Identifying Unauthorized Activities In Social Network

Guide: Ms. Suganya P (Alwin A, Gokulnath G, Ragul R, Rahavan R)

Dept. of Information Technology Of (M.A.M. College Of Engineering And Technology), Tiruchirapalli, India

Abstract— Users can share their informations, images and videos in social media platforms like instagram, Facebook,ect..The networks are influenced by the spammers and lot of work has been done for identification and fixing. In particular, Cyber Attacks against Social Networks is an on-demand, portable, controllable by the cloud consumer and available through the pay-per-use cost model. The main objective detection of Intruder System against Social Networks, which is a network and signature based IDS for the cloud model.

Index Terms—Cloud storage, fog server, Xor-Combination, CRH, privacy

1 INTRODUCTION

Social media provides us with a platform to share our lives and express our opinions, it also poses a risk of unauthorized activities that can compromise our privacy and security.

One of the common concerns is the ability for others to download or take screenshots of a user's posts without their permission. This can result in the user's private information or sensitive content being shared with others. The major contribution for this work is a scalable and customizable cloud-based service that provides cloud consumers with IDS capabilities regardless of the cloud model. Social Networks administrators have the abilities to monitor and react to attacks on multiple VMs residing within a consumer's Virtual Private Cloud (VPC), and to identify specific attacking scenarios based on their application needs. The system can adapt its performance to the traffic load by activating the on-demand elasticity feature.

exposure by hackers in 2013, Apple's iCloud leakage in 2014, Dropbox data privacy breach in 2016, particularly iCloud's leakage event, where numerous Hollywood actresses' private photos were exposed and caused massive outcry. Such incidents affect company's reputation fervently [9-11]. In traditional cloud computing scenario, once users outsource their data to the cloud, they can no longer protect it physically. Cloud Service Provider (CSP) can access, search or modify their data stored in the cloud storage. At the same time, the CSP may loss the data unintentionally due to some technical faults.

Alternatingly, a hacker can violate the privacy of the user data. Using some cryptographic mechanisms (such as encryption, hash chain), confidentiality or integrity can be protected [12]. However, cryptographic approach cannot prevent internal attacks, no matter how much the algorithm improves [13]. To protect data confidentiality, integrity and availability (CIA), several research communities introduced the idea of Fog Computing placing fog devices in between the user and the cloud

IEEE Transactions on Cloud Computing 06 Sep 2022

Consequently, people are finding new mediums to store their data. Giving preference to powerful storage capacity, a growing number of users have switched to cloud storage; they even prefer to save their private data to the cloud. Storing data on a commercial public cloud server will be a prevalent trend in the near future. Getting inspired by the fact, many organizations, such as Dropbox, Google Drive, iCloud and Baidu cloud are providing a variety of storage services to their users. However, advantages of cloud storage are accompanied with a set of cyber threats [5-8]. Privacy issue is one of the major threats in addition to loss of data, malicious modification, server crash are some examples of cyber threats. There are some prominent cyber incidents in the history, for example, Yahoo's three billion accounts

server. One of the prominent and recent works in this field is proposed by Wang et al. They utilized *Reed Solomon code* and hash digest centric customized algorithms to preserve confidentiality and integrity of the data respectively [12]. They also formulated the computational intelligence (CI) to determine the portion of data to be stored in cloud, fog and user's local machine. They maintained a rating system for cloud server so that user can rate the cloud servers and the cloud servers tend to act responsively. Nonetheless, this scheme reveals that some portion of data (not the entire data) to the cloud and their customized hash algorithm, despite taking extra computation/storage overhead, adds no value over standard hash algorithm (i.e. MD5) in terms of collision resistance. In this paper, we propose a fog-based cloud storage scheme for data confidentiality, integrity and availability. For confidentiality and availability (even after malicious events), we propose a method referred to as $Xor-Combination$ that splits the data into several blocks, combine multiple blocks using Xor

operation and outsource the resulted blocks to different cloud/fog servers. In order to prevent any individual cloud server to retrieve a portion of original data, the proposed technique $Block - Management$ selects the cloud server to store each particular data blocks. $Xor - Combination$ along with $Block - Management$ helps to protect data and to retrieve data from multiple sources even when some blocks are missing. At the same time, we propose a noble hashing mechanism titled as $Collision\ Resolving\ Hashing$ (CRH) operation based on traditional hash algorithm (i.e., SHA256, MD5) that withstands collision in hashing [14] and security features. The proposed scheme thrives to be a robust solution for efficient and secure cloud storage. The main contributions of the paper can be summarized as follows:

- We proposed a secure cloud storage scheme based on fog computing employing $Xor - Combination$, $Block - Management$ and CRH operation. $Xor - Combination$ together with $Block - Management$ contributes to maintain privacy and to prevent data loss. CRH operation ensures detection of data modification.
- Theoretical security analysis proves the privacy guarantee, data recoverability, and modification detection of the proposed scheme.
- We implemented a prototype version of the scheme and conducted experiments to verify its performance in comparison with the contemporary scheme. Results prove its efficiency in terms of time and memory usage.

Organization: Rest of the paper is organized as follows: Section 2 discusses some related works and section 3 defines the system model, threat model and design goal. Section 4 presents the proposed scheme in details. Section 5 analyses theoretical security/privacy, recoverability, modification detection of the proposed scheme. Experiment and performance analysis are illustrated in section 6. Section 7 concludes the paper with discussing the result and some future research directions.

2 Related Work

Importance of cloud storage draws attention of researchers from both academia and industry. Improving the performance of the cloud storage as well as maintaining the security level are the main research domains. Security issues are always the focus of research in order to enhance credibility of the storage mechanisms [15]. A range of survey papers [16-19] indicated that privacy breaches, malicious modification (or integrity violation), data loss are the main cyber threats of cloud storage. Kaufman argued that, to cope with the aforementioned experienced security threats, cloud servers have to establish coherent and effectual policy [20]. Zissis et al. evaluated cloud security by identifying unique security requirements and presented a conceptual solution using trusted third party (TTP). As underlying cryptographic tool they used public key cryptography to ensure confidentiality, integrity and authenticity of data and communication while addressing specific vulnerabilities [21]. Wang et al. focused on integrity protection on cloud computing and proposed public auditability scheme as a counter measure [22]. They set two goals of their work, one was the efficient public auditing without requiring local copy of data and the other one was not to cause any vulnerability of the data. They utilized homomorphic authenticator with random masking for privacy preserving public auditing of cloud data. However, public key centric homomorphic authenticator caused computational burden and this work did not focus on partial/entire data loss. An efficient public auditing protocol using sampling block-less verification was proposed in [23]. At the core of their proposed protocol there was a noble dynamic data structure which consisted of doubly linked info table and a location array. This structure reduces the computation/communication cost substantially. Conversely, like previous scheme, it does not address cyber threats other than integrity checks.

Xia et al. proposed a mechanism titled Content Based Image Retrieval (CBIR) to protect image outsourced to cloud server relying on locality sensitive hashing (LSH) and secure k-nearest-neighbors (kNN) algorithms [24]. It is equally applicable to other data types (i.e., text) as well. It preserves privacy of sensitive images and ensures efficient retrieval but does not guarantee integrity or elimination of an image (or other type of data). Arora et al. enlisted and compared some cryptographic primitives

