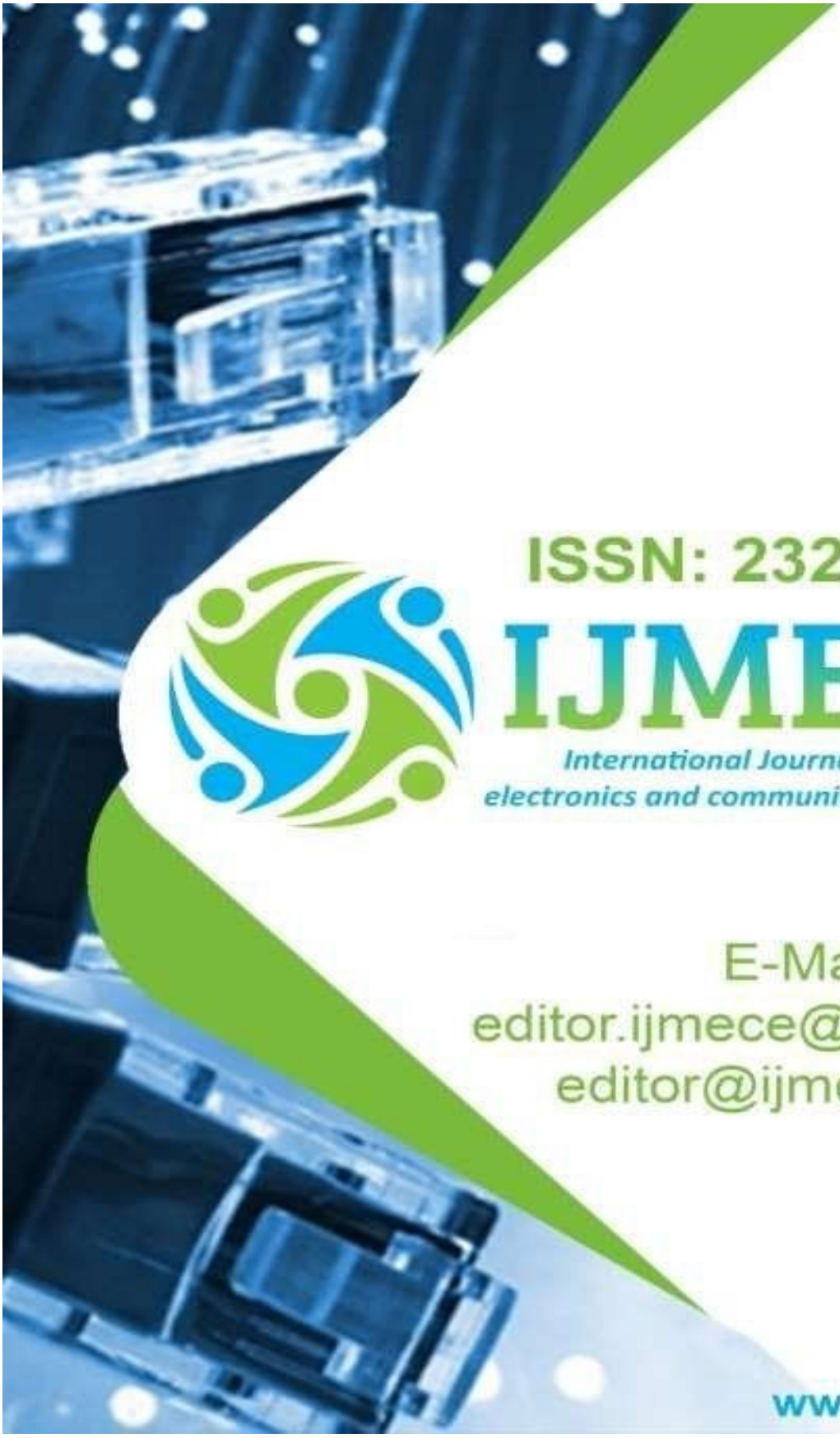


ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

ENHANCING PRIVACY AND SECURITY IN SOCIAL MEDIA INTERACTIONS USING BLOCKCHAIN

K.Mounika[1]
Assistant Professor
Department of CSE(DS)
TKR College of Engineering and Technology
kmounika@tkrcet.com

M. Varshitha Reddy[2]
B. Tech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
varshithareddy167@gmail.com

R. Lahari[3]
B. Tech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
laharirasmalla@gmail.com

S. Upendar Reddy[4]
B. Tech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
reddyupendar933@gmail.com

N.Nikith Kumar[5]
B. Tech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
nenavathnikith@gmail.com

ABSTRACT

With the increasing use of social media platfrom platforms, concerns about privacy breaches, data leaks, and security vulnerabilities have escalated. Traditional social media platforms rely on centralized data storage, making them susceptible to hacking and unauthorized access. Blockchain technology presents a revolutionary approach to addressing these challenges by leveraging decentralization, encryption, and smart contracts. This paper explores how blockchain can enhance privacy and security in social media interactions by mitigating risks such as identity theft, unauthorized data sharing, and cyber attacks.

