IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12569

PHOTO CHAIN A BLOCKCHAIN BASED SECURE PHOTO SHARING FRAMEWORK FOR CROSS-SOCIAL NETWORK

Mr.A.Anist[1], M.Prajith[2], M.Raymond Raj[3], L.Sathiya Prakash[4]

[1] Assistant Professor, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India

[2]B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India

[3]B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India

[4]B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India

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 user's life 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. The extensive experiments and security analysis demonstrate the security, efficacy and efficiency of our proposed framework.

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 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 of sharing, Facebook has stood out as the most renown SNSs in the world where 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 facebook users has been constantly appearing on international press either because of the companies privacy policy or because of users unaware-ness of content sharing consequences.

As a research says the simple disclosure of date and place of birth of a pro le in Facebook 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 someone's identity. These kinds of problems are defined as collateral damage: users unintentionally put their own privacy or their friends privacy at risk when performing events on SNSs such as Facebook.

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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12569

II.LITERATURE SURVEY

[1]*Hidden Privacy Risks in Sharing Pictures on Social Media*

Author: Kambiz Ghazinour *, John Ponchak
Year: 2017

Problem identified:
People are sharing more data, and with more people, such unknowing users easily become the victims of numerous types of privacy attacks.

Objective:
The aim of this project is each piece of media shared has hidden privacy violations stored in their metadata. Over the past two decades, social media sites, and shared media on them, have grown exponentially.

Methodology:
In this study creating a GUI based metadata reader and editor, much of this security risk can be alleviated for common users. By bringing the capability to view and change metadata to different platforms, the true risk, hidden in all shared media, can be brought outright and mitigated.

Findings:
This paper is to help the problem to growing usage of social media networks have opened a new world of privacy concerns. At the top of this list is the exploitation of metadata of uploaded media, such as photos and videos. To combat this growing issue, we have developed a model and an application to allow users to easily view their metadata, change their metadata, and hide their true posting location.

[2].*Photo Sharing in Social Media Platform*

Author: R. Regin, B. Sneha
Year: 2022

Problem identified:
The social communication platform, sharing snapshots, videos, and much more information has become a prominent way of retaining connections with multiple users. Despite the sensitive data the photo holds, it will be an effortless way for the evil-minded user to steal the data of those who appear in the picture.

Objective:
To aim of this project privacy-protected mechanism based on the level of assurance the interconnected client gives to the person who uploads the picture. The thought process of this mechanism is while uploading an image of a co-owned photo, and a request is sent to the related user based on the reply the related user gives; the photo is displayed to the followers of the uploader. With the help of this privacy, the related user will not be compromising.

Methodology:
This paper brings out an adaptive concealment policy indicator mechanism stated in that provides a policy to the client while sharing the picture with multiple clients. This policy helps the client decide whether to share an image based on their trust in the recipient.

Findings:
This paper is help to the problem of Sharing sensitive information such as images and videos may help connect with others. On the other side, those data may be misused and threaten the lives of others. The privacy-protected photo sharing mechanism helps users bother about their privacy the most to connect with others and safeguard sensitive information. finally, it displays a hidden image where the particular person's face is blurred. This proposed mechanism proves to be an effective method in controlling the loss of privacy.

[3] *My Privacy My decision: Control of Photo Sharing on Online Social Networks*

Author: Prashant Abhang, S. B. Rathod
Year: 2017

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12569

Problem identified:
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.

Objective:
To this project proposes an efficient facial recognition system that can recognize everyone in the photo. Online photo sharing applications have become popular as it provides users various new and innovative alternatives to share photos with a range of people.

Methodology:
In this study of mechanism has been designed to make users aware of the posting activity and make them actively take part in the photo posting and decision-making paradigm for which a facial recognition (FR) system is recommended which can recognize everyone present in the photo.

Findings:
The proposed scheme is very useful in protecting users' privacy in photo/image sharing over online social networks. Photo sharing is the process of publishing or transfer of a user's digital photos on-line. Individuals in a co-photo are identified by the proposed FR system. The system reveals the detailed description of our system.

