IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 13, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

Photo Chain: A Blockchain based Secure Photo Sharing Framework for Cross-Social Network

Dr .R. Vadivelu [1], S.Ajmeer Kaja [2], K.Arun Vinod [3]

Head of the Department, Department Of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology,Coimbatore,Tamilnadu, India[1]

U.G Scholar, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology Coimbatore, Tamilnadu, India [2, 3]

ABSTRACT: Social Networks is one of the major technological phenomena on the Web 2.0. The evolution of social media has led to a trend of posting daily photos on online Social Network Platforms (SNPs). 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. We propose PhotoChain, a blockchain-based secure photo sharing framework that provides powerful dissemination control for cross-SNP photo sharing. 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. We use these protocols to create platform-free dissemination trees for every image, providing users with complete sharing control and privacy protection. Considering the possible privacy conflicts between owners and subsequent re-posters in cross-SNP sharing, we design a dynamic privacy policy generation algorithm that maximizes the flexibility of re-posters without violating formers' privacy. Moreover, Go-sharing also provides robust photo ownership identification mechanisms to avoid illegal reprinting. It introduces a random noise black box in a two-stage separable deep learning process to improve robustness against unpredictable manipulations. Through extensive real-world simulations, the results demonstrate the capability and effectiveness of the framework across a number of performance metrics.

KEYWORDS: Photo sharing, Privacy-preserving, Cross-SNP, Blockchain.

I. INTRODUCTION

Blockchain is one of the most cutting edge, disruptive application technologies today. In the blockchain network, all user transactions are recorded in a distributed ledger. The framework for consensus means that all blockchain nodes need to be approved before transactions are recorded. It prevents data manipulation or retrievals, most importantly, platform network and mobile technologies. This method propose a blockchain based privacy-preserving photo sharing framework for online social networks, which enables the photo sharer to enjoy efficient and privacy-preserving social network service. THe number of photos being posted on various Social Network Platforms (SNPs) is increasing exponentially. More than 120 million active Instagram users will upload photos daily, and more than 567 million photos are uploaded to Facebook2 every day. This widespread photo sharing causes privacy concerns. Users frequently attempt to repost or upload photos from other users without permission .Some research attempts to circumvent these issues and increase user privacy protection. For instance, Privacy Respecting-based Sharing schemes have been proposed to protect users' privacy by requiring photo service
providers (or picture takers) to enforce privacy policies .Some research attempts to circumvent these issues and increase user privacy protection. For instance, Privacy Respecting-based Sharing schemes .have been proposed to protect users' privacy by requiring photo service providers (or picture takers) to enforce privacy policies.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

II. RELATED WORK

1. Influencing Photo Sharing Decisions on Social Media: A Case of Paradoxical Findings

Author: Mary Jean Amon ; Rakibul Hasan; Kurt Hugenberg; Bennett I. Bertenthal; Apu Kapadia

Date of Publication: 21 May 2020

Proposed Methodology

Here the effects of perspective taking, privacy cues, and portrayal of photo subjects on decisions to share photos of people via social media. In an online experiment we queried 379 participants about 98 photos in three conditions: (1) Baseline: participants judged their likelihood of sharing each photo; (2) Perspective-taking: participants judged their likelihood of sharing each photo when cued to imagine they are the person in the photo; and (3) Privacy: participants judged their likelihood to share after being cued to consider the privacy of the person in the photo. While participants across conditions indicated a lower likelihood of sharing photos that portrayed people negatively, they - surprisingly - reported a higher likelihood of sharing photos when primed to consider the privacy of the person in the photo. Frequent photo sharers on

real-world social media platforms and people without strong personal privacy preferences were especially likely to want to share photos in the experiment, regardless of how the photo portrayed the subject. These findings suggest that developing interventions for reducing photo sharing and protecting the privacy of others is a multivariate problem in which seemingly obvious solutions can sometimes go awry.

2. My Privacy My Decision: Control of Photo Sharing on Online Social Networks

Author: Kaihe Xu; Yuanxiong Guo; Linke Guo; Yuguang Fang; Xiaolin Li

Date of Publication: 10 June 2015

Proposed Methodology

Photo sharing is an attractive feature which popularizes online social networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus-based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform.

