ISSN 2063-5346

SECUREFRAME: A SECURE PHOTO SHARING SOLUTION FOR CROSS-SOCIAL NETWORKS USING BLOCKCHAIN FRAMEWORK

M.YOGAPRIYA, DEEPA ABISHEK P.K, JEGADISH.M, DEEPAK.S

Article History: Received: 01.02.2023 Revised: 07.03.2023 Accepted: 10.04.2023

Abstract

The usage of online social networks (OSN) has significantly increased in recent years due to advancements in mobile applications and online interactions. However, sharing and posting photos on social networking services (SNS) often leads to insufficient protection of user photos when distributed on other platforms, posing serious consequences and endangering user safety. While privacy issues have been the main focus of research, there needs to be a balance between privacy protection and effective social networking services, such as data sharing, retrieval, and access. To address this, SecureFrame is a blockchain-infused framework designed to ensure reliable photo sharing among strong distribution controls. It leverages Gaussian mask blurring, PreHash photo integrity checking, and access control algorithms to ensure secure data sharing and fair data retrieval and access without compromising user privacy. The framework's dynamic privacy policy generation algorithm maximizes the flexibility of reposters while protecting the privacy of authors. SecureFrame also provides a mechanism to prevent illegal reprinting by identifying the ownership of photos. Extensive safety experiments and analysis were conducted to prove the productiveness, efficiency, and safety of the given framework i.e., SecureFrame provides a secure photo sharing solution that balances privacy protection and efficient social networking services while ensuring the safety and privacy of users.

Keywords: online social networks (OSNs)-PreHash photo integrity checking-blockchain based framework- social networking services (SNS) -Gaussian mask blurring-data sharing, retrieval, and access control-Distributed Ledger Technology (DLT)-involves converting a photo into blurred version-photo sharing-flexibility and control over their shared content.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Veltech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai

DOI:10.31838/ecb/2023.12.s1-B.324

I INTRODUCTION

The pervasive use of social media has brought about unintentional disclosure of distinctive information by users. While some users may not be concerned about the compromise of their personal information, others take measures to protect themselves from potential attackers and privacy breaches. In recent years, the Internet and web services have grown in popularity, leading to the rise of Social Networking Sites (SNS) that facilitate collaborative information sharing. SNSs have become a global means of communication that allows people to stay connected across borders, and they are now widely used by news agencies, companies, governments, and celebrities. Facebook is the most popular SNS worldwide, and users spend hours sharing info, photos, personal preferences, and information with their friends and family. However, privacy concerns continue to arise in relation to Facebook users, either due to the organization's security policy or users' lack of awareness to the significance of sharing content. For example, a study found that simple disclosure of a user's date and place of birth on Facebook could be used to foretell their social security number (SSN). Posting a friends list can also leak a lot of information, and previously undisclosed private information can be derived using predictive algorithms. Sometimes, sensitive information is embedded in photos as metadata, which can be used to identify the people in the photos, even without explicit tags. These issues are known as collateral damage, as users inadvertently put their own or their friends' privacy at risk when using SNSs like Facebook. The primary goal is to allow each user to treat only their private photo collection as local training data to discover local training results, which can then be exchanged between multiple users to form global knowledge.

II Related works

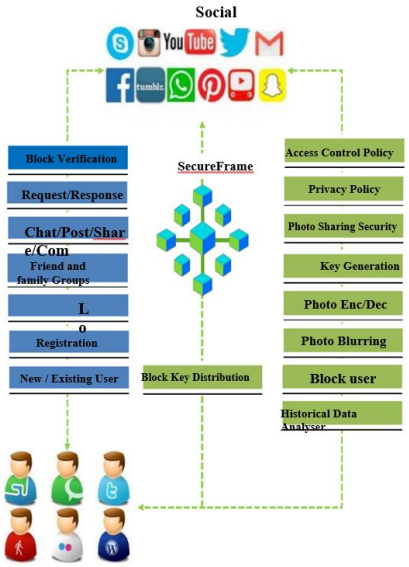
Ghazinour and Ponchak (2017) proposed a graphical user interface (GUI)-based metadata reader and editor to mitigate privacy risks associated with sharing pictures on social media. Their approach aims to enable users to view and edit metadata across various platforms, allowing them to identify and mitigate real privacy risks associated with shared media. By doing so, ordinary users can be better protected from potential privacy breaches.