This model also raises concerns over user privacy, data ownership, and transparency, as users have limited control over how their information is used or shared.By leveraging a distributed ledger, blockchain eliminates reliance on a single authority, ensuring that data is securely stored across multiple nodes. Additionally, it enhances user privacy through cryptographic protocols, allowing users to retain control over their information.

Keywords: Social media platforms, Privacy breaches, Data leaks, Security vulnerabilities, Centralized data, Hacking, Unauthorized access, Blockchain technology, Decentralization, Encryption, Smart contracts.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

INTRODUCTION

Social media has revolutionized communication, networking, and information sharing, connecting billions of users worldwide. However, these platforms also pose significant privacy and security challenges due to their centralized data storage models. User data is often collected, stored, and controlled by a few entities, making it susceptible to breaches, cyberattacks, and unauthorized access. Issues such as identity theft, data leaks, surveillance, and misuse of personal information have become major concerns, raising the need for a more secure and transparent system. Additionally, social media companies often monetize user data through targeted advertising, sometimes without explicit user consent, further exacerbating privacy concerns.

Blockchain technology offers a transformative solution to these challenges through decentralization, encryption, and smart contracts. By eliminating the reliance on central authorities, blockchain ensures that data is distributed across a secure network, reducing the risk of hacking and unauthorized modifications. Cryptographic techniques further enhance data integrity and privacy, allowing users to have greater control over their personal information. Unlike traditional platforms, blockchain-based systems enable peer-to-peer data sharing without intermediaries, reducing exposure to third-party surveillance.

Smart contracts play a crucial role in ensuring secure and transparent interactions. These self-executing contracts automatically enforce predefined rules and conditions, preventing unauthorized data access and sharing. Furthermore, blockchain's transparency ensures that all transactions and modifications are recorded on an immutable ledger, reducing the risk of fraud and manipulation.

Beyond security, blockchain also enhances user autonomy. Decentralized identity (DID) systems allow users to authenticate themselves without relying on centralized databases, minimizing the risk of identity theft. Moreover, blockchain-based social media platforms can introduce token-based incentive models, rewarding users for content creation and engagement while maintaining transparency in revenue generation.

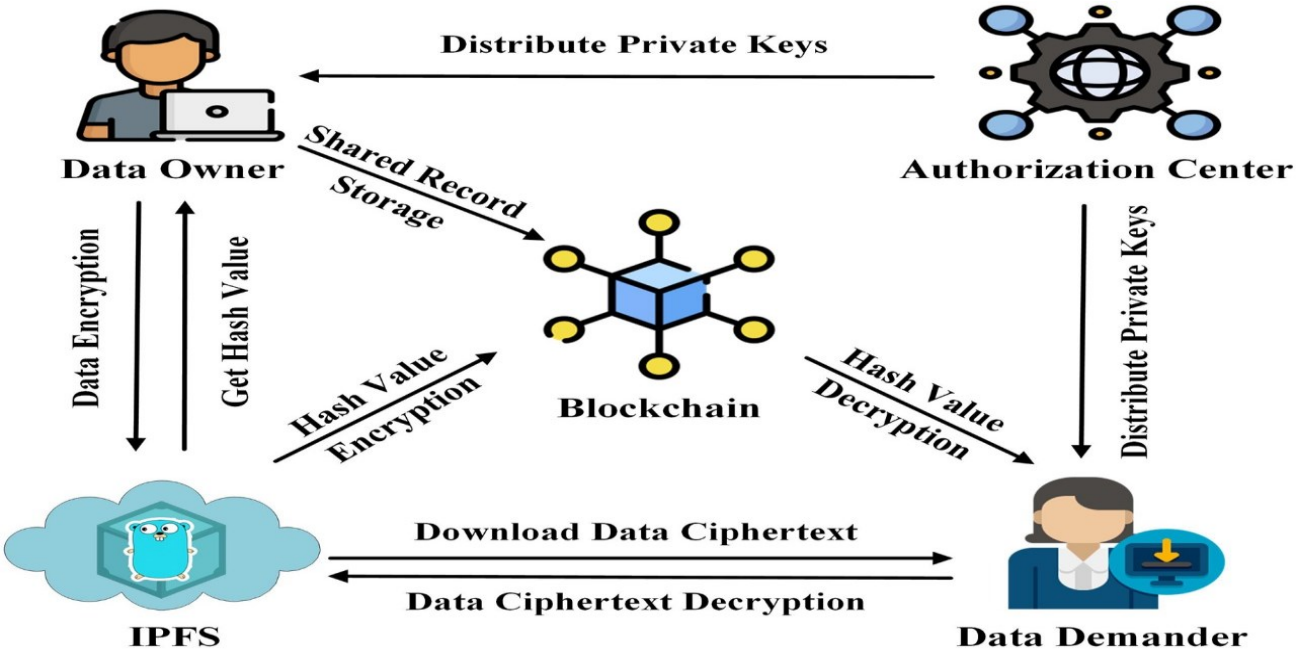
This paper explores how blockchain can redefine privacy and security in social media by mitigating risks, ensuring transparency, and empowering users with control over their data. Implementing blockchain-based solutions can help create a safer digital environment, fostering trust, data sovereignty, and reliability in online interactions. As the adoption of blockchain in social media grows, it has the potential to revolutionize the way online communities interact, ensuring a balance between connectivity and privacy.

