Photochain: A Blockchain Based Secure Photo Sharing Framework for Cross-Social Network

***Benisha*[1], *Agilan*[1], *Latha M* [2]**

[1]*Student, Department of Computer Science and Engineering, Adithya Institute of Technology, Anna University, Tamilnadu, India*

[2]*Supervisor, Department of Computer Science and Engineering, Adithya Institute of Technology, Anna University, Tamilnadu, India.*

Corresponding Author: benireddy101@gmail.com

Abstract: - In recent years, online social networks (OSNs) have become increasingly popular due to the rapid development of mobile applications and the explosive growth in online interaction. With the growth and accessibility of technology and internet, the ease of posting and sharing photos on social networking services (SNSs) has increased exponentially. The privacy of online photos is often protected carefully by security mechanisms. However, these mechanisms will lose effectiveness when someone spreads the photos to other platforms the illegal disclosure of user's private data can cause damaging consequences and even threaten the safety of users' life. In recent years, there are some research works to address this privacy issue, yet they do not always focus on providing the normal social network services for users, such as data sharing, data retrieval and data access services. Therefore, it is a challenge to ensure the security of sensitive data while providing efficient and privacy-preserving social network services for users. In this paper, we propose PhotoChain, a blockchain-based secure photo sharing framework that provides powerful dissemination control for cross-social network photo sharing. Combined blockchain, Gaussian Blurr for Face Masking, PreHash Algorithm for Photo integrity verification and Access Control, Mechanism can achieve secure data sharing, data retrieving, and data accessing with fairness and without worrying about potential damage to users' interest. In contrast to security mechanisms running separately in centralized servers that do not trust each other, our framework achieves consistent consensus on photo dissemination control through carefully designed smart contract-based protocols. Considering the possible privacy conflicts between owners and subsequent re-posters in cross social network photo sharing, we design a dynamic privacy policy generation algorithm that maximizes the flexibility of re-posters without violating formers' privacy. Moreover, PhotoChain also provides robust photo ownership identification mechanisms to avoid illegal reprinting. Finally, this project implements a prototype of the framework and deploy it to a locally simulated social network. The extensive experiments and security analysis demonstrate the security, efficacy and efficiency of our proposed framework.

Key Words: —*Photo chain, Block-chain technology,* PreHash Algorithm, Prototype of the framework, Locally simulated social network, Data sharing, Data retrieving, and data accessing.

I. Introduction

With the huge popularity of sharing and the vast usage of social networking sites users unknowingly reveal certain kinds of personal information. Social-networking users may or may not have the idea of getting their personal information will be leaked or could pro t the malicious attackers and may perpetrate significant privacy breaches. The rest decade of 21st century has seen the extreme popularization of Internet and the growth of web services which facilitate participatory information sharing and collaboration. Social Networking Sites (SNSs) have become a boundless communication media to keep in touch beyond boundaries. SNSs are a part of human culture than just a web application. Use of SNSs has out spaced in almost every field as news agencies, big and small companies, governments, and famous personalities etc. to interact with each other. With the adoration

Manuscript revised May 14, 2023; accepted May 15, 2023. Date of publication May 17, 2023.

This paper available online at www.ijprse.com

ISSN (Online): 2582-7898; SJIF: 5.59

of sharing, socialmedia has stood out as the most renown SNSs in the world were people hangout for hours. With the extravagancy of technology and services sharing of news, photos, personal taste and information with friends and family has led to an ease. But along with this user privacy should also be taken into consideration. An issue related to privacy with socialmedia users has been constantly appearing on international press either because of the company's privacy policy or because of users unaware-ness of content sharing consequences. As research says the simple disclosure of date and place of birth of a profile in socialmedia can be used to predict the Social Security Number (SSN) of a citizen in the U.S. Many a times just by simply publishing their friends list, users might be revealing a large amount of information. For example, through the use of prediction algorithms it is possible to infer private information that was previously undisclosed. Sometimes sensitive information even comes embedded in the photo as metadata and may identify people on the photo by accompanying more information that could be exploited, like captions, comments and photo tags; marked regions. Even if the individuals in a photo are not explicitly identified by photo tags, the combination of publicly available information and face recognition software can be used to infer some one's identity. These kinds of problems are defined as collateral damage: users unintentionally put their own privacy or their friend's privacy at risk when performing events on SNSs such as social media. The main focus is to let each user only deal with his/her private photo set as the local train data which can be used by the users to learn out the local training result. Once the local training results are achieved then it can be exchanged among various users to form a global knowledge.