Regin and Sneha (2022) proposed an adaptive hidden policy indicator mechanism to facilitate photo sharing on social media platforms. Their approach involves providing clients with policies while sharing images with multiple recipients, which helps customers to share images based on trust in the recipient. This mechanism can help users make informed decisions about photo sharing and ensure that their privacy is protected.

Abhang and Rathod (2017) proposed a mechanism to raise awareness among users about photo sharing and involve them in the decision-making process. Their approach involved the use of a facial recognition system (FR) that would be used by all individuals in the photo. This would allow for greater control over who sees the photo and enable users to make more informed decisions about photo sharing.

Maragatham and Yuvarani (2020) addressed privacy concerns related to photo sharing on online social networks. Their approach involves using an editor to predict the potential loss of privacy for each associated user when a photo is shared with a certain user. Unlike previous work, posters do not need to communicate with other users before posting photos. The mechanism checks the trust between users to measure the potential loss of privacy. This approach can help posters make more informed decisions about photo sharing and protect their privacy.

Xu and Bao (2018) proposed a technique for privacy-preserving photo sharing in online social networks using image processing. They suggested a model where photos are converted into multiple layers, each containing an ambiguous face, and the final photo presented to the viewer is generated by overlaying certain layers based on the user's privacy policy. A similar approach was presented by Lee et al. (2014), where they proposed a multi-party access model for photo sharing in OSNs. The granularity of access control can be adjusted incrementally from photo level to face level in their model. These techniques demonstrate the possibility of managing privacy concerns in photo sharing effectively.



Full detailed block diagram of photo chain

Amon and Hasan (2019) investigated the factors influencing photo sharing decisions on social media. They found that privacy-preserving sharing platforms, such as I-Pic and COIN, can allow users to post their privacy preferences, which can be respected by nearby photographers. The study also examined the frequency of photo sharing by participants and how it relates to their privacy concerns. Overall, the findings suggest that users are more likely to share photos when they feel their privacy preferences are respected.

III Methodology

SecureFrame is a secure photo sharing framework that utilizes blockchain technology and several algorithms to provide effective Regulating the spread of photos shared across various social networks. The framework includes techniques such as Gaussian Blur for photos, which masks faces, and the Pre-Hash algorithm, which verifies photo integrity and controls access. These mechanisms ensure secure data sharing, retrieval, and access control without compromising users' interests.

Blockchain is a decentralized digital ledger system, where transactions are recorded in blocks, and each block contains several transactions. The ledger is replicated and distributed across the network of computers on the blockchain. This technology is a type of Distributed Ledger Technology (DLT), which is managed by multiple participants. In a blockchain, each transaction is recorded with a cryptographic signature known as a hash, which makes the record immutable. This means that if any block in the chain is altered, it will be immediately detected, and the system will indicate that it has been tampered with. To hack a blockchain system, attackers would need to modify every block in the chain across all distributed versions of the chain.

IV Proposed System

Our system uses Machine Learning methods, specifically the K-Neighbours Classifier algorithm, to detect co-owner faces in shared data and tag them to the co-owner's accounts. This allows for permission to be obtained from the co-owners before the data is shared, ensuring that personal information is not leaked and that users' privacy is protected. Social-

networking consumers may not always must be prepared to their personal information could be revealed, which could lead to significant privacy breaches. To address this issue, we also propose SecureFrame, a secure photo sharing framework based on blockchain technology. SecureFrame uses Gaussian Blur technology for Face Masking, Pre-Hash Algorithm for Photo authenticity verification, and methods of Access Controls to achieve reliable photo sharing, data retrieval, and data access. our Privacy Preserving Framework and SecureFrame provide powerful tools for secure data sharing in social networks, while protecting users' personal information and privacy. By using advanced Machine Learning and blockchain technology. We have developed a system that guarantees the security, fairness, and protection of users' interests when it comes to data sharing, retrieval, and access..