The rapid evolution of social media platforms has transformed how

individuals communicate, share, and consume information. However, as these platforms grow, significant challenges arise, particularly in centralized data management. Centralized social

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

media networks often hold immense amounts of user data on single servers, making them vulnerable to breaches, censorship, and unauthorized access.



2. RELATED WORK

Several studies and technological advancements have explored the integration of blockchain in social media to enhance privacy and security. Researchers have highlighted the vulnerabilities of centralized social media platforms, emphasizing the risks associated with data breaches, third-party surveillance, and unauthorized access.

The integration of blockchain technology into social media has gained significant attention in recent years due to its potential to address privacy and

security concerns. Traditional social media platforms rely on centralized data storage, making them vulnerable to hacking, data breaches, and unauthorized data monetization. Researchers have explored various blockchain-based solutions, including decentralized social media platforms, cryptographic security techniques, smart contracts, decentralized identity management, and token-based incentive models. These approaches aim to enhance user privacy, reduce dependency on third parties, and provide greater transparency in data management.

Blockchain for Decentralized Social Media.

Various decentralized social media platforms, such as Steemit, Mastodon, and Minds, have emerged as alternatives to traditional platforms. These platforms utilize blockchain to distribute data across nodes, preventing single points of failure and reducing the risk of hacking. Research by Xu et al. (2020) discusses the benefits of decentralization in mitigating data privacy risks.Decentralized social media platforms leverage blockchain technology to eliminate single points of failure and reduce the risk of unauthorized access. Platforms like Steemit, Mastodon, and Minds use distributed ledger systems to store and manage user-generated content securely. Unlike traditional social networks, where data is controlled by a central authority, decentralized platforms distribute data across multiple nodes, making

them more resilient to cyberattacks and censorship.

A. Cryptographic Techniques for Secure Communication

Blockchain employs cryptographic methods such as hashing and public-private key encryption to enhance data security. Studies, including those by Nakamoto (2008), have demonstrated how cryptographic techniques ensure data integrity and prevent unauthorized modifications. The use of end-to-end encryption within blockchain-based social media applications further enhances secure communication.highlight how cryptographic security mechanisms prevent unauthorized data modifications and enhance privacy protection. In social media applications, end-to-end encryption powered by blockchain can secure direct messages and prevent interception by third parties. Additionally, zero-knowledge proofs (ZKPs) are being explored as a method for verifying user identities without exposing sensitive personal data, further strengthening privacy in social interactions.

B. Smart Contracts for Privacy Enforcement

Several studies have explored the use of smart contracts to automate data access control in social media. Wang et al. (2019) proposed a blockchain-based access control framework that allows users to define who can view or share their data through smart contracts, ensuring transparency and eliminating third-party interference. Smart contracts, self-executing programs running on blockchain networks, provide an effective way to enforce data privacy policies in social media. Wang et al. (2019) proposed a blockchain-based access control framework that allows users to specify data-sharing permissions through smart contracts, eliminating the need for intermediaries. For example, a user could define conditions under which their personal data can be accessed, ensuring transparency and accountability. Smart contracts also enable the automation of user agreements, reducing risks related to unauthorized data sharing. Despite these benefits, concerns regarding smart contract vulnerabilities and their immutability require further research and optimization.

