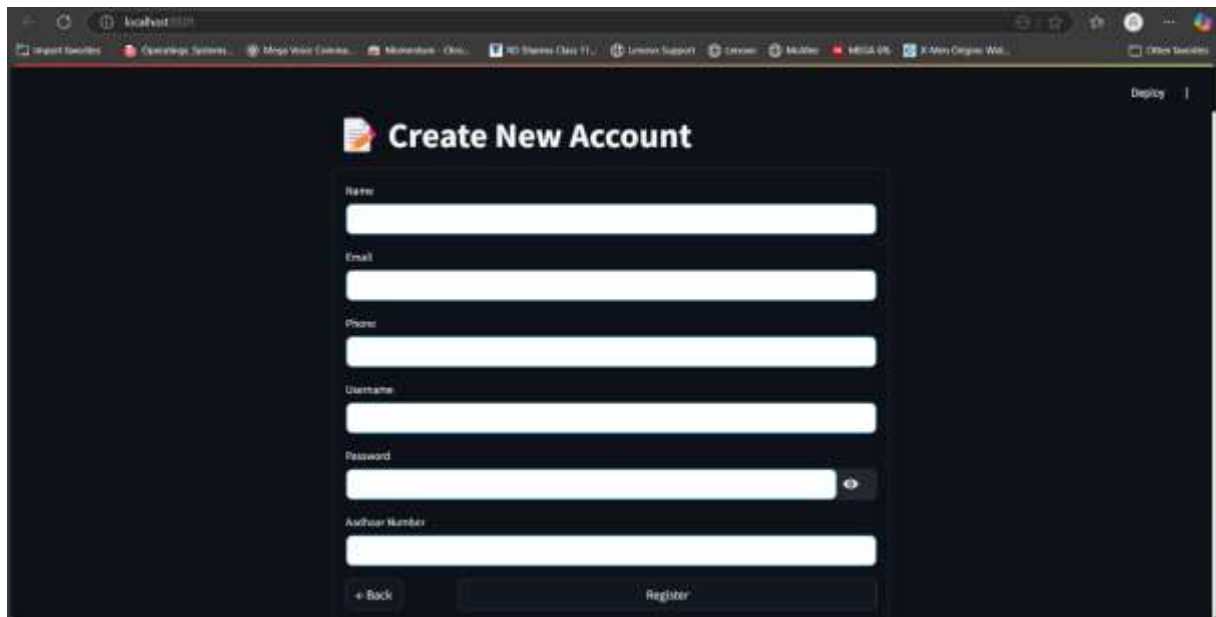
A screenshot of a web browser displaying a 'Create New Account' form. The form is titled 'Create New Account' with a document icon. It contains several input fields: 'Name', 'Email', 'Phone', 'Username', 'Password' (with a toggle for visibility), and 'Aadhaar Number'. At the bottom of the form are two buttons: '+ Back' and 'Register'. The browser's address bar shows 'localhost' and the page title is 'Create New Account'.

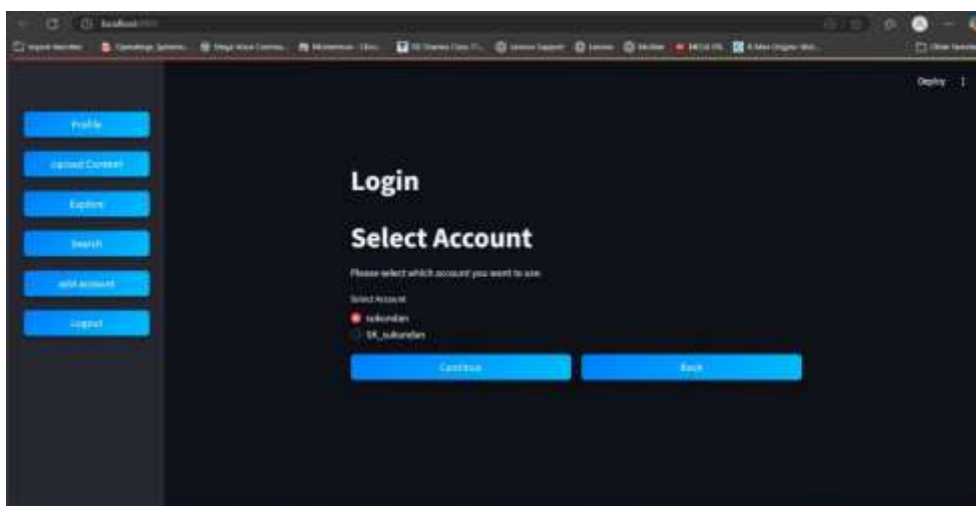
Fig.2 Displays a new account registration form with fields for personal information, including an Aadhar Number.