[4]. Security Concerns during Photo Sharing in Social Network Platforms

Author: T Maragatham, P Yuvarani
Year: 2020
Problem identified:
Security concern mechanism is outlined to assist the distributor to form an educated choice. Or maybe, the distributor predicts the misfortune of security for any connected client as it were since a single client offers the symbol.

Objective:
To proposed believe based privacy-preserving photo sharing in online social systems. This strategy chooses the picture's fashion and compared to numerical points of interest. Pictures give the onlooker with a number of expand records, now and then unfavorable to the protection of the individual.

Methodology:
A Privacy Concerns for Photo Sharing in Online Social Networks is proposed to help the publisher to make a proper decision. Different from our previous work the publisher does not communicate with other related users before he posts the photo. Instead, the publisher predicts the privacy loss to each related user in case that the photo is shared with a certain user. This mechanism explores the trust between users to measure the privacy loss.

Findings:
A system for security employments in specific values to characterize an anonymized picture. With the assistance of the benefit supplier, the picture that a client wishes to compare is held quickly. The benefit merchant calculates the extent of misfortune of security by sharing the picture as empowered by the relationship of certainty between the users. Instead, by utilizing the author, the benefit merchant makes a choice with the help of comparing the misfortune of security with a edge such that an unbiased must be evacuated from the picture.

[5] ***Trust-based Privacy-Preserving Photo Sharing in Online Social Networks.***

Author: Lei Xu, Ting Bao
Year: 2018

Problem identified:
The rich information contained in a photo makes it easier for a malicious viewer to infer sensitive information about those who appear in the photo. How to deal with the privacy disclosure problem incurred by photo sharing has attracted much attention in recent years.

Objective:
To propose a trust-based privacy preserving mechanism for sharing such co-owned photos. The basic idea is to anonymize the original photo so that users who may suffer a high privacy loss from the sharing of the photo cannot be identified from the anonymized photo. The privacy loss to a user depends on how much he trusts the receiver of the photo.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12569

Methodology:
In this study the help of image processing techniques, we can realize a fine-grained privacy management of photo sharing. In, Ilia et al proposed an access control model for photo sharing, where a photo is transformed into a set of layers each of which contains a single blurred face. Based on each user's privacy policy, the final photo presented to a viewer is generated by superimposing certain layers. In [17], Lee et al proposed a multiparty access model for photo sharing in OSNs, where the granularity of access control can be gradually tuned from photo level to face level.

Findings:
This paper is to help the problem sharing one co-owned photo in an OSN may compromise multiple users' privacy. To deal with such a privacy issue, in this paper we propose a privacy-preserving photo sharing mechanism which utilizes trust values to decide how a photo should be anonymized. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

[6]. *Influencing Photo Sharing Decisions on Social Media: A Case of Paradoxical Findings*.

Author: Mary Jean Amon ,Rakibul Hasan
Year: 2019

Problem identified:
The follow-up study with 100 participants explaining their responses revealed that the Privacy condition led to a lack of concern with other privacy. 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.

Objective:
To this has not been an extensive focus of past research in the photo sharing literature, as we discuss below, we hypothesize that habitual photo sharing may play a potent role in individuals future willingness to share photos. Balancing privacy and accessibility is a chronic problem in security, and we believe that behavioral interventions may play an important role in helping people sensibly choose when photo-sharing may be harmful to others.

Methodology:
In this study of the there are privacy-preserving sharing platforms that enable users to publish privacy preferences so that nearby photographers can learn and respect their preferences ,including I-Pic and COIN , which alert registered users whenever another user in the vicinity takes a photo. Thus, in the present work we also investigate the extent to which participants are high middling-, or low-frequency sharers of photos.

