International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

SecureShare: Trust-Based Photo Privacy

Dr. M. Raju
Associate Professor
Department of Computer Science and Engineering
Nalla Malla Reddy Engineering College
Narapally, Divyanagar, Hyderabad
raju.cse@nmrec.edu.in

Sushmitha, Rishi, Sai Prasad, Revanth
B.Tech Final Year
Department of Computer Science and Engineering
Narapally,Divyanagar,Hyderabad
19B61A0550@nmrec.edu.in

Abstract- With the development of social media technologies, sharing photos in online social networks has now become a popular way for users to maintain social connections with others. However, 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. When sharing a photo that involves multiple users, the publisher of the photo should take into all related users' privacy into account. In this paper, we 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. And the user's trust in the publisher is affected by the privacy loss. The anonymization result of a photo is controlled by a threshold specified by the publisher. We propose a greedy method for the publisher to tune the threshold, in the purpose of balancing between the privacy preserved by anonymization and the information shared with others. Simulation results demonstrate that the trust-based photo sharing mechanism is helpful to reduce the privacy loss, and the proposed threshold tuning method can bring a good payoff to the user.

Index Terms – Security, Machine Learning, Facial Recognition, Privacy, Access control

I. INTRODUCTION

Social media has become an integral part of our daily lives, allowing individuals to connect with one another by sharing and creating content. User-generated content, such as text posts, photos, and videos, is the backbone of social media platforms. However, this content often contains sensitive information that can compromise the privacy of the creator. As a result, privacy concerns related to information sharing have been a prevalent topic in social media research. Digital photo sharing is a significant form of content sharing on social media sites.

II. LITERATURE SURVEY

The rise of social media on the internet has had a significant impact on the way individuals communicate with each other about products and companies. Consumer-to-consumer communication has been greatly amplified, and this article argues that social media is a hybrid element of the promotion mix. It enables companies to communicate with customers in a traditional sense, but also allows customers to communicate directly with one another in a non-traditional sense. The content, timing, and frequency of these conversations are beyond the control of managers, unlike in the traditional integrated marketing communications paradigm. Thus, managers must learn to shape these conversations in a way that aligns with the organization's mission and performance goals. Methods for achieving this include providing networking platforms for consumers and engaging customers through blogs, social media tools, and promotional tools. Many business executives today are focused on making profitable use of social media applications such as Wikipedia, YouTube, Facebook, Second Life, and Twitter. This article presents ten pieces of advice for companies that decide to use social media. This special issue of "Telecommunications Policy" titled "The Governance of Social Media" begins with a definition of social media that informs all contributions in the issue. It also describes the challenges associated with the governance of social media and provides an overview of the articles included in the issue. While social interaction on the internet has always been prevalent, the emergence and rapid diffusion of Web 2.0 functionalities during the first decade of the new millennium enabled a leap forward in the social component of web use. Social media services are currently internet-based applications that utilize Web 2.0 technologies.

2.1 PLATFORM OVERVIEW

A photo-sharing platform known as Trust-based photo sharing has been developed to enable users to share their photos exclusively with a chosen group of people whom they trust. The platform aims to increase the privacy and security of photo sharing by guaranteeing that only the intended recipients can access the shared photos. Trust-based photo sharing operates on the fundamental principle of trust, which restricts users to share photos only with people they trust. Users can establish a trusted network by adding friends, family members, or colleagues to their trusted group and share their photos with this group exclusively. By doing so, users can ensure that their photos are not shared with individuals who are not trusted or strangers.

2.2 FUNDAMENTALS

Trust-based photo sharing emphasizes the importance of trust, which is the foundation of the platform. The platform enables users to share their personal photos only with people they trust, including family members, friends, or colleagues. This creates a secure and safe environment for sharing personal photos. Privacy is also a crucial aspect of trust-based photo sharing, and users have complete control over who can view their photos. This ensures that only trusted individuals can access the photos and that they are not shared with strangers or unauthorized individuals. Security is a critical consideration in trust-based photo sharing. The platform should have robust security measures, such as end-to-end encryption and two-factor authentication, to ensure that photos are protected and cannot be accessed by unauthorized individuals. Users should also have complete control over their photos and how they are shared. The platform should offer features that allow users to set expiration dates, revoke access to photos, and manage their privacy settings.

In summary, trust-based photo sharing is a platform designed to create a safe and secure environment for sharing personal photos. The platform emphasizes trust, privacy, and security, and provides users with complete control over their photos and how they are shared. By implementing robust security measures and offering a range of privacy and sharing options, trust-based photo sharing enables users to share their personal photos with confidence and peace of mind.