A screenshot of a web application's 'Output' section. It features a 'Clear' button in the top right corner. The text 'Enter Aadhaar Number: 638525515674' is displayed, followed by a red 'X' icon and the text 'Invalid Aadhaar Number'.

Fig.3 Displays the result of an Aadhaar number validation, indicating the entered number is invalid.

A screenshot of a web application's 'Output' section. It features a 'Clear' button in the top right corner. The text 'Enter Aadhaar Number: 639852515674' is displayed, followed by a green checkmark icon and the text 'Valid Aadhaar Number'.

Fig.4 Shows the validation of an Aadhaar number, The verification of Aadhaar Number is done through automatically using Verhoeff Algorithm confirming its validity

A screenshot of a web application's 'Login' page. The page has a dark background with a sidebar on the left containing buttons for 'Profile', 'Logout', 'Update', 'Search', 'Add Account', and 'Logout'. The main content area is titled 'Login' and 'Select Account'. It includes a sub-header 'Please select which account you want to use' and a section 'Select Account' with two radio buttons: 'rehabilitation' (selected) and 'SR, rehabilitation'. At the bottom are two buttons: 'Continue' and 'Back'.


```
Enter the Aadhar Number: 639852515674
Enter the Password : Sugu@123
• Original String: 639852515674 Sugu@123
• Generated Salt: c11d0ebf1ef8f164bca3b5306c41271d
• Hashed Output: 6421a69e6c1684e736ab4eea19bd74babfba57c8bf9fd3b0a5cf9d8e0d2c4002
```

Fig.6 Presents a demonstration of hashing, showing the original string (Aadhar number and password), the generated salt, and the resulting hashed output. After verified the Adhaar number is valid, two new hash value is created one is for token id (which can be 22 characters long) and another is for secret key (which can be 16 characters long). The two values can be linked with each other.

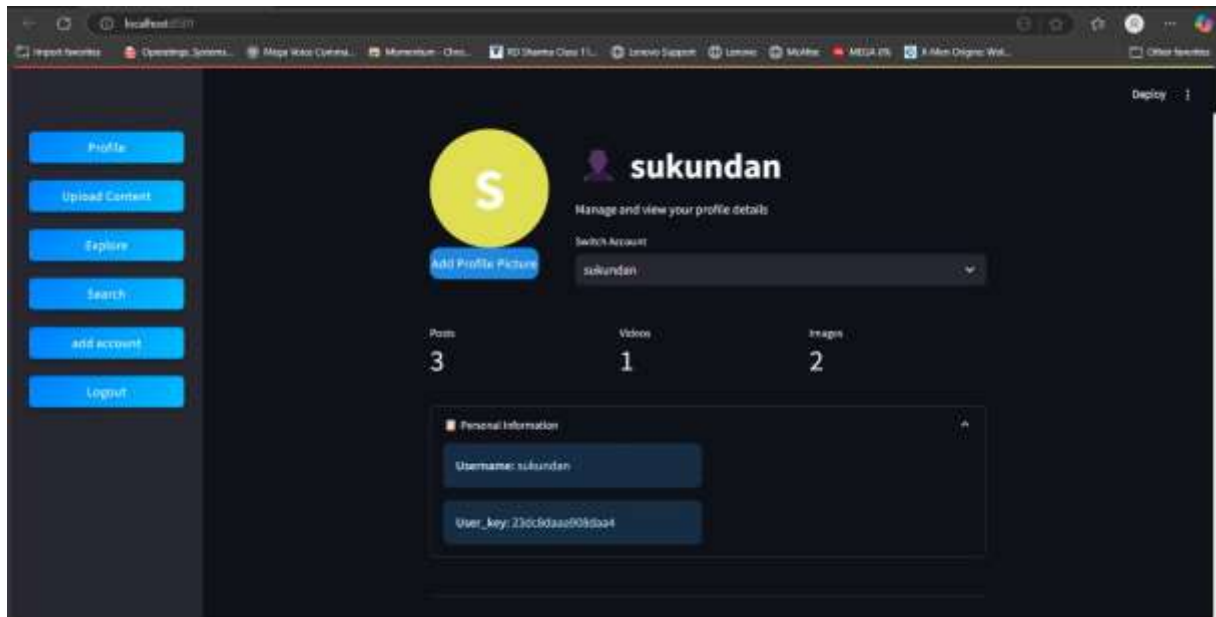


Fig.7 Displays a user profile interface showing 'sukundan' with navigation options, profile statistics, and personal information including username and user key.