Findings:
Finally, the present research focused exclusively on meme like photos. Whereas these photos are consistently shared using traditional social media platforms such as Facebook, it is unclear whether the present results would generalize to more ephemeral photo-sharing platforms such as Snapchat. The more ephemeral nature of these media may encourage additional risk-taking (i.e., sharing very personal or embarrassing photos), which may make the paradoxical effects of our interventions even more potent in such contexts. The goal of developing new interventions for reducing photo sharing, especially of embarrassing or unflattering photos, is clearly a multivariate problem that will require a great deal more research.

[7].*Detection of Morphed Face Images Using Discriminative Wavelet Sub-bands*

Author: Poorya Aghdaie, Baaria Chaudhary
Year: 2021

Problem identified:
Morphed images have exposed face recognition systems' susceptibility to false acceptance, resulting in dire consequences, especially for national security applications. To detect morphing attacks, we propose a method which is based on a discriminative 2D Discrete Wavelet Transform (2D-DWT).

Objective:
To aim of this project is propose a method which is based on a discriminative 2D Discrete Wavelet Transform (2D-DWT). A discriminative wavelet sub-band can highlight inconsistencies between a real and a morphed image. We observe that there is a salient discrepancy between the entropy of a given sub band in a bona fide image, and the same sub-band's entropy in a morphed sample.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12569

Methodology:
A morphed image is generated using genuine face images from two different individuals. Because the resulting morphed image inherits characteristics of both subjects, it can be verified against both real subjects. Morphed images are generated using two approaches. In the first approach [1]–[3], two real face images are alpha blended in order to create a morphed image.

Findings:
In this paper, we proposed a framework to detect morphed face images using undecimated 2D-DWT. To select the optimal and informative bands, we found the distribution of the entropy for all the 48 wavelet sub-bands considering both the bona fide, and morphed images. The KL-divergence between the given distributions, integrated in a data-driven approach, led us to select the 22 most discriminative sub-bands.

[8].*Security of Photo Sharing on Online Social Network*

Author: Harshali Chandel, Dr. A. M. Bagade2
Year: 2017

Problem identified:
Social-networking users may or may not have the idea of getting their personal information will be leaked or could profit the malicious attackers and may perpetrate significant privacy breaches. Thefirst decade of 21st century has seen the extreme popularization of Internet and the growth of web services which facilitate participatory information sharing and collaboration.

Objective:
The proposed scheme is used to prevent possible privacy leakage of a photo. Forth is 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 user's private photos by designing a personalized FR system and also provide security while posting the photo.

Methodology:
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 of sharing, Facebook has stood out as the most renown SNSs in the world where people hangout for hours. With the extravagancy of technology and services sharing of news, photos, personal taste and information with friends and family has lead to an ease.

Findings:
Photo sharing is one of the most popular features in online social networks such as Facebook. Photo sharing is the process of publishing or transfer of a user's digital photos online. To control the privacy leakage, this project proposed the FR system to identify the individuals in a co-photo. After identifying the individual, with their permission the photo will be post. The proposed system is featured with low computation cost and confidentiality of the training set. Various websites offer services such as uploading, hosting, and managing for photo-sharing (publicly or privately).

[9].*Photo Sharing And Storing Over Online Social Networks Based Trust & Privacy*

Author: Vatsavai Srija & T Sai Durga
Year: 2020

Problem identified:
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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12569

Objective:
To 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 K- Neighbours Classifier algorithm for detection of users in shared data.

Methodology:
In this study of the face matching concept, we are using the K-Nearest Neighbour's algorithm. In the KNN algorithms there are multiple sub methods are there, in our project we are using Ball-Tree algorithm. Ball-Tree algorithm also called as Binary Tree algorithm. In this algorithm each and every node creates a D-dimensional hypersphere, containing a subset of the points to be searched. After constructing the B–Tree we save the prediction parameters in clf file.

Findings:
This paper is to help for this we are using Machine Learning methods of K-Neighbours Classifier algorithm for detection of users in shared data. Based on these situations we are proposing a system called Privacy Preserving Framework for sharing data in social networks. Our architecture will match the co-owner faces from the sharing data and tag to the co-owner's accounts for taking permission from the co-owners.