3. Security of Photo Sharing on Online Social Networks

Author: Harshali Chandel1, Dr. A. M. Bagade

Date of Publication: 6, June 2017

Proposed Methodology

Photo sharing is an attractive feature in Online Social Networks (OSNs) but it may leak users privacy if they are allowed to post, comment, and tag a photo freely. This issue of sharing the photos of individual or himself/herself is addressed by the proposed scheme. The proposed scheme is used to prevent possible privacy leakage of a photo. For this purpose, an efficient facial recognition (FR) system is required that can recognize everyone in the photo. However, to train the FR system, more demanding privacy setting may limit the number of the photos that are publicly available. To solve this problem, the proposed scheme attempts to utilize users private photos by designing a personalized FR system and also provide security while posting the photo. A distributed consensus based method is also developed to reduce the computational complexity and protect the private training set. The efficiency of proposed scheme is calculated by using recognition ratio. The proposed mechanism is implemented as a proof of concept on Android

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

application in OSN's (Online Social Networks) on Facebook platform.

4. Photo sharing and storing over online social networks based trust & privacy

Author: VATSAVAI SRIJA & T SAI DURGA

Date of Publication: 7 July 2020

Proposed Methodology

In online web world, social networking sites are playing major role with various advantages. The main advantages of social network are creation of the social circle virtually and share data to friends and public. Sharing data like photos and videos in online social applications has now become a common behavior for sharing their status, mood and activity with their social associations or public. While sharing these data like pictures may consists of other user's information, publisher may tag to the other users who are present in the data or tag to the users who relative that post, this process is called Tagging. This tagging may damage the tagged user's privacy that may express data of user's location, presence or sexual content etc. It is a

privacy loophole for the user's who are taking space in the photo with publisher of the picture. Privacy preserving in social networks in sharing data is current hot research topic in Social Networking. For this we are proposing a system called Privacy Preserving Framework for sharing data in social networks. Our System will identify the co-owner faces from the sharing data and tag to the co-owner's accounts for taking permission from the co-owners. For this we are using Machine Learning methods of KNeighbours Classifier algorithm for detection of users in shared data.

III. EXISITING SYSTEM

- **Invisible Cloak**

Proposed a new method, named one person one mask (OPOM), to generate person-specific (class-wise) universal masks A cloaking device is a hypothetical or fictional stealth technology that can cause objects, such as spaceships or individuals, to be partially or wholly invisible to parts of the electromagnetic (EM) spectrum.

- **QR Code**

A QR code (short for Quick Response code) is an array of black and white squares or pixels set in a grid that stores data for a machine to read .QR codes with high-quality images can prevent photographs that are uploaded to the social network.

- **Attribute Based Encryption (ABE):**

ABE is an encryption schema which can perform a fine-grained access control with encryption where a user with certain attributes can read the data or parts of the data which the attributes grant access to. When compared with other schemas ABE has a complex access control and decryption process. The public is generally hosted in the cloud which can be accessed by the users in the cloud to create their private keys. Using attributes, we can make use of both IBE and RBAC algorithms using ABE. This motivated me to pursue a study based around ABE schemas.

IV. PROPOSED SYSTEM

- **PhotoChain**

A blockchain-based secure photo sharing framework that provides powerful dissemination control for cross-social network photo sharing. we propose a classification table of private information for images in Social Networking Services as such guidelines in order to improve privacy awareness and prevent future privacy invasion. We then verify it by submitting the table to the users and asking them to rank information according to privacy level. Results reveal

that people agree to it and feel the need of such classification table. Finally propose a method that uses these guidelines in order to create settings for access control.

- **Gaussian Blur**

A **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.

