TRUST BASED PRIVACY PRESERVING PHOTO SHARING IN ONLINE SOCIAL NETWORKS

V. Sarala madam [1], Ch. Mahalakshmi,

[1]**Assistant professor , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - vedalasarala21@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - chmahalakshmi62@gmail.com

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.

1 INTRODUCTION

Social media [1], which enable people to interact with each other by creating and sharing information, has now become an importation part of our daily life. Users of social media services create a huge amount of information in forms of text posts, digital photos or videos. Such user-generated content is the lifeblood of social media [2], [3]. However, user-generated content usually involves the creator's sensitive information, which means the sharing of such content may compromise the creator's privacy. How to deal with the privacy issues caused by information sharing is a long active topic in the study of social media [4], [5]. A major form of the content

sharing activities in social media websites is the sharing of digital photos. Some popular online social networking services, such as Instagram1, Flicker2, and Pinterest3, are mainly designed for photo sharing. Compared to textual data, photos can deliver more detailed information to the viewer, which is detrimental to individual's privacy. Moreover, the background information contains in a photo may be utilized by a malicious viewer to infer one's sensitive information. On the good side, it is more convenient for a user to hide his sensitive information, without too much damage to insensitive information, by image processing (e.g. blurring) than by text editing. In this paper we study the privacy issue raised by photo sharing in online social networks (OSNs). Privacy policies in current OSNs are mainly about how a user's information will be explored by the service provider, and through which methods a user can control the scope of information sharing. Most OSNs offer a privacy setting function to their users [6]. A user can specify, usually based on his relationships with others, which users are allowed to access the photo he shares.

Literature Survey

A literature survey on "trust-based privacy-preserving photo sharing in online social networks" would typically explore various research papers, articles, and studies that focus on methods and frameworks for ensuring user privacy while sharing photos in online social networks, particularly through mechanisms based on trust. Here's an outline of what such a survey might cover:

1. Introduction to Privacy Concerns in Online Social Networks:

- Overview of the growing popularity of online social networks (OSNs)
- Importance of privacy in photo sharing due to sensitive nature of personal images
- Challenges posed by current OSN platforms in maintaining user privacy

2. Trust-Based Approaches to Privacy Preservation:

- Definition and significance of trust in the context of privacy preservation
- How trust mechanisms can enhance user control over shared content
- Types of trust models used in OSNs (e.g., direct trust, recommender systems)

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

In [12], Yuan et al. proposed a privacy-preserving photo sharing framework which uses visual obfuscation technique to protect users' privacy. When processing a photo, the proposed framework considers both the content and the context of a photo. In [13], Xu et al. designed a mechanism that enables all the related users of a photo participate in the decision-making process of photo sharing. With the help of a facial recognition technique, they developed a distributed consensus-based method to generate the final decision. Based on the encryption algorithm proposed in [14], Ma et al. proposed a key management scheme to authorize and repeal a user's privilege of

accessing multimedia data [15].

Disadvantages:

- There is no threshold-based access control on Photo Sharing in online social network.
- Less security due to no fine-grained privacy management of photo sharing

Proposed System & alogirtham

In the proposed, the system considers a photo-sharing scenario where the user who publishes the photo, referred to as publisher, decides how to process the photo so as to protect privacy of related users. A trust-based mechanism is proposed to help the publisher make a proper decision. Different from our previous work [10], 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.

4.1 Advantages:

- More Security due to Trust-based Photo Anonymization and Trust-based Privacy-Preserving Approaches.
- A threshold is introduced to control the number of users deleted from a photo. To find a balance between privacy preserving and photo sharing, the system proposes a method to make the threshold adaptive to the trust relationship between users