Agreeableness (A) means is one of the five personality traits of the Big Five personality theory. A person with a high level of agreeableness in a personality test is usually warm, friendly, and tactful. They generally have an optimistic view of human nature and get along well with others. Neuroticism (N) Means is one of the Big Five higher-order personality traits in the study of psychology. Individuals who score high on neuroticism are more likely than average to be moody and to experience such feelings as anxiety, worry, fear, anger, frustration, envy, jealousy, guilt, depressed mood, and loneliness, which will be further, used by the system to shortlist their CV or candidates. After completing the top 10 or above shortlisted candidates, auto mail is sent. We present a set of techniques that makes the whole recruitment process more effective and efficient also. We have implemented a system that ranks the top employee based on work feedback policy as well as suggestions. This system will focus not only in qualification and in experience but also focuses on other important aspects, which are required for a particular job position. This system will help the human resource department to select the right candidate for a particular job profile, which in turn provides an expert workforce for the organization. For all this process we use Artificial Intelligence (AI). It refers to technology used to do a task that requires some level of intelligence to accomplish. AI technologies offer significant opportunities to improve HR functions to Finding the right information, with lower costs, in less time and in a secure manner helps to build momentum step by step, beginning with the recruitment process.

1.1 Algorithms and Techniques used

- Smart Contract
- Gaussian Blur
- PreHash Algorithm
- Access Control mechanism
- Hash Key to verify the integrity of the shared photo

II. Software Description

2.1 Python 3.7.4

Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This tutorial gives enough understanding on Python programming language.

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. Python is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. Python is currently the most widely used multi-purpose, high-level programming language. Python allows programming in Object-Oriented and Procedural paradigms. Python programs generally are smaller than other programming languages like Java. Programmers have to type relatively less and indentation requirement of the language, makes them readable all the time. Python language is being used by almost all tech-giant companies. The biggest strength of Python is huge collection of standard libraries which can be used for the following:

- Machine Learning
- GUI Applications
- Web frameworks
- Image processing
- Web scraping
- Test frameworks
- Multimedia
- Scientific computing
- Text processing and many more

III. Modules Description

3.1 SN Web App

Build a social networking service is an online platform in which people use to build social networks or social relationships with other people who share similar personal or career interests, activities, backgrounds or real-life connections. Social networking services vary in format and the number of features.

3.2 Ender user Cpanel

3.2.1. Register

Users in this application, who want to access and share their images into this site, they should register their information in this site. After they registered their data in this site, they can log into the application for providing and accessing images which are shared by their friends or some other persons in social networks. Users can not only look at the images from this site, but also, they can upload their images either by private or public. In which, users can give friend requests, accept friend requests, and key request to reveal private images in the site.

3.2.2. Login

The user will demonstrate social network features wherein he will perform following operations: [1] Edit Profile [2] View and Add Friends [3] Search Users [4] View User Profile

3.3. Add Friends /Family Groups

Friend Request A log in/out button could be used for log in/out with the social website. After logging in, a greeting message and the profile picture will be shown. This prototype works in three modes: a setup mode, a sleeping mode and a working mode.

Picking Close Friends, A user needs to manually specify the set of "close friends" from their friend list on social website and form the neighborhood by clicking the button "Pick friends".

3.4. Share/Post/Comment/Chat

Sharing Photo User can share a photo only to friends on list. According to the proposed scheme, this friend list should be intersection of owner's privacy policy and co-owners' exposure policies.

Policy mining: Users can establish the uploaded image whether the image is private or public; then eligible users (friend only view the public images) can access these images otherwise images will be hidden. If users want to view private content, then the content owner should provide the key for that image. Policy mining is carried out within the same category because images in the same category are more likely under a similar level of privacy protection. E) Policy prediction: In this phase they generate several candidate policies while the goal of this system is to return the most promising one to the user. Thus, it presents an approach to choose the best candidate policy that follows the user’s privacy tendency. It provides a predicted policy of a newly uploaded image to the user for their reference.

3.5. Request/Response

To respond to a friend request, you have two choices. One is to click one of the two buttons to the right of your potential friend's name. One button reads Confirm and one reads Not Now. Click one of those buttons and (respectively) you add a friend or ignore the request quietly.

IV. Photo Privacy

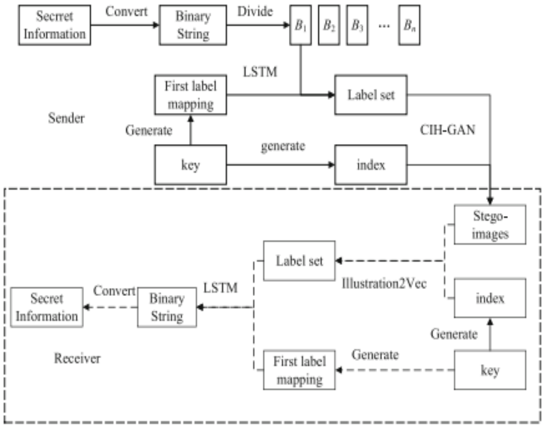
4.1. Key Generation

In this process, privacy information of the photo is protected by using the selected protection tool and a secret key (or a set of keys) set by the sender. Apart from providing a proper security level and an efficient implementation, one relevant challenge is to properly manage all the encryption keys used in the system. We propose a centralized approach where all keys are stored in the trusted Key Server.

