International Scientific Journal of Engineering and Management
Volume: 02 Issue: 04 | April – 2023 DOI:
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
www.isjem.com

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

Guru Prakash G, Prabhakaran P, Sanjay M, Santhosh M, Mrs.Vanitha (AP/CSE)

CSE & Selvam College of technology

Abstract

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.

Key Words; Photo sharing, privacy-preserving, cross-SNP, Blockchain

1. INTRODUCTION

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 protect the Malicious attackers and may perpetrate significant privacy breaches. The rest decade of 21stcentury 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 fields as news agencies, big and small companies, governments, and famous personalities etc. to interact with each other. With the adoration of sharing, Face book 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.

Online diversion has become steadily planned into a many people's everyday schedules. Billions of people all around the planet use virtual diversion to share information and make affiliations. On a singular level, virtual amusement grants you to talk with friends and family learn new things, encourage your tendencies, and belocked in. Privacy-preserving social media data-sharing scheme by introducing the authorization mechanism and attribute-based encryption (ABE) based on block chain. Automatically encrypts the detected private information leveraging attribute- based

encryption (ABE), so that legitimate users can recover the private information with their attributes.

2. Related Work

Data privacy has increasing becoming an issue that researchers try to build models and methods to protect. In 8 Barker et al. introduce data privacy taxonomy to introduce a guideline to assess privacy-awareness of different models. In 9, 10 the researchers propose a recommender system that helps the users to pick a better privacy setting in their social network. In 11, 12 the researchers facilitate understanding of ambiguous and long privacy policies to the users in an easy-to-understand format. There are even attempts to introduce access control models to dynamically

Reflect security policies 14

As previously mentioned, metadata is a form of data that is included on all videos and pictures and is used to store information about that data, such as date photo was taken, photographic information and GPS coordinates. This information is often used by operating systems to save information such as the last date a document was edited. This information is occasionally very helpful to person sharing the photos. In a court case1 in 2012, a freelance photographer was cleared of charges of interfering with the arrest of another citizen by "aggressively" blinding the police officer with flash from his camera. The free-lance photographer was cleared of this charge by viewing the metadata which show that his flash did not fire at all during the time he was taking pictures. The police officer was later charged with fabricating an arrest record1.

3. Methodology:

PhotoChain 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, 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.

4 .PROBLEM STATEMENT AND HYPOTHESIS

4.1 Privacy policy and exposure policy

In this paper, we assume that each user i has a privacy policy Pi(x) and a exposure policy Vi(x) for a specific photo x. The privacy policy Pi(x) indicates the set of users who can access photo x and exposure policy Vi(x) indicates the set of users who can access x when user is involved. After people on co-photo x are recognized with our algorithm as a set I, the set of users who follow both the privacy policy and exposure policy could be calculated by:

$S = Pi(x)\backslash k \in IVk(x)$ (1)

We assume that our users have defined their privacy Policy and exposure policy and these policies are mod-If able. The exposure policy is treated as a private data That shall not be revealed, and a secure set intersection Protocol [11] is used to find the access policy S in 1.

4.2 FR with social contexts

An FR engine for a large-scale social network may require discriminating millions of individuals. It seems to be a daunting task that could never be accomplished .However, when we decompose it into several personal FR engines, the situation will change for better. Social contexts contain a large amount of useful information which could be utilized as a priori knowledge to help the facial recognition [19]. In [12], Mavridis, Kazmiand Tousles develop a three-realm model to study facial.

4.3 FR system

We assume that user i has a photo set of size Ni of Himself/herself as his/her private training samples (say, stored on his/her own device such as smart phone). From the private photo set, a user detects and extracts the faces on each photo with the standard face detection

ISSN: 2583-6129
www.isjem.com

Method [23]. For each face, a vector of size p is extractedas the feature vector. Then, for user i, his/her private training set could be written as xi of size Ni × p. In the rest of this paper, we use one record and one photo inter changeably to refer one row in xi With the private training set, each user will have a personal FR engine to identify his/her one-hop neighbors. The personal FR can be constructed as a multi-class classification system, where each class is corresponding to one user (himself/herself or one friend). In the rest of this paper, we use one class interchangeably with the appearance of one user. In the realm of machine learning, usually a multi-class classification system is constructed by combining several binary classifiers together with the one of the following strategies[7]:

One-against-all method uses winner-

Take- all strategy. It constructs n binary classifiers for each of n classes. The goal of each binary classifier is to distinguish one class from the rest with a decision function. Hence, the decision function is trained by taking records from user i as positive samples and the records from all the other users as the negative samples. When a testing record x comes, if fi concludes that it belongs to class i, x is labeled as class i.

One-against-one method uses max-voting

Win strategy. It constructs n(n − 1)/2 binary classifiers, in which each classifier is aimed to distinguish two classes. The idea is that if we can distinguish any two classes, then we can identify any of them. Hence, classifier u ij is constructed by taking records from i as positive samples and records from j as Negative ones. Later on when we are trying to identify a test record x, if u ij concludes that x is in class i, then the vote of class i is added by one. After testing all the n(n − 1)/2 classifiers, x is assigned to the class with the largest voting value.

5. Modules Description

5.1 SN Web App

Construct a long range informal communication administration is a web-based stage in which individuals use to fabricate informal organizations or social associations with others who share comparable individual or vocation interests, exercises, foundations or genuine associations. Person to person communication administrations change in design and the quantity of elements. Clients in this application, who need to access and share their pictures into this site, they ought to enroll their data here.