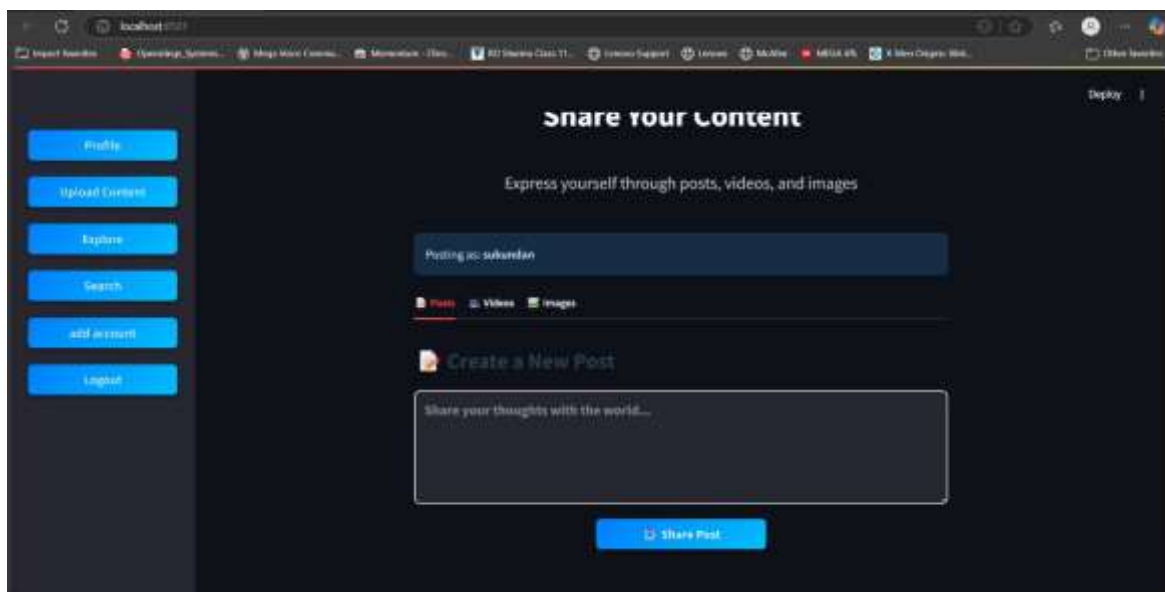


Fig.8 Presents a content sharing interface, allowing user 'sukundan' to create posts, videos, and images with a 'Share Post' option.