III.PROPOSED SYSTEM

Photo chain, a blockchain-based secure photo sharing framework that provides powerful dissemination control for cross-social network photo sharing. Combined blockchain, Gaussian Blur for Face Masking, Pre-Hash 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.

Algorithms and Techniques used:
- Smart Contract
- Gaussian Blur
- Pre-Hash Algorithm
- Access Control mechanism
- Hash Key to verify the integrity of the shared photo

3.2.1 Advantages
- Reduced risks related to cybercrimes, frauds and tampering
- More transparent processes with a proper record creation and tracking
- Highly secure due to cryptographic and decentralized Blockchain protocols
- Blockchain supply chain network proof of concept
- Web platform for managers to access Image tracking data
-

IV.RESULT AND DISCUSSION

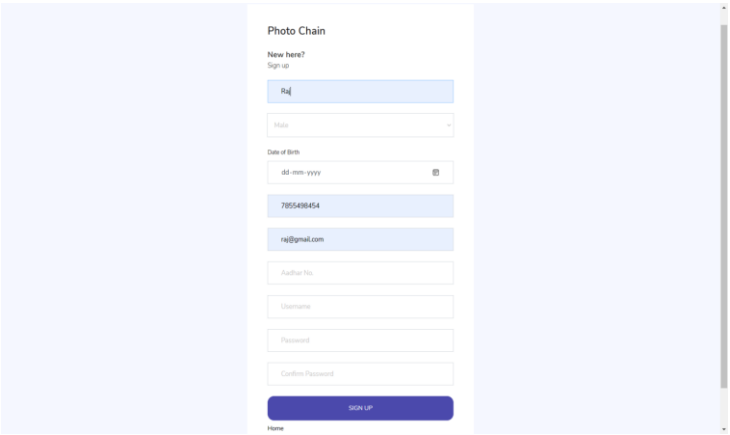

Fig 1. Output

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12569

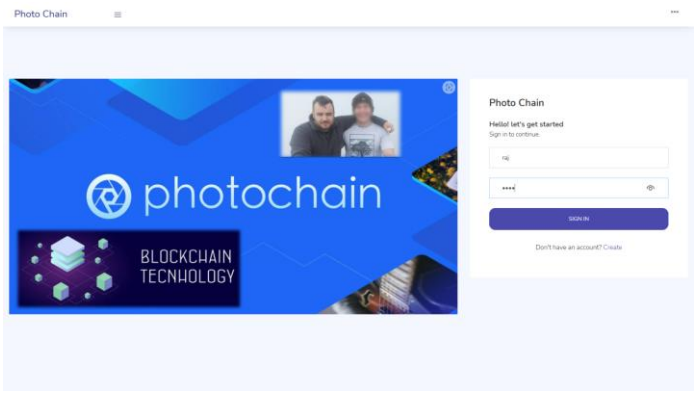

Fig 2. Output

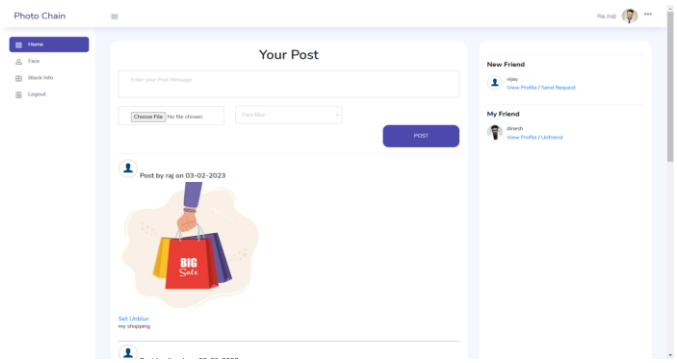

Fig 3. Output

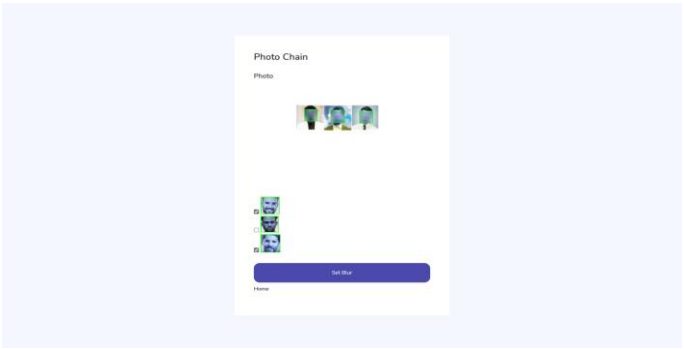

Fig 4. Output

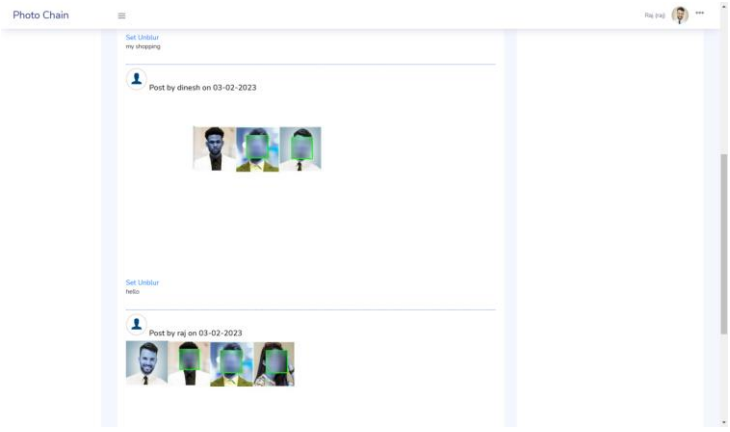

Fig 5. Output

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12569

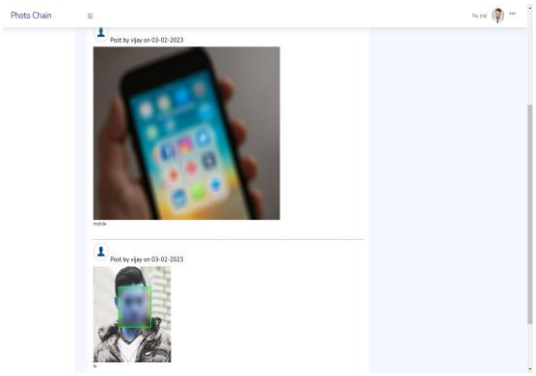

Fig 6. Output