C. Decentralized Identity (DID) Management

Researchers such as Sovrin Foundation (2021) have examined the role of decentralized identity (DID) in social media security. DID frameworks on blockchain eliminate the need for centralized authentication, reducing the risks of identity theft and data leaks. Decentralized identity (DID) frameworks offer a blockchain-based approach to authentication, reducing reliance on traditional login credentials stored by centralized entities. Sovrin Foundation (2021) discusses how DID systems enable users to control their identity and share only necessary information with service providers. Unlike conventional social media logins that require email or phone number verification, DID systems use cryptographic keys and verifiable credentials to authenticate users without exposing their full identity. This reduces the risks of identity theft, phishing attacks, and unauthorized data collection. However, widespread adoption of DID in social media faces technical and regulatory challenges that must be addressed to ensure interoperability and usability.

E. Token-Based Incentive Models

Studies have also investigated how blockchain-based social media platforms incentivize users while ensuring transparency. Platforms like BitClout and Steemit reward users for content creation using tokens, as discussed by Lee et al.(2022). This model ensures fair These studies

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

and implementations demonstrate reliancprivacy, security, and transparency concerns. However, challenges such as scalability, regulatory compliance, and user adoption remain areas for further exploration. Blockchain-based social media platforms incorporate token-based incentive mechanisms to encourage content creation and engagement while maintaining transparency in revenue distribution. Studies by Lee et al. (2022) explore platforms such as Steemit and BitClout, where users earn tokens based on their contributions, eliminating the need for intrusive advertisements and centralized monetization models. These tokens can be used for various purposes, including tipping content creators, purchasing digital assets, and accessing premium features. The transparency of blockchain ensures that rewards are distributed fairly, increasing user trust in the platform. However, the volatility of cryptocurrency-based incentives poses economic risks that need to be managed for sustainable implementation.

These studies highlight the potential of blockchain in reshaping social media by addressing privacy, security, and data ownership concerns. While blockchain-based solutions offer significant improvements, challenges such as scalability, regulatory compliance, and user adoption remain key obstacles. Future research and technological advancements are needed to optimize blockchain-based social media models for mainstream use.