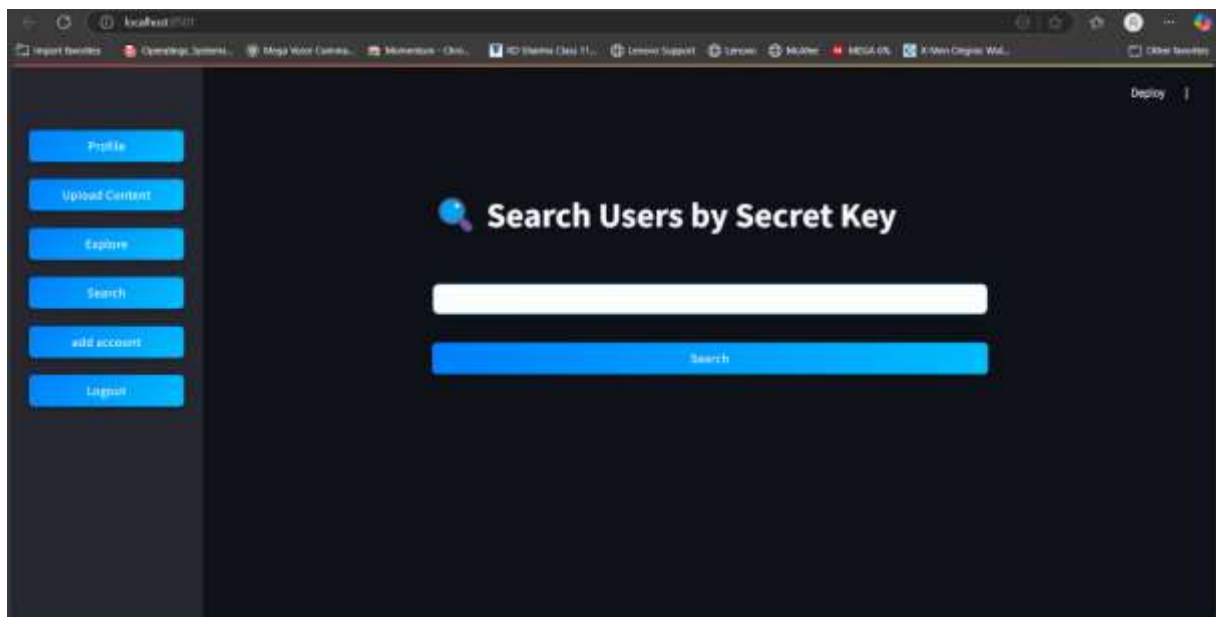


Fig.9 Depicts a search interface enabling users to find other users by their secret key.

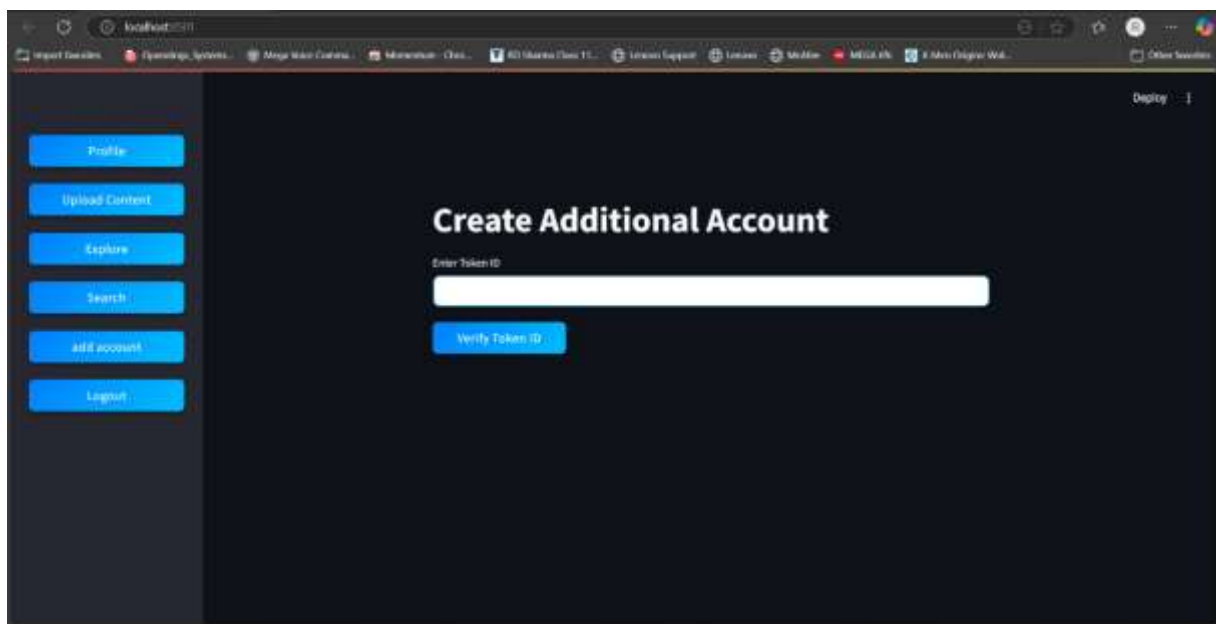


Fig.10 Shows an interface to create an additional account by entering and verifying a Token ID.