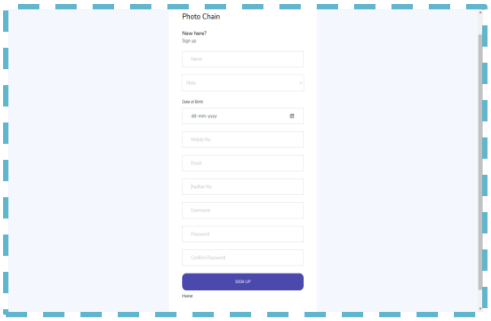
- **PreHash Algorithm**

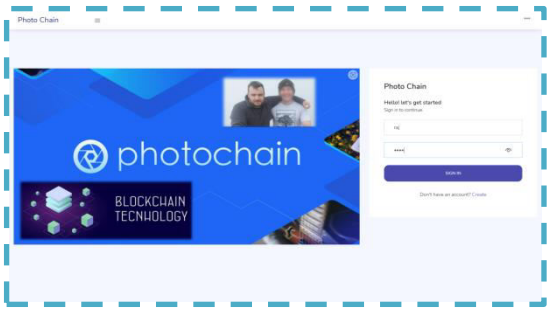
For photo integrity verification, The prehash crate provides the type Prehashed , which stores a value of any type along with aprecomputed hash. This makes it possible to avoid computing large expensive hashes many times, for example when searching for a particular value in a variety of hash tables.

V. METHODOLOGY

- **Social Networking Web App**

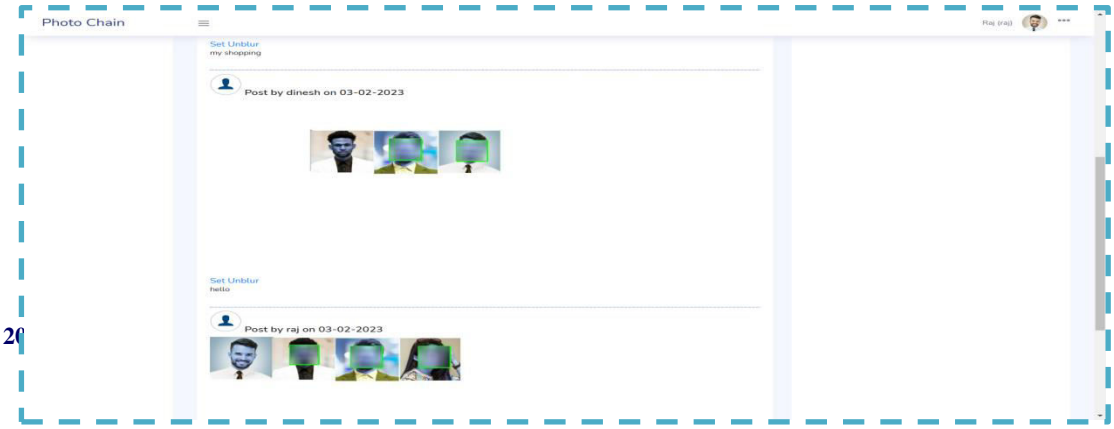
Build a social networking service is an online platform in which people use to build social networks or social relationships with other people who share similar personal or career interests, activities, backgrounds or real-life connections.Through this web app one care share their personal photos or images.





- **Photo Blur**

Gaussian blur (also known as Gaussian smoothing) is the result of blurring an image by a Gaussian function.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 Security effect produced by an out-of-focus lens or the shadow of an object under usual illumination**.**



|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

- **Photo Privacy Violation**

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.

VI. CONCLUSON

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.

REFERENCES

1. P. Oghazi, R. Schultheiss, K. Chirumalla, N. Philipp Kalmer and Fakhreddin F. Rad, "User self-disclosure on social network sites: A cross-cultural study on Facebook's privacy concepts", Journal of Business Research, vol. 112, pp. 531-540, 2020.
2. R. Hasan et al., "Can privacy be satisfying? On improving viewer satisfaction for privacy-enhanced photos using aesthetic transforms", Proc. CHI Conf. Hum. Factors Comput. Syst., pp. 1-13, 2019.
3. L. Pan, R. Hartley, M. Liu and Y. Dai, "Phase-only image based kernel estimation for single image blind deblurring", Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 6027-6036, 2019.
4. K. Ghazinour and J. Ponchak, "Hidden privacy risks in sharing pictures on social media", Procedia Comput. Sci., vol. 113, pp. 267-272, Dec. 2017.
5. K. Ghazinour and J Ponchak, "Hidden Privacy Risks in Sharing Pictures on Social Media", Procedia computer science, vol. 113, pp. 267-272, 2017.
6. L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure jpeg," in Computer Communications Workshops, 2015.
7. M. Duggan and J. Brenner, "The demographics of social media users 2012," 2013
8. K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 2, March 2017
9. C. Ma, Z. Yan, and C. W. Chen, "Scalable access control for privacyaware media sharing," IEEE Transactions on Multimedia, pp. 1–1, 2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details