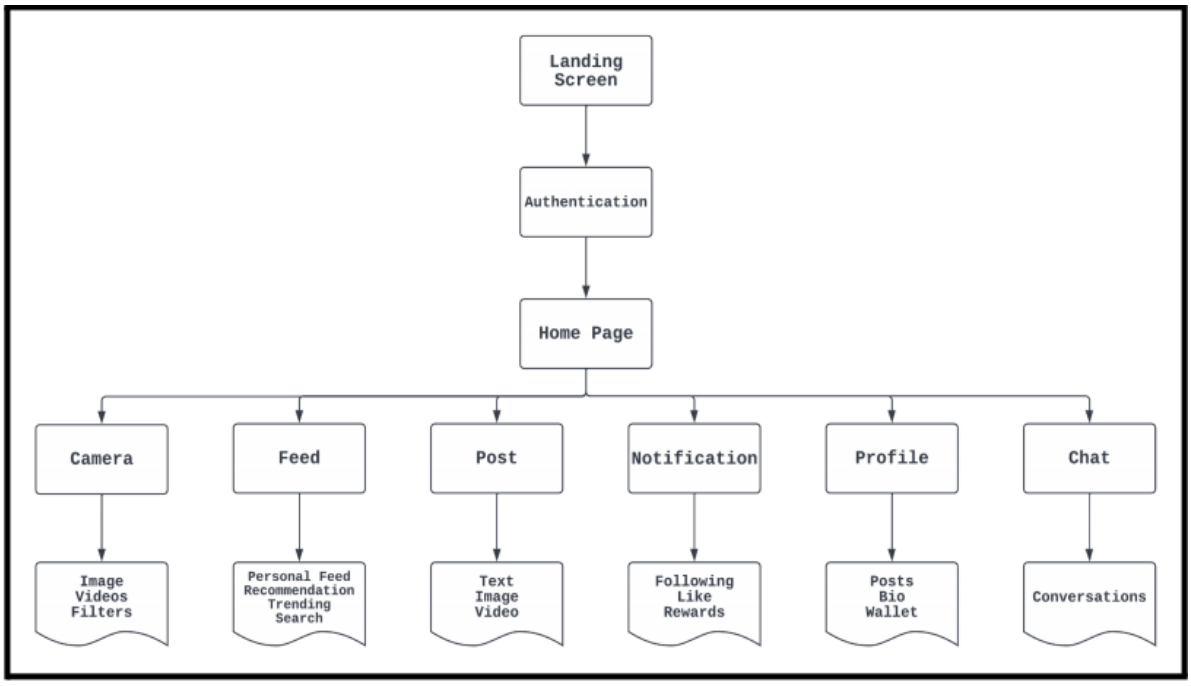


Fig 3-1 : Flowchart of Social Media Application

3.METHODOLOGY

SPLASH Screen :

Splash screens (also known as launch screens) provide a simple initial experience while your mobile app loads. We have a splash screen to make the user experience for our app intuitive and fun to use.

Authentication :

We have an authentication screen where the user has to either register/sign-in him/herself to use our application if it's their first time using our app or log in if they already have an account. The user has to give some details about them like their name and other details just for verification purposes to ensure that it's a genuine user.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

The data entered here won't be used for other purposes rather than the authentication. For eg. The user can login with the wallet id, username, or any other details mentioned.

Flow chat:

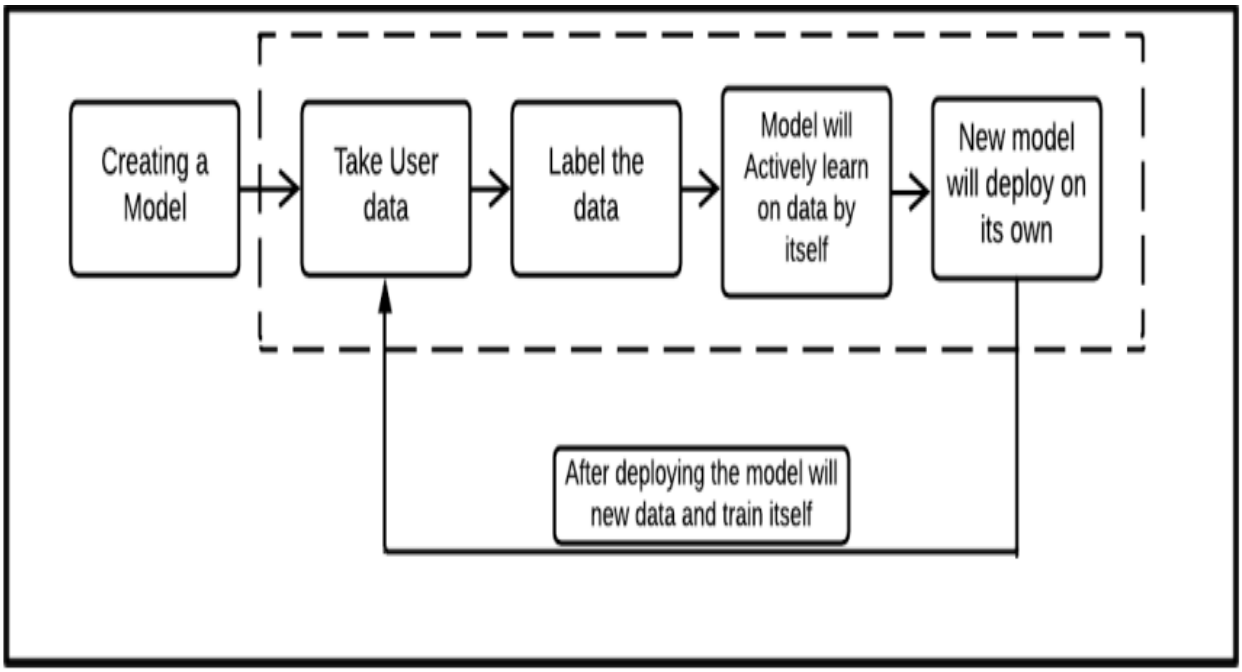


Fig 3-2 : Flowchart on how Active Learning model will process

Home Screen :

The Home screen of our application consists of the following tabs :

1. Feed :

The feed will consist of the posts according to the preference of his choice of the content. It can consist of text, videos, photos, etc. It will enable the user to stay connected to all the happenings in the world especially as per his / her liking. This feed will work on recommendation analysis by creating a model. It will consist of all the posts that the users of our application deem are trending at that instance. Similar to, trending tab in Youtube, twitter, and explore tab on Instagram. The motive behind creating this section of the app was to help the users stay updated with all the latest information thats there in our social media and the world.