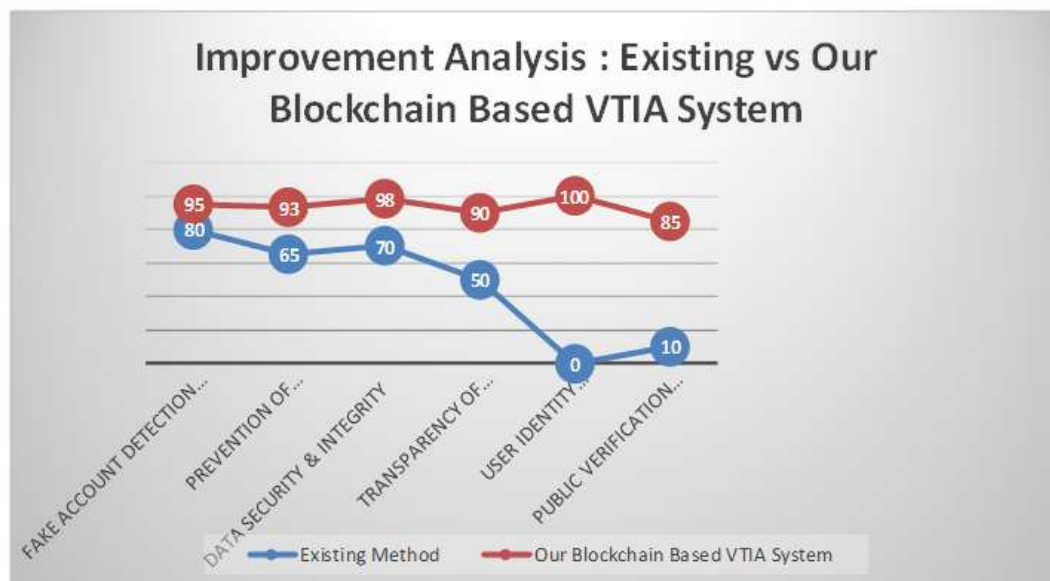
6. PERFORMANCE ANALYSIS

To determine the reliability and effectiveness of our proposed blockchain-based fake account detection device, we evaluated it across numerous performance metrics which can be critical for any identity verification mechanism. These metrics include fake account detection accuracy, facts integrity, transparency, protection against tampering, prevention of reproduction debts, and person identification area of expertise. Traditional systems include CAPTCHA validation, email or smartphone-primarily based verification, or even a few gadgets learning-based approaches often offer first rate accuracy in detecting bots or suspicious hobbies, commonly ranging between 70% to eighty-five%. However, they tend to rely heavily on centralized servers, which leads them to susceptible to data breaches and tampering. Moreover, these conventional methods usually do not offer transparency or a way to publicly verify the authenticity of an account. In contrast, our system introduces Aadhaar-based registration with Verhoeff algorithm verification; secure data storage through blockchain, and a unique Token ID and Secret Key mechanism for tracking and linking accounts. This combination of features allows our system to excel in almost every key metric, offering a high level of security, transparency, and reliability that traditional techniques struggle to match.

Table III. Comparative Analysis of Existing Technologies

Features	Existing Technologies (CAPTCHA, Email/Phone Verification, ML Models)	Our VTIA-Based Blockchain System
Identity Verification	Basic (Email/Phone, sometimes skipped)	Aadhaar-based with Verhoeff Algorithm
Fake Account Detection Accuracy	Moderate (70–85%)	High Accuracy (Up to 95%)
Data Storage Method	Centralized Databases	Decentralized Blockchain (Tamper-Proof)
Transparency in Verification	Low	High (Public Search via Secret Key)
Prevention of Duplicate Accounts	Limited or Bypassed Easily	Strong (Token ID Linkage Prevents Multiple Accounts)
Tamper Resistance	Vulnerable to Attacks	Tamper-Proof Through Block Integrity
Public Search & Linking of Accounts	Not Available	Available (Secret Key Based Account Linking)
User Data Privacy	Depending on Provider Policies	Secured with IPFS and Blockchain Hashing
Detection Logic	Heuristic, Behavior Analysis, AI/ML Models	Deterministic via Aadhaar, Verhoeff, and Blockchain Validation
Real-World Identity Binding	No Real Binding	Strong Real Identity Link with Aadhaar
Scalability	May Slow Down with User Growth	Scalable with Decentralized Network Design

The above table III. compares traditional false account identification technologies with the VTIA-based blockchain system. Traditional methods use e-mail or telephone confirmation, which can be circumvented, while the VTIA system uses base-based verification through the Verhoeff algorithm. Traditional systems only achieve moderately false account identification accuracy, while VTIA receives 95% accuracy when using determined arguments. The VTIA model uses a decentralized, tamper-proof blockchain, ensures openness and prevents duplicate account construction. It also ensures user data person protection using IPF -er and blockchain hashing, and uses determined arguments based on base and blockchain verification. The decentralized network design provides efficient and scalable performance.