2.3 DEVELOPMENT

End-to-end encryption is a type of security measure that is used in trust-based photo sharing platforms to protect the privacy and security of photos. When photos are transmitted through the platform, they are encrypted so that they can only be decrypted by the intended recipient. This makes it more difficult for unauthorized users or hackers to access the photos. The encryption process is done at the user's device before the photos are transmitted to the platform, and the decryption process is done on the recipient's device. This ensures that the photos are protected throughout the entire transmission process. Two-factor authentication is another security measure that can be used in trust-based photo sharing platforms. With two-factor authentication, users are required to provide a second form of authentication in addition to their password. This could be a code that is sent to their phone or a fingerprint scan. By requiring two forms of authentication, the platform adds an extra layer of security to ensure that only authorized users have access to the photos. Some platforms also use machine learning to detect and prevent unauthorized sharing of photos. Machine learning technology can analyze patterns and identify potential security risks. For example, if a user suddenly starts sharing photos with a large number of new contacts, the platform may flag this as a potential security risk and ask the user to verify their identity or limit access to the photos. By using machine learning to detect potential security risks, trust-based photo sharing platforms can proactively prevent unauthorized sharing and protect the privacy and security of their users.

2.4 APPLICATION

A web application, commonly referred to as a web app, is a type of software application that is accessed using a web browser through an active network connection. Unlike traditional applications that are installed and run on a computer's operating system, web applications are accessed through the World Wide Web. These applications can react to user input and dynamically change, much like applications created using programming languages such as C or C++. Essentially, a web app is a program that runs on a web server and is delivered to users through a browser interface. This allows for greater flexibility in terms of accessibility, as users can access the application from any device with an internet connection and a web browser.

III. EXISTING SYSTEM

The sharing of multimedia content has gained immense popularity in online social networks due to its visual appeal. However, the widespread and quick dissemination of multimedia content can pose a severe threat to an individual's privacy if the content contains sensitive information. In the case of photo sharing, all the users associated with the photo become vulnerable to privacy breaches. This has prompted researchers to delve deeper into privacy issues associated with multimedia content sharing. Currently, there is no effective mechanism to balance photo sharing and privacy preservation in online social networks. Thus, it is

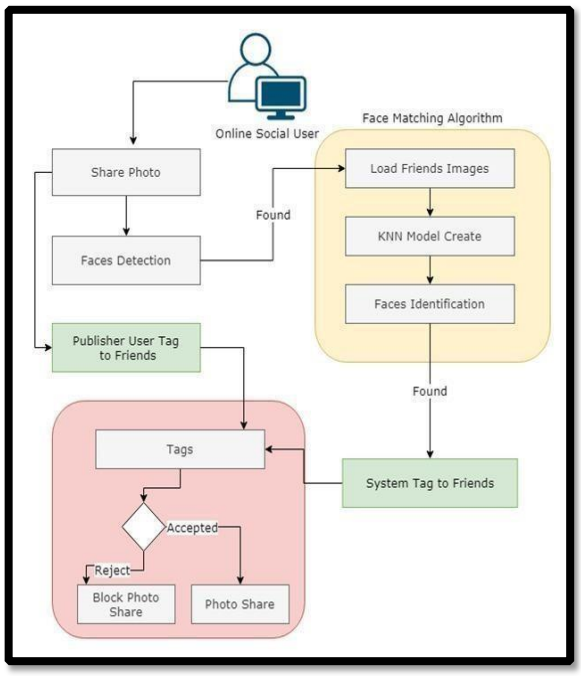
imperative to explore ways to control photo sharing and safeguard user privacy in such networks.

3.1 LIMITATIONS

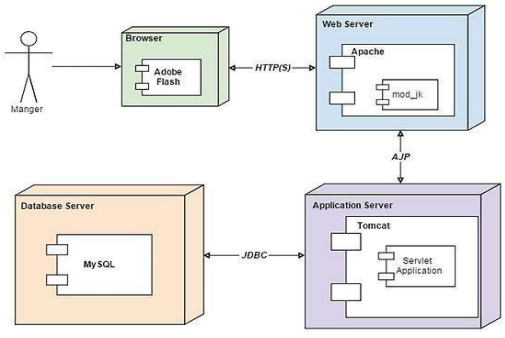
Trust-based photo sharing platforms have a key feature of limiting the number of individuals that users can share their photos with, ensuring that photos are shared only with trusted individuals. However, technical limitations may exist that restrict the size or quality of the photos that can be shared. Additionally, there is always a risk of data loss when using any online platform, including trust-based photo sharing platforms, so users should take measures to back up their photos. While these platforms are designed to enhance privacy and security, there is always a risk of privacy breaches, and users should take steps to ensure that their photos remain secure. Some trust-based photo sharing platforms may charge a fee for their services, which may be a limitation for some users. Furthermore, these platforms rely on internet connectivity, so users may not be able to access their photos if they do not have an internet connection.