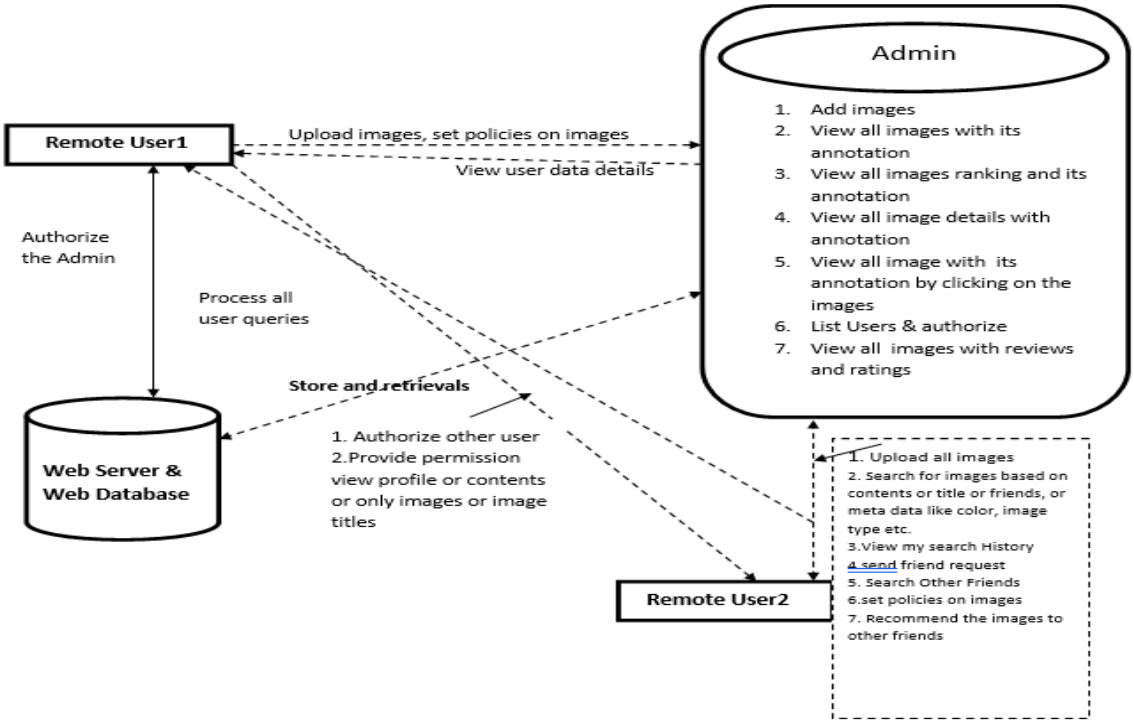


Fig:3.1 System Architecture

IMPLEMENTATION

ORGANIZATION OF PROJECT

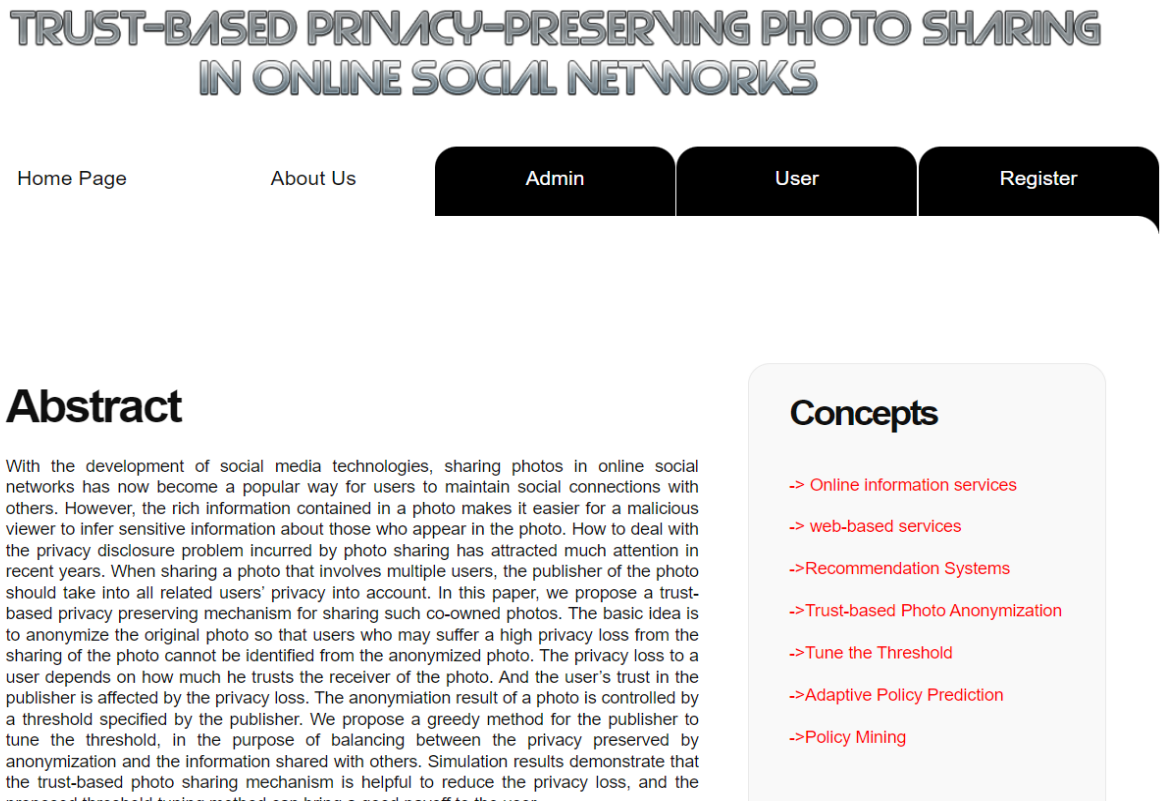
An Adaptive Privacy Policy Prediction (A3P) is projected in this place project that equipment consumers a question free solitude backgrounds knowledge by create embodied tactics without thinking. The A3P plan checkout consumer-uploaded representations and determinants that influence one's solitude scenes of concepts: The impact of public atmosphere and private traits. Social circumstances of consumers support the description news and friendships accompanying possible choice, and support additional facts had connection with solitude options. However, utilizing coarse tactics across all consumers or consumers accompanying complementary characteristics manage to be excessively simple and not placate individual options. Users grant permission has intensely various beliefs even on an equivalent in a way figure.