The development assessment line graph compares the overall performance of existing faux account detection strategies with the proposed Blockchain-Based VTIA System throughout six key metrics. The present methods, represented by means of way of the blue line, show mild overall performance in areas like fake account detection (eighty%), prevention of duplicate bills (sixty five%), and information integrity (70%), but drop appreciably in superior standards which encompass transparency of identity verification (50%), person identification place of information (0%), and public verification guide (10%). In assessment, the VTIA gadget, represented by the crimson line, continues continually excessive overall performance throughout all metrics—achieving ninety-five% in faux account detection, ninety-three% in duplicate prevention, 98% in facts safety, ninety% in transparency, one hundred% in Aadhaar-based totally identity area of expertise, and eighty-five% in public verification assist. This truly illustrates that the VTIA-based machine extensively outperforms conventional methods in phrases of accuracy, security, transparency, and real-world identity binding.

7. CONCLUSION AND FUTURE WORK

This research proposed a Blockchain based Decentralized model using VTIA for controlling anonymous user account creation and posting misinformation. In contrast to existing systems, this model never paves the way for creating fake users without the knowledge of the verifiable users. Furthermore, this paper also enhances security and pretends to be safe and supports for performing e-commerce growth by a Token ID is generated once per user during initial registration cannot be modified. Users cannot request a new Token ID unless a strict verification process is followed. This model has feasible and stable detection performance on detecting false users and information creations. The false information detection and Blockchain task processing model shown in this paper has performance advantages and application value. However, to improve the user experience, this model will focus on working for retrieving lost token id . On the other hand, Users cannot seek new Token ID requests if there is problem in reading Token ID . As a Future development, this research would deploy Multi signature authentication algorithm will supports to avoid account locking if the user lost their email which perceive the token id.

REFERENCES

- [1] Farah Abu-Dabaseh, Mahmoud Alghizzawi, Baker Ibrahim Alkhlaifat, "Enhancing Privacy and Security in Decentralized Social Systems: Blockchain-Based Approach" (2024), 2nd International Conference on Cyber Resilience (ICCR), doi:10.1109/ICCR61006.2024.10533137.
- [2] Pranay Ambre, Shubham Bane, Aakansha Singh, "Turtl: IPFS Based Decentralized File Sharing System" (2023), 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), doi:10.1109/ICPCSN58827.2023.00255.
- [3] Parth Kayade, Aniket Pardeshi, Suyog Patil, "Decentralized Application using Blockchain", 2024 5th International Conference on Image Processing and Capsule Networks, doi:10.1109/ICIPCN63822.2024.00156.
- [4] Charusheela Nehete, Anish Lohiya, Meet Mulik, Vallari Patil, Ajinkya Morankar, "DeGram - Decentralized Social Media Application", 2024 3rd International Conference on Applied Artificial Intelligence and Computing, doi: 10.1109/ICAAIC60222.2024.10575902.
- [5] Kachapilly Varghese Alfred Anthony, T. Mathu, "Decentralized Social Media using Blockchain and IPFS", 2024 4th International Conference on Pervasive Computing and Social Networking, doi:10.1109/ICPCSN62568.2024.00094.
- [6] M.L. Dhole, Soham Ratnaparkhi, Rohan Sasne, Om Surase, Rushikesh Chandak, "Next Generation Social Media Platform to Move from Centralization to Decentralization of Data", 2023 7th International Conference On Computing, Communication, Control And Automation, doi: 10.1109/ICCUBEA58933.2023.10392043.
- [7] N. Palanivel, K. Madhan, C. S. Kumar, R. SarathKumar, T. Ragupathi and D. S, "Securing IoT-Based Home Automation Systems Through Blockchain Technology: Implementation," 2023 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India, 2023, pp. 1-7, doi: 10.1109/ICSCAN58655.2023.10395653.
- [8] B.S.S. Perera, G.G.S. Dhananjani, A.M.C.A. Bandara, A.W.Y.I.K. Abeykoon, Kavinga Yapa Abeywardena, "DeMedia: Decentralization of Social Media", 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT), doi: 10.1109/CSNT60213.2024.10545716.
- [9] S. Nagini, Karthik Akkala, Venkata Nikhil Thanikella, Venkat Jagarlamudi, Teja Kumar Kalimera, "Decentralized Social Media Application using Blockchain Technology", 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), doi: 10.1109/ACROSET62108.2024.10743920.
- [10] Parth Kayade, Aniket Pardeshi, Suyog Patil, Prashant Raut, Pranav Shetkar, Madhuri Barhate, "Decentralized Application using Blockchain", 2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN), doi: 10.1109/ICIPCN63822.2024.00156.