Post : This section will allow users to post the desirable content of various file formats. These

file formats include - text , image , video. The users have a freedom of speech to posts whatever and however they like. Users will receive incentive if the post receives more than a particular range of likes.

In this section users can communicate with other users (the one they follow) . They can create multiple groups with two or more users. The chats will be end to end encrypted i.e. 21only the sender and receiver can read / access those images. Users can share videos, images and also currency to each other. The data will be stored locally and no one will have any kind of authority over the data on the server.

2. Profile :

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

This section will comprise of users data - Username , Followers and following number, Profile picture, content posted. Active learning is the name used for the process of prioritising the data which needs to be abelled in order to have the highest impact to training a supervised model. In our application Active learning is used as the amount of data is too large to be labelled and some priority needs to be made to label the data in a smart way. Active learning is used to optimise the data points chosen for labelling and training a model based on them. We will be using the following steps to use active learning on our data: The first thing which we did is that we took a very small subsample of this data that needs to be manually labelled. Once there is a small amount of labelled data, the model was trained on it. After the model is trained, the model is used to predict the class of each remaining unlabelled data point.

Model based on Active Learning :

Active learning is the name used for the process of prioritising the data which needs to be labelled in order to have the highest impact to training a supervised model. In our application Active learning is used as the amount of data is too large to be labelled and some priority needs to be made to label the data in a smart way. Active learning is used to optimise the data points chosen for labelling and training a model based on them. We will be using the following steps to use active learning on our data: The first thing which we did is that we took a very small subsample of this data that needs to be manually labelled. Once there is a small amount of labelled data, the model was trained on it. After the model is trained, the model is used to predict the class of each remaining unlabelled data point. 22A score is chosen on each unlabelled data point based on the prediction of the model. In the next subsection we will present some of the possible scores most commonly used. Once the best approach has been chosen to prioritize the labeling, this process can be iteratively repeated: a new model can be trained on a new labeled data set, which has been labeled based on the priority score. Once the new model has been trained on the subset of data, the unlabelled data points can be run through the model to update the prioritisation scores to continue labelling. In this way, one can keep optimising thelabelling strategy as the models become better and better. The model will be deployed on the basis of consensus.

4.THEORETICAL FUNDATIONS

4.1 Flutter

Flutter is a cross-platform framework that targets developing high-performance mobile applications. Flutter was publicly released in 2016 by Google. Besides running on Android and iOS flutter applications also run on Fuschia. Flutter is chosen as Google's application-level framework for its next-generation operating system. Flutter is exceptional because it is dependent on the device's OEM widgets rather than consuming web views. Flutter uses a high-performance rendering engine to render each view component using its own. This provides a chance to build applications that are as high-performance as native applications can be. In view of architecture, the engine's C or C++ code involves compilation with Android's NDK and LLVM for iOS respectively, and during the compilation process, the Dart code is compiled into native code. Hot reload feature in Flutter is called as Stateful hot reload and it is a major factor for boostingthe development cycle. Flutter supports it during development. Stateful hot reload is implemented by sending the updated source code into the running Dart /Virtual Machine (Dart VM) without changing the inner structure of the application, therefore the transitions and actions of the application will be well-preserved after hot reloading.

Flutter uses widgets as the main concept within the code. Widget is the nickname for every component part that is built in Flutter. This could mean a box or a text that is referred to as a widget.

A noticeable part of the widgets is that they are created by the Flutter developers to look native and developers are able to fully customize these to their liking.

4.2 Dart

In Flutter, every application is written with the help of Dart. Google has developed and maintained a programming language called Dart. It is extensively used inside Google and it has been verified to have the proficiency to develop enormous web applications, such as AdWords. Originally Dart was developed to replace and succeed JavaScript. Thus, it implements most of the important characteristics of JavaScript's next standard (ES7), such as the keywords "async" and "await". 15Nonetheless, to attract developers that are not acquainted with JavaScript, Dart has a Java-like syntax. Flutter application renews the view tree on every new frame even when few other systems use reactive views. This behavior leads to a drawback that many objects, which might survive for a singular frame, will be created. As Dart is a modern programming language, it is optimized to handle this scenario in memory level with the help of "Generational Garbage Collection".