A3P Algorithm Steps:

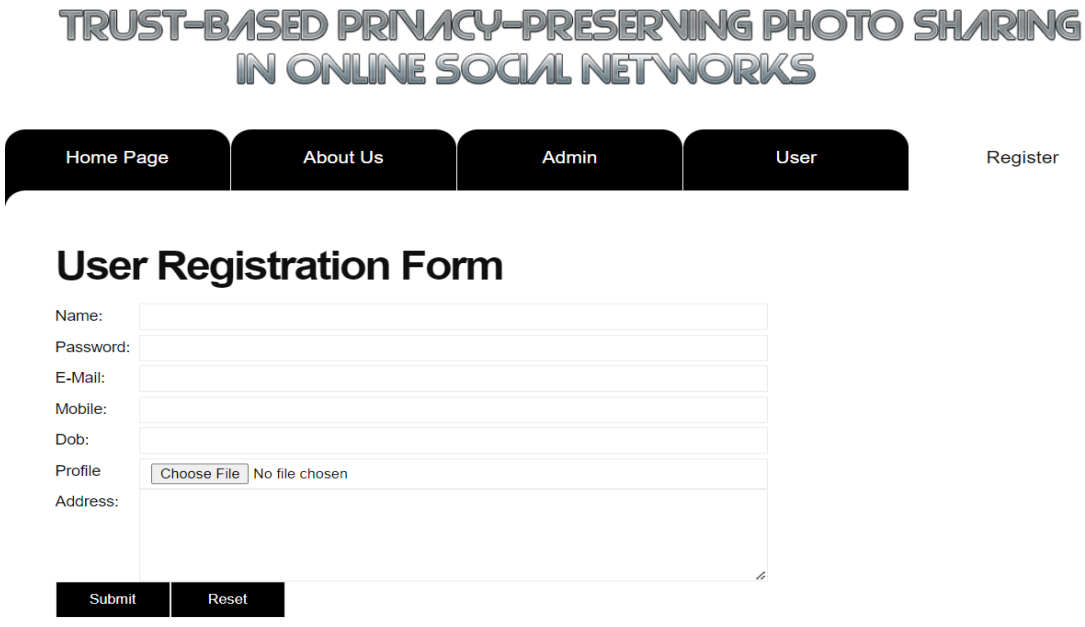
1. when user uploads an image I, it sends to A3P core
2. if A3P core classifies image
3. then it predicts policies P to the user
4. end of if
5. else if A3P social is called
6. then it identifies social group to the user
7. end of if
8. predicted policy P is displayed to the user
9. if user satisfied by the policy
10. then it will be accepted A
11. end of if.