-
- [11] Marc Jayson Baucas, Petros Spachos, "Secure Private Blockchain-Based Instant Messaging Platform for Social Media Services", IEEE Networking Letters (Volume: 6, Issue: 2, June 2024),doi: 10.1109/LNET.2024.3386974. [12]. Mahavir A. Devmane, "D-Space: A Decentralized Social Media App", 2023 2nd International Conference on Edge Computing and Applications (ICECAA),doi: 10.1109/ICECAA58104.2023.10212341.
- [12] Prashanth, M.S., Maheswari, V.U., Aluvalu, R., Kantipudi, M.V.V.P. (2024). "SocialChain: A Decentralized Social Media Platform on the Blockchain". In: Castillo, O., Sudhakar Babu, T., Aluvalu, R. (eds) Pervasive Knowledge and Collective Intelligence on Web and Social Media. PerSOM 2023. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 517. Springer, Cham. https://doi.org/10.1007/978-3-031-66044-3_14.
- [13] Manchi Sarapu, S., Hegde, N.P., Vikkurty, S., Garimella, K.P.V.S. (2023). "Metacart—Decentralized Social Media Marketplace to Incentivize Creators and Ensure User Data Privacy". In: Reddy, A.B., Nagini, S., Balas, V.E., Raju, K.S. (eds) Proceedings of Third International Conference on Advances in Computer Engineering and Communication Systems. Lecture Notes in Networks and Systems, vol 612. Springer, Singapore. https://doi.org/10.1007/978-981-19-9228-5_47.
- [14] Lavania, G., Sharma, G. (2023). "Security on Social Media Platform Using Private Blockchain". In: Nedjah, N., Martínez Pérez, G., Gupta, B.B. (eds) International Conference on Cyber Security, Privacy and Networking (ICSPN 2022). ICSPN 2021. Lecture Notes in Networks and Systems, vol 599. Springer, Cham. https://doi.org/10.1007/978-3-031-22018-0_20.
- [15] Kripa, M., Nidhin Mahesh, A., Ramaguru, R., Amritha, P.P. (2021). "Blockchain Framework for Social Media DRM Based on Secret Sharing". In: Senjyu, T., Mahalle, P.N., Perumal, T., Joshi, A. (eds) Information and Communication Technology for Intelligent Systems. ICTIS 2020. Smart Innovation, Systems and Technologies, vol 195. Springer, Singapore. https://doi.org/10.1007/978-981-15-7078-0_43
- [16] Papadopoulos, P., Pitropakis, N., Buchanan, W.J. (2022). "Decentralized Privacy: A Distributed Ledger Approach". In: Hussain, C.M., Di Sia, P. (eds) Handbook of Smart Materials, Technologies, and Devices. Springer, Cham. https://doi.org/10.1007/978-3-030-84205-5_58
- [17] Praveena Anjelin, D., Ganesh Kumar, S. (2021). "Blockchain Technology for Data Sharing in Decentralized Storage System". In: Dash, S.S., Das, S., Panigrahi, B.K. (eds) Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 1172. Springer, Singapore. https://doi.org/10.1007/978-981-15-5566-4_32
- [18] Fake Profile Detection Using Machine Learning Techniques” Partha Chakraborty, Mahim Musharof Shazan, Mahmudul Nahid, Md. Kaysar Ahmed, Prince Chandra Talukder Department of Computer Science & Engineering, Comilla University, Cumilla, Bangladesh. <https://doi.org/10.4236/jcc.2022.10100062>
-