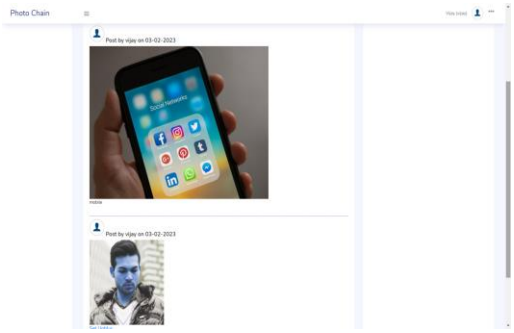

Fig 7. Output

As a research says the simple disclosure of date and place of birth of a pro le in Facebook 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.Combined blockchain, Gaussian Blur 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. The proposed scheme is used to prevent possible privacy leakage of a photo. For this purpose, an efficient facial recognition system is required that can recognize everyone in the photo.

V.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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12569

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, Mu-rat 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. [Online]. Available: https://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=4%2f28%2f2016&id=pr945&ed=12%2f31%2f2016
[7] J. Bort. A High School Coach was Fired for this Facebook Photo. Accessed: Jun. 8, 2019. [Online]. Available: https://www.chron.com/technology/businessinsider/article/A-HighSchool-Coach-Was-Fired-For-This-Facebook-4975389.php
[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. [Online]. Available: https://www.rmit.edu.au/news/all-news/2017/may/not-just-_revengeporn–image-based-abuse-hits-1-in-5-australian
[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.