4.3 Python

Historically, a wide range of different programming languages and environments have been used to enable machine learning research and application development. However, as the general-purpose. Python language has seen a tremendous growth of popularity within the scientific computing community within the last decade, most recent machine learning and deep learning libraries are now Python-based. With its core focus on readability, Python is a high-level interpreted programming language, which is widely recognized for being easy to learn, yet still able to harness the power of systems-level programming languages when necessary.

Aside from the benefits of the language itself, the community around the available tools and libraries make Python particularly attractive for workloads in data science, machine learning, and scientific computing. According to a recent KDnuggets poll that surveyed more than 1800 participants for preferences in analytics, data science, and machine learning, Python maintained its position at the top of the most widely used language in 2019. The amount of data being collected and generated today is massive, and the numbers continue to grow at record rates, causing the need for tools that are as performant as they are easy to use. The most common approach for leveraging Python's strengths, such as ease of use while ensuring computational efficiency, is to develop efficient Python libraries that implement lower-level code written in statically typed languages such as Fortran, C/C++, and CUDA. In recent years, substantial efforts are being spent on the development of such performant yet user-friendly libraries for scientific computing and machine learning.

The Python community has grown significantly over the last decade, and according to a GitHub report, the main driving force "behind Python's growth is a speedily-expanding 16community of data science professionals and hobbyists." This is owed in part to the ease of use that languages like Python and its supporting ecosystem have created. It is also owed to the feasibility of deep learning, as well as the growth of cloud infrastructure and scalable data processing solutions capable of handling massive data volumes, which make once-intractable workflows possible in a reasonable amount of time. These simple, scalable, and accelerated computing capabilities have enabled an insurgence of useful digital resources that are helping to further mold data science into its own distinct field, drawing individuals from many different backgrounds and disciplines. With its first launch in 2010 and purchase by Google in 2017, Kaggle has become one of the most diverse

of these communities, bringing together novice hobbyists with some of the best data scientists and researchers in over 194 countries. Kaggle allows companies to host competitions for challenging machine learning problems being faced in industry, where members can team up and compete for prizes. The competitions often result in public datasets that can aid further research and learning. In addition, Kaggle provides instructional materials and a collaborative social environment where members can share knowledge and code. It is of specific interest for the data science community to be aware of the tools that are being used by winning teams in Kaggle competitions, as this provides empirical evidence of their utility.

4.4 Distributed File Storage

Distributed File System (DFS) is a client-server based application which permits its users to access, process or modify the data which is stored on a remote server as if it existed on their own systems. When a client accesses a file, the server or the host provides the user a duplicate copy of the requested file. The file itself is cached on the user's system while the data is processed and returned back to the server. In DFS, multiple central servers store files, which can be accessed by several isolated users at a time in the network. With the proper authorization rights, clients only can access these files.

The client is able to work with the file in the same way as if it is stored locally on their local system. If the client is finished working with the file, it is returned over the network back to the server, which stores the original or altered file for retrieval at a later time by the same or another user. DFS also uses a different naming scheme to map and to keep the track of files located in different non-central servers.

It arranges its files according to the hierarchical file 17management system. DFS distributes the related documents over different clients by arranging a centralized storage. NFS from Sun Microsystems and DFS from Microsoft are some popular examples of distributed file systems. The reason behind the extensive utilization of DFS depends on the ease of their information sharing with multiple clients concurrently by exporting file systems efficiently. The main features such a International Conference on Computing, Communication and Automation (ICCCA 2016) 754 system must accomplish are: Data consistency, Uniform access, Reliability, Efficiency, Performance, Manageability, Availability, and Security.

4.5 Blockchain

Blockchain could be regarded as a public ledger and all committed transactions are

stored in a list of blocks. This chain grows as new blocks are appended to it continuously.

Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency.

Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services.

Those fields favor blockchain in multiple ways. First of all, blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers.

Besides, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain.

5. CONCLUSION

Blockchain technology presents a transformative solution to enhancing privacy and security in social media interactions. By decentralizing data storage and leveraging cryptographic encryption, blockchain eliminates the risks associated with centralized social media platforms, such as data breaches, unauthorized surveillance, and identity theft. Unlike traditional platforms that rely on centralized servers vulnerable to cyberattacks, blockchain-based social media systems distribute data across a secure network, significantly reducing single points of failure. This ensures that users have greater control over their personal data, mitigating risks of misuse .Enhancing Privacy and Security in Social Media Using Blockchain. *Blockchain technology can greatly improve privacy and security in social media by giving users more control over their personal information. Traditional social media platforms store user data on central servers, making them vulnerable to hacking and data leaks. With blockchain,*

decentralized identity systems like self-sovereign identities (SSI) allow users to verify their identity without sharing unnecessary details.