It is essential that the server is able to uniquely identify images in order to be able to generate unique keys for each picture and region in it. As we have mentioned, the Key Server randomly generates a unique identifier for each protected picture that is sent back to the LockPic application at encryption time. This unique ID is included in the metadata of the encrypted picture. Another approach could be to use the hash of the picture as ID. The problem of using the hash as the ID is that the hash has to be performed in the mobile application, which might be an expensive operation depending on the size of the picture, and could present security problems in the case that hash collisions are found. More importantly, the key server would be able to analyse some usage patterns as it would be able to recognize if two different users encrypt the same picture.

4.2. Photo and Message Encode/Decode Image and Message Encoding

Our encoder network consists of down sampling layers, residual layers, and up sampling layers. The structure of encoder network is shown in Fig. 2. In the resent, it includes many skip connections to fuse the shallow features and deep features in the different convolution stages. The shallow feature includes a lot of low-level efficient information about the outline and color of image, which is very beneficial for the generation of steganographic images. The works of constructed the encoder network similar to the structure of U-Net, and its results have proved that the skip connection is effective to reduce the distortion of steganographic images and improve the visual quality of steganographic images.



a. original image

4.3 Image and Message Decoding

The decoder network composed of a 6-layer full convolutional network extracts the secret color images (S’) from steganographic images (C’). The decoder network and the encoder network in the previous section constitute the generator of the proposed model HIGAN. The architecture of the decoder network has been proven in previous work to effectively reconstruct single-channel grayscale secret images and three-channel color secret images. All 3×3 convolutional layers with stride 1 and padding 1 are followed by batch normalization (BN) operation and ReLU activation function. But, sigmoid activation function was used after the last convolutional layers. Finally, the decoder network reveals the secret image S’.

b. generated image

4.4. Photo Blurring

Gaussian blur (also known as Gaussian smoothing) is the result of blurring an image by a Gaussian function (named after mathematician and scientist Carl Friedrich Gauss).

It is a widely used effect in graphics software, typically to reduce image noise and reduce detail. The visual effect of this blurring technique is a smooth blur resembling that of viewing the image through a translucent screen, distinctly different from the bokeh effect produced by an out-of-focus lens or the shadow of an object under usual illumination.

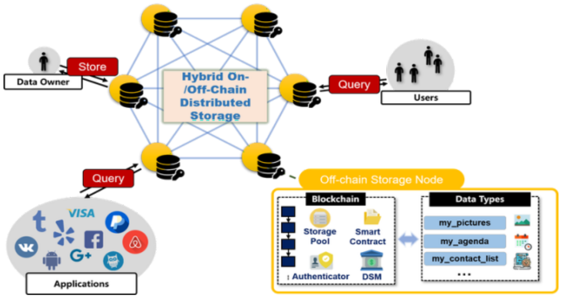
Gaussian smoothing is also used as a pre-processing stage in computer vision algorithms in order to enhance image structures at different scales—see scale space representation and scale space implementation.

4.5 Privacy Violation

Check Policy Status The privacy policy status is set for individual users. The policy should satisfy both the privacy policy and the exposure policy of the individuals. Post or Block If the policy is satisfied then the notification is sent to the co-owner. The photo is posted once the owner gives permission to upload it else it is not uploaded.

V. PhotoChain Integration

PhotoChain, which is a decentralized SN data storage and sharing system based on blockchain that decouples user data and applications to return data ownership to the user.



We adopt Personal Data Store to extend off-chain storage for the online data, set up an identity establishment mechanism that can support WebID-based authentication functions using a unique identity assignment (i.e., WebID) as well as certificateless cryptography, and design a general framework that leverages smart contracts to help securely store and share social data in an automated manner.

5.1 Photo Verification Module

This module retrieves auditing information from blockchain regarding data access and usage upon data owner or auditor request leveraging the traceability feature provided by the blockchain.

5.2 Test Cases and Expected Results

5.2.1 Test Case: Uploading a photo with face detection enabled

- Input: Upload a photo with the "Face Detection" feature enabled
- Expected Result: The system should detect faces in the photo and automatically blur them using the Gaussian blur algorithm, and the blurred photo should be stored securely on the blockchain.

5.2.2 Test Case: Requesting access to a photo

- Input: Request access to a photo that has been shared with you
- Expected Result: The photo owner should receive a notification that a request for access has been made, and the owner should be able to grant or deny access to the photo. If access is granted, the user should be able to view the photo.