5 RESULTS AND DISCUSSION

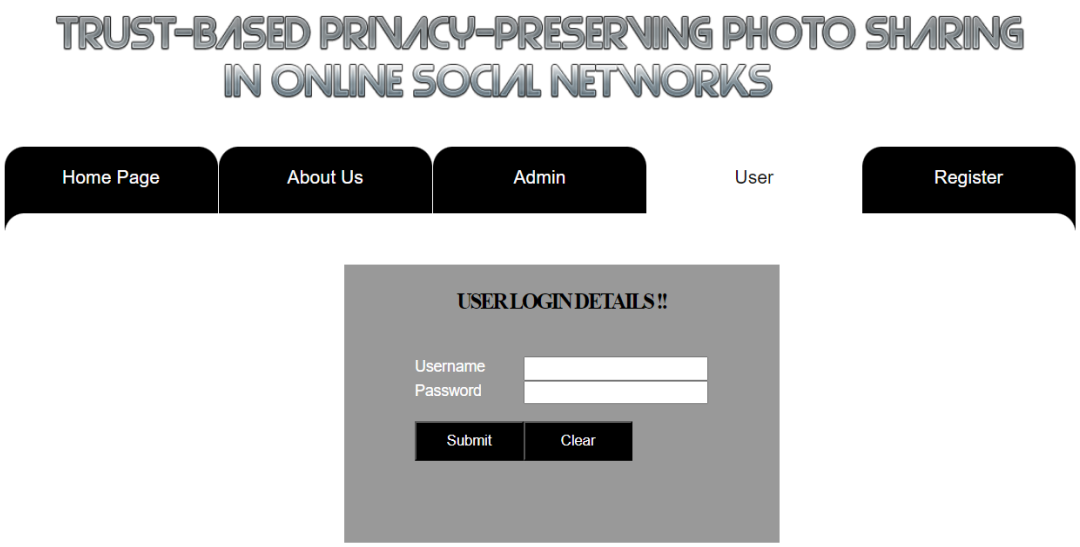
HOME PAGE:



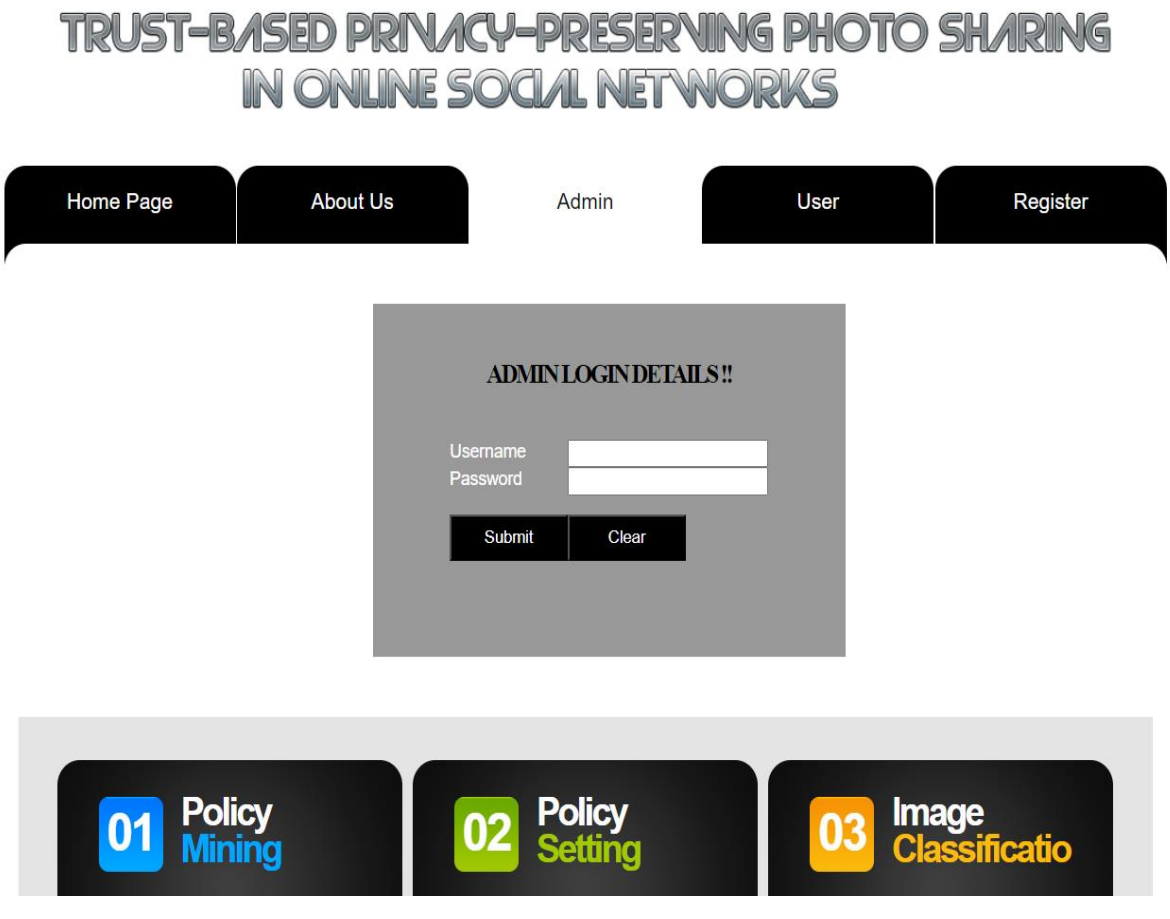
USER REGISTRATION FORM:



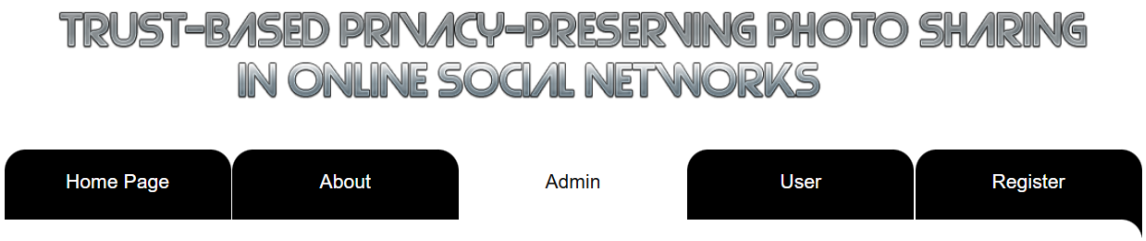
USER LOGIN DETAILS:

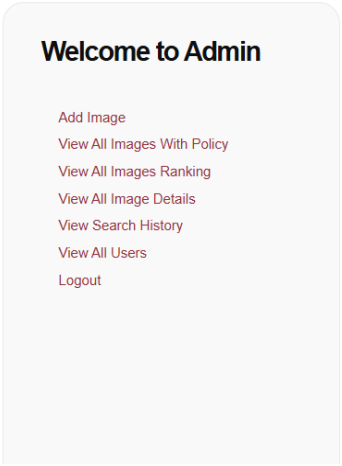


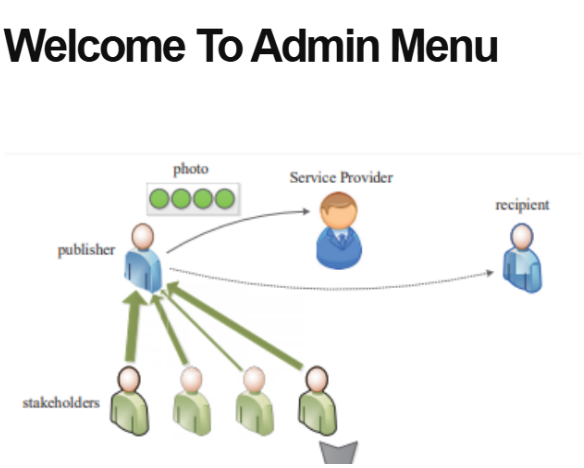
ADMIN LOGIN DETAILS:



ADMIN MENU PAGE:







6. CONCLUSION AND FUTURE WORK

CONCLUSION

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. The photo that a user wants to share is temporarily holden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders' privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher controls the trade-off between privacy preserving and information sharing, we propose a service provider assisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold

tuning method.

7. REFRENCES

- 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.
- M. Kaplan and M. Haenlein, “Users of the world, unite! the challenges and opportunities of social media,” Business horizons, vol. 53, no. 1, pp. 59–68, 2010.
- J. A. Obar and S. S. Wildman, “Social media definition and the governance challenge-an introduction to the special issue,” 2015.
- 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.
- 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
- Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, “What (or who) is public?: Privacy settings and social media content sharing,” in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.
- C. Squicciarini, M. Shehab, and F. Paci, “Collective privacy management in social networks,” in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.
- H. Hu, G.-J. Ahn, and J. Jorgensen, “Detecting and resolving privacy conflicts for collaborative data sharing in online social networks,” in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.
- J. M. Such and N. Criado, “Resolving multi-party privacy conflicts in social media,” IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016. L. Xu, C. Jiang, Y. Qian, Y. Zhao, J. Li, and Y. Ren, “Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 271–285, February 2017.