V Results and future scope

Our team has developed and tested a comprehensive blockchain-based framework, called SecureFrame, that facilitates secure photo sharing on various social networks while preserving user privacy. SecureFrame enables users to control the distribution of their uploaded photos to ensure that they are only accessible to authorized parties. It also binds photo access control policies without interfering with the display process, providing users with more flexibility and control over their shared content. To enhance our scheme, we plan to incorporate additional security levels for various user groups and consider more user-related attributes to offer more precise access control. Additionally, we aim to investigate the potential of emerging technologies, such as federated learning, to protect user privacy in CrossSNs.

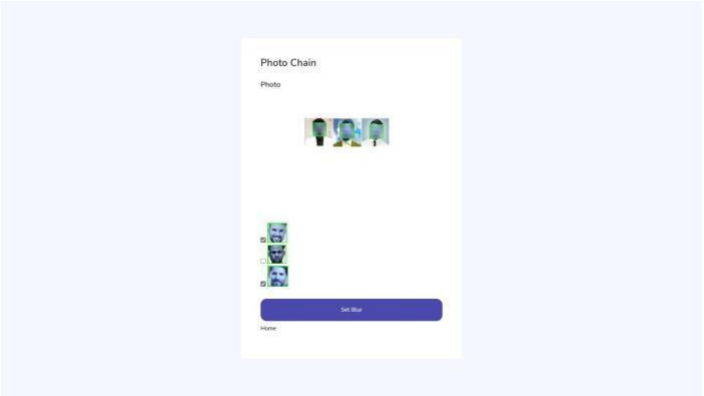


Fig1. Only the followers who have been accepted can see the proper image

Our photo sharing approach involves a multiparty access model in OSNs, where the final photo for viewers is created by overlaying specific layers that are generated based on each user's privacy policy. The access control granularity can be adjusted in a precise manner, ranging from the photo level to the face level.

Fig2. If someone wants to view the image, they need to send request

We have developed a system that guarantees the security, fairness, and protection of users' interests when it comes to data sharing, retrieval, and access.

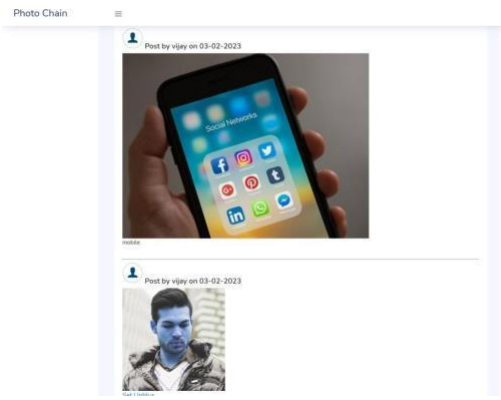


Fig4. The image viewed by the followers

Our approach ensures secure data sharing, retrieval, and access control, protecting users' interests and preventing potential privacy breaches that may occur with photo sharing.

VI Conclusion

SecureFrame is a framework that can assist social network users in safeguarding their privacy by hiding their private data from unwanted audiences, even on different social networks. This framework ensures that shared photos are protected and cannot be accessed by unauthorized users, while also allowing users to conceal their searches for images, thus preventing content from being shared without their knowledge. Furthermore, SecureFrame reduces system overhead while preserving user privacy. Results from evaluations demonstrate the effectiveness of the framework. The proposed scheme guarantees confidentiality, integrity, and privacy by disrupting information sharing between legitimate users and preventing unauthorized users from accessing private information.