5.2.3 Test Case: Photo integrity check

- Input: Upload a photo and check its integrity
- Expected Result: The system should generate a PreHash for the photo and store it on the blockchain. When the photo is accessed or downloaded, the system should check the photo's PreHash against the stored value to ensure that the photo has not been altered or tampered with.

5.2.4 Test Case: Cross-Social Network Sharing

- Input: Share a photo on one social network and access it from another social network
- Expected Result: The photo should be accessible from both social networks, and the face detection and photo integrity features should be applied regardless of the social network on which the photo was shared.

5.2.5 Test Case: Stress testing

- Input: Simulate a high volume of photo uploads and access requests
- Expected Result: The system should be able to handle a large volume of requests and uploads without crashing or slowing down. The system should scale up as needed to handle the increased traffic.

5.2.6 Test Case: Integration Testing

- Input: Integrate the platform with third-party services or social media platforms
- Expected Result: The platform should be able to interact with external APIs and transfer data correctly between systems without any loss of data or functionality.

By performing these tests and ensuring that the expected results are met, developers can ensure that PhotoChain is functional, secure, and user-friendly, and meets the needs of its intended user base.

5.3 Future enhancement

There are several areas where Photochain can be enhanced and improved for better performance and user experience. Some of the potential future enhancements for Photochain include:

- *Integration with more social media platforms:* Currently, Photochain is designed to work with a limited number of social media platforms. Future enhancements can include expanding the framework to integrate with more social media platforms, making it more accessible to a wider range of users.
- *AI-based photo recognition:* The use of artificial intelligence (AI) algorithms can help in the automatic recognition of photos based on their content. This feature can enhance the search and discovery of photos, making it easier for users to find the photos they are looking for.

- *Integration with decentralized storage systems*: Photochain can be integrated with decentralized storage systems such as IPFS or Swarm to provide a more secure and reliable storage solution for photos.
- *Improved user interface*: The user interface of Photochain can be improved to make it more user-friendly and intuitive, making it easier for users to manage and control their photos.
- *Integration with third-party apps***:** Photochain can be integrated with third-party apps such as photo editors, adding more functionality and features to the framework.

Hence, these future enhancements can help Photochain to become a more comprehensive and efficient photo sharing framework, providing better security, privacy, and user experience to its users.

VI. Conclusion

In conclusion, the Photochain framework provides a secure and efficient way to share photos across multiple social media platforms, using the power of blockchain technology, pre-hashing algorithm, and Gaussian blur technique provides an innovative and secure solution to the challenges of sharing personal photos across multiple social media platforms. The use of pre-hashing algorithm ensures that photos are not tampered with and are only accessible by authorized users. The Gaussian blur technique further enhances the privacy of the photos, making them less recognizable to anyone who might try to access them without authorization. The Photochain framework leverages the decentralized and immutable nature of blockchain technology to ensure that users have control over their photos and can share them securely without the risk of unauthorized access, infringement of privacy, or theft. The use of smart contracts enables automated and secure photo sharing while maintaining the privacy of users. The proposed Photochain framework also provides a user-friendly interface that allows users to easily manage and control their photos while maintaining full ownership of their data. Additionally, the framework enables the seamless transfer of photos across social media platforms, simplifying the photo-sharing process for users. Thus, the blockchain-based secure photo sharing framework has the potential to transform the way people share personal photos online, providing a more secure and efficient method of sharing personal photos across social networks. The framework can be further enhanced and expanded to address the emerging needs and challenges of photo sharing in the rapidly evolving digital landscape.

References

[1]. A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang," Social circles: Tackling privacy in social networks", in Proc. Sympsable Privacy Security, 2008.

[2]. J. Bonneau, J. Anderson, and L. Church," Privacy suites: Shared privacy for social networks", in Proc. Symp. Usable Privacy Security, 2009

[3]. C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt," Providing access control to online photo albums based on tags and linked data", pp. 9-14, 2009.

[4]. A. Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1563-1572, 2010.

[5]. Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham," Semantic web-based social network access control", pp. 108-115, 2011.

[6]. CareerBuilder. Number of Employers Using social media to Screen Candidates has Increased 500 Percent Over the Last Decade. Accessed: Jun. 8, 2019.

[7]. J. Bort. A High School Coach was Fired for this Facebook Photo. Accessed: Jun. 8, 2019.

[8]. J. Dent. Revenge Porn: Image-Based Abuse Hits 'One in Five' Australians. Accessed: Jun. 8, 2019.

[9]. G. Kaszubska. Not Just 'Revenge Porn'—Image-Based Abuse Hits 1 in 5 Australians. Accessed: Jun. 8, 2019.

[10]. A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, ''A3P: Adaptive policy prediction for shared images over popular content sharing sites,'' in Proc. 22Nd ACM Conf. Hypertext Hypermedia, New York, NY, USA, 2011, pp. 261–270.