5.2 Share/Post/Comment/Chat

In which, clients can give companion demands, acknowledge companion demands, and key solicitation to uncover private pictures in the site .Sharing Photograph Client can share a photograph just to companions on list. As per the proposed plot ,this companion rundown ought to be crossing point of proprietor's protection strategy and co- proprietors 'openness policies. Friend Solicitation A sign in/out button could be utilized for sign in/out with the social site. Subsequent to signing in, a hello message and the profile picture will be shown. This model works in three modes: an arrangement mode, a resting mode and a Functioning mode. To answer a companion demand, you have two options. One is to click one of the two buttons to one side of your expected companion's name.

5.3 Photo Privacy

In this cycle, security data of the photograph is Safe guarded by utilizing the chose insurance device and a mystery key (or a bunch of keys) set by the Shipper. Aside from giving a legitimate security level and a productive execution, one important testis to appropriately deal with all the encryption keys utilized in the framework. We propose a concentrated methodology where all keys are put a way in the believed Key Server. The works of built the encoder network like the design of U-Net, and its outcomes have

demonstrated that the skip association is compelling to decrease the bending of steganographic pictures and work on the visual nature of steganographic images. Gaussian obscure (otherwise called Gaussian smoothing) is the consequence of obscuring a picture by a Gaussian capability (named after mathematician and researcher Carl Friedrich Gauss).

5.4 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.

5.5 Photo Verification Module

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.

Conclusion

In this project, we designed, implemented and evaluated an extended control framework for blockchian enabled privacy-preserving photo sharing across different social networks, called Photo Chain .It helps social networking users to preserve their privacy requirements assigned on their uploaded photos, by control the operations of the following users on a dissemination chain. Meanwhile, it binds the access control polices to photos without disturbing the display phase. As a result, Photo Chain could help social networking users to hide privacy areas away from unwanted viewers even in different social networks. Photo chain not only protects the shared photos so that no unauthorized users can access them, but also enables users to blur their image search so that the search can also be shared to a cross social networking site obliviously without leakage on the query contents or results. The concept of PhotoChain which provides confidentiality, Integrity and privacy. In the future, we intend to explore the role of the latest technologies, such as federated learning, in preserving users' privacy in Cross SNs.

Reference

[1] AnielloCastiglione∗,Bonaventura D'Alessio†"S steganographic and Secure Communication on Online Social Networks and Online Photo Sharing" University degli Studi di SalernoI-84084 Fisciano (SA).

[2] LIHONG TANG1,2 "Faces are protected as Privacy: An Automatic Tagging Framework against Unpermitted Photo Sharing in Social Media"DigitalObjectIdentifier10.1109/ACCESS.2019.2921029 date of current, version date of current version June 21, 2019.

[3] Fenghua Li_y, Zhe Sun An Extended Control Framework for Privacy-Preserving Photo Sharing Across Different Social Networks 2019 International Conference on Computing.

[4]Edwin Yang, Song Fang Poster: Photo Lock: Autonomous Privacy-preserving Photo Sharing in Online Social Networks University of Oklahoma.

[5] Kaihe Xu, My Privacy My Decision: Control of Photo Sharing on Online Social Networks IEEE Transactions on Dependable and Secure Computing

[6]P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-based distributed support vector machines. J. Mach. Learn. Res., 99:1663– 1707, August 2010.

[7] J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on

ISSN: 2583-6129
www.isjem.com

online social networks. Multimedia, IEEE Transactions on, 13(1):14–28,2011.

[8] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J.Eckstein. Distributed optimization and statistic all earning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan.2011.

[9] Ferreira, B., Rodrigues, J., Leitao, J.,Domingos, H.: Privacy-preserving content-based image retrieval in the cloud. In: Proc. of IEEE SRDS 2015

[10] Fogues, R.L., Murukannaiah, P.K., Such, J.M., Singh, M.P.: Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making.ACM Transactions on Computer- Human Interaction 24(1), 5 (2017)[11] He, J., Liu, B., Bao, X., Jin, H., Kesidis, G.: On privacy preserving partial image sharing. In: Proc. of IEEE ICDCS 2015

[12] He, J., Liu, B., Kong, D., Bao, X., Wang, N.,Jin, H., Kesidis, G.: Puppies: Transformation-supported personalized privacy preserving partial image sharing. In: Proc. of IEEE/IFIP DSN 2016

[13]Hu, H., Ahn, G.J., Jorgensen, J.: Multiparty Access control for online social networks: model And mechanisms. IEEE Transactions on Knowledge and Data Engineering 25(7), 1614–1627 (2013)

[14] Ilia, P., Polakis, I., Athanasopoulos, E., Maggi, F., Ioannidis, S.: Face/off: Preventing privacy leakage from photos in social networks. In: Proc. Of ACM CCS 2015

[15] R. Trenholm. Most Facebook Photos are Taken While We're Drunk, Survey Says. Accessed:Jun. 8, 2019.[Online].Available:https://www.cnet.com/news/most-facebook photos-are-taken-whilewere- drunk-survey-says/

[16] 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/press releases detail.aspx?sd=4%2f28%2f2016&id=pr945&ed=12%2f31%2f2016

[17] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, ``My privacy my decision: Control of photo sharing on online social networks," IEEE Trans. Dependable Secure Comput., vol. 14, no. 2, pp.199_210, Apr. 2017.

[18]Camera & Imaging Products Association, Standardization Committee, “Exchangeable image file format for digital still cameras: Exif Version2.3,”http://www.cipa.jp/english/hyoujunka/kikaku/pdf/DC-008-2010_E. pdf, 26 April 2010.

.

.