For example, if someone needs to prove they are over 18, they can do so without revealing their exact birthdate. This prevents personal data from being misused by companies for targeted ads or tracking. By using encryption and secure verification methods, blockchain helps keep user information private and safe.Additionally, blockchain can work with advanced technologies like artificial intelligence (AI) and zero-knowledge proofs (ZKPs) to improve security. AI can help detect harmful content like fake news or cyberbullying while ensuring fair moderation without bias. Meanwhile, ZKPs allow users to prove something (such as identity or participation in a vote) without revealing personal details. This makes online interactions safer and more private. As blockchain technology develops, it can help create social media platforms that prioritize user privacy, prevent data misuse, and promote a more secure online experience.

6. REERENCES

[1] T. Poongodi, R. Sujatha, D. Sumathi P. Suresh, B. Balamurugan1. (2020). *BLOCKCHAIN IN SOCIAL NETWORKING,* Cryptocurrencies and Blockchain Technologies & Applications, Chapter 4. Scrivener Publishing.

[2] Renita M. Murimi. (2019). *A Blockchain Enhanced Framework for Social Networking.* VOL 4, S1- pg:67-81. LEDGER Publishing.

[3] Archana Prashanth Joshi, Meng Han, Yan Wang.(2018). *SECURITY AND PRIVACY ISSUES OF BLOCKCHAIN TECHNOLOGY* Volume 1, Number 2.

[4] Shuai Zeng, Yong Yuan, Fei-Yue Wang,(2019), *A decentralized social networking architecture enhanced by blockchain,* IEEE.

[5] Shaik V. Akram, Praveen K. Malik, Rajesh Singh, Gehlot Anita, Sudeep Tanwar.(2020), *Adoption of blockchain technology in various realms: Opportunities and challenges.* Wiley.

[6] Le Jiang, Xinglin Zhang.(2019). *BCOSN: A Blockchain-Based Decentralized Online Social Network.* IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, VOL. 6. IEEE.

[7] Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland.(2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data.* CS Security and Privacy Workshops. IEEE.

[8]. Antorweep Chakravorty, Chunming Rong. (2017). *Ushare: user controlled social media based on blockchain.* IMCOM.

[9] Yanji Jiang, Xueli Shen, Sifa Zheng .(2021*). An Effective Data Sharing Scheme Based on*

Blockchain in Vehicular Social Networks. Electronics MDPI

[10] *Decentralized Social Networking Protocol*URL:https://drive.google.com/file/d/1IcZqMWCTYvgsuEMyKdRN11TBLkUUe8qn/view

[11] Ajay Kumar Shrestha, Julita Vassileva, Ralph Deters .(2020). A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives. Frontiers in Blockchain Volume 3. Frontiers . 34

[12] P. Freni, E. Ferro, G. Ceci .(2020). *Fixing Social Media with the Blockchain*. GoodTechs.

[14] Barbara Guidi .(2020). *When Blockchain meets Online Social Networks*. ELSEVIER.

[15] Chao Li, Balaji Palanisamy.(2019). Incentivized Blockchain-based Social Media Platforms: A Case Study of Steemit. WebSci.

[16] T. Cai, Z. Hong, S. Liu, W. Chen, Z. Zheng, and Y. Yu, "SocialChain: Decoupling social data and applications to return your data ownership," *IEEE Trans. Services Comput.*, vol. 16, no. 1, pp. 600–614, Jan./Feb. 2023.

[17] X. Zhu, D. He, Z. Bao, M. Luo, and C. Peng, "An efficient decentralized identity management system based on range proof for social networks," *IEEE Open J. Comput. Soc.*, vol. 4, pp. 84–96, Mar. 2023.

[18] F. Li, X. Yu, R. Ge, Y. Wang, Y. Cui, and H. Zhou, "BCSE: Blockchainbased trusted service evaluation model over big data," *Big Data Min. Anal.*, vol. 5, no. 1, pp. 1–14, Mar. 2022.

[19] A. Theophilo, R. Giot, and A. Rocha, "Authorship attribution of social media messages," *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 1, pp. 10–23, Feb. 2023.

[20] P. Piamjinda et al., "CHIVID: A rapid deployment of community and home isolation during COVID-19 Pandemics," *IEEE J. Transl. Eng. Health Med.*, vol. 12, pp. 390–400, 2024.