IV.ARCHITECTURE

System architecture refers to the design and organization of the technology infrastructure of an enterprise, solution, or system. In the case of a web application, the system architecture outlines the flow of the application and the interactions between different stakeholders, such as the user and the tagged user. This flow can be represented in a diagrammatic format to better understand the structure and behavior of the system. The diagram provides a visual representation of the application's components and their interactions, making it easier to identify potential areas of improvement or issues.



The current application is being built using the 3-tier architecture as a blueprint. This model follows a client-server architecture where the web browser serves as the client, IIS (Internet Information Services) manages the appointment requests and visitor status checks, and a separate tier for SQL server handles database functions such as storing and viewing user and tagged user details. The 3-tier approach offers benefits such as increased scalability and separation of business logic from display and database layers. By dividing the application into three separate layers, each layer can be developed and maintained independently, making it easier to scale and maintain the application. Additionally, this approach allows for better security and reduces the risk of data loss. However, there are also challenges to implementing a 3-tier architecture, such as increased complexity and a higher initial cost.



TECHNICAL ARCHITECTURE

V.RESULT ANALYSIS

Trust-based photo sharing is a secure and privacy-focused way for users to share their personal photos with others. With trust-based photo sharing platforms, users have complete control over who can access their photos, thus protecting their privacy. These platforms employ advanced security measures, including encryption and two-factor authentication, to ensure that photos remain secure and cannot be accessed by unauthorized parties. The user experience is a top priority for trust-based photo sharing platforms, and they are designed to be user-friendly and easy to navigate. By ensuring that users feel comfortable sharing their photos, trust-based photo sharing can help build trust between individuals and within communities. One of the key benefits of trust-based photo sharing is that it can significantly reduce the risk of unauthorized sharing. With these platforms, users can rest assured that their photos are protected and that only authorized individuals can access them. This can help prevent privacy breaches and other security issues, providing users with peace of mind when sharing their personal photos. In summary, trust-based photo sharing is a secure and user-friendly way for individuals to share their personal photos with others. By providing advanced security measures and allowing users to control who can access their photos, trust-based photo sharing can help build trust within communities and reduce the risk of unauthorized sharing, thus protecting users' privacy and security.

VI. CONCLUSION

In social media platforms where photos can be co-owned by multiple users, sharing a single photo may pose a risk to the privacy of all the users involved. To address this privacy concern, a new privacy-preserving photo sharing mechanism has been proposed in a research paper. This mechanism makes use of trust values to determine how a photo should be anonymized. The level of trust between the users involved is taken into account to ensure that the privacy of all stakeholders is protected. By employing a trust-based approach, the publisher is encouraged to prioritize the protection of the privacy of all users involved in the co-owned photo. This helps to mitigate the risk of privacy breaches and other security issues that may arise from the sharing of sensitive photos. In summary, the proposed privacy-preserving photo-sharing mechanism utilizes trust values to determine the best approach to anonymizing co-owned photos. By promoting trust and encouraging the protection of stakeholders' privacy, this approach provides a more secure and privacy-focused way to share photos in social media platforms.

VII.REFERENCES

1. W. G. Mangold and D. J. Faulds, “Social media: The new hybrid element of the promotion mix,” Business horizons, vol. 52, no. 4, pp. 357–365, 2009.
2. M.Kaplan and M.Haenlein, “Users of the world, unite! the challenges and opportunities of socialmedia,”Businesshorizons,vol.53, no. 1, pp. 59–68, 2010.
3. J. A. Obar and S. S. Wildman, “Social media definition and the governance challenge-an introduction to the special issue,” 2015.
4. L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, “Information security in big data: Privacy and data mining,” IEEE Access, vol. 2, pp. 1149–1176, 2014.
5. S.K N, S.K, and D.K, “On privacy and security in social media a comprehensive study,” Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st International Conference on Information Security and Privacy 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211
6. J. M. Such and N. Criado, “Resolving multi-party privacy conflicts in social media,” IEEETransactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016