IEEE Transactions on Cloud Computing

for preservation of privacy and integrity of cloud storage [25]. This comparison is also befitting for other computing architecture. One recent work reported by Shen et al. used cloud infrastructure for urbanization. Their proposal illustrated cloud to share data between urban people and/or applications [26]. To protect privacy of shared data they used attributed based encryption (ABT). However, they concentrated on the privacy of data and relied on cloud server for integrity and data loss prevention. Precisely, Khan et al. emphasized trust in cloud computing. The challenges of trust in cloud and how a cloud server can achieve trust of its customer have been discussed in their article [27]. The previous researches discussed so far are most commonly related to integrity preservation by various public/private auditing frameworks. Privacy, on the other hand, is best protected by encryption, though the encryption techniques making the searching operation difficult. Hence, different searchable encryption schemes came into existence related to searching on encrypted cloud data [28-30]. In contrast with different third party auditor (TTA) based solutions, fog server centric solutions have upper hand in terms of preventing cyber threats. For example, TTA solutions are good for finding malicious modification but they do little for privacy preservation. Similarly, searchable encryption related solutions work well for preserving privacy and (comparatively) efficient

retrieval of data but they have issues like data loss and modification. Conversely, fog server which is an extension of cloud server at proximity of the user can provide a prospective solution to fight against various cyber threats. However, fog based solutions to combat cyber threats are yet to be explored in detail. Tian et al. proposed a new scheme of cloud storage resorting to fog server in order to protect against different attacks [13]. They adopted three-layered architecture, kept the fog server in between the cloud server and the users. Considering fog server being trusted by the user, they presented a noble scheme for privacy preservation, modification detection, and data loss prevention. They encode the data utilizing Reed-Solomon code and deduce Computation Intelligence (CI) to determine the amount of data to be outsourced to cloud/fog servers so that no individual cloud server can reconstruct the data. However, fraction of data gets exposed to each outsourcing cloud server. On the other hand, they formulate Malicious Modification Detection (MMD) to detect malicious modification that has no advantage over traditional hashing algorithms to detect malicious modification. Another recent work proposed [12] also undertook the similar work with same architecture. These papers recommend the use of fog based solutions for secure cloud storage and more importantly, to protect against the cyber threats, those directed towards cloud data. In this paper, the authors propose a secure cloud storage scheme on the basis of fog server considering Tian et al.'s scheme as the benchmark.

3 THREAT MODEL

The problem of PLPC investigates privacy leakage in a system where privacy control is enforced. Given a privacy control mechanism, PLPC examines whether a user's private personal information is leaked even if the user properly configures privacy rules to protect the corresponding information. The problem of PLPC in OSNs involves two parties, distributor and receiver. A user who publishes and shares his/her personal information is a distributor while the user whom the personal information is shared with is a receiver. An adversary is a receiver who intends to learn a distributor's information that is not shared with him. Correspondingly, the target distributor is referred to as victim. Prior research (Zheleva and Getoor, 2009; Chaabane et al., 2012; Balduzzi et al., 2010) mainly focuses the inference of undisclosed user information from their publicly shared information. Since the effectiveness of these inference techniques will be hampered by increasing user awareness of privacy concern (Chaabane et al., 2012), we further include insiders in our analysis. The adversaries have the incentive to register as OSN users so that they may directly access a victim's private personal information or infer the victim's private personal information from other users connected with the victim in OSNs. The capabilities of an adversary can be characterized according to two factors. The first factor is the distance between adversary and victim. According to privacy rules available in existing OSNs, a distributor usually chooses specific receivers to share her information based on the distance between the distributor and the receivers. Therefore, we classify an adversary's capability based on his distance to a victim. Considering the social network as a directed graph, the distance between two users can be measured by the number of hops in the shortest connected path between the two users. An n-hop adversary can be defined such that the length of the shortest connected path from victim to adversary is n hops. We consider the following three types of adversaries in our discussion, 1-hop adversary, 2-hop adversary, and k-hop adversary, where k > 2. On Facebook, they correspond to Friendonly, Friend-of-Friend, and Public, respectively. On Googleþ, they correspond to Your-circles, Extended-circles, and Public, respectively. For ease of readability, we use friend, friend of friend, and stranger to represent 1-hop adversary, 2-hop adversary, and k-hop adversary (where k > 2) adversaries, respectively: 1) If an adversary is a friend of a victim, he is stored in the outgoing list in the victim SR set. The adversary can view the victim's information that is shared with her friends, friends of friends, or all receivers in an OSN. However, the adversary cannot view the information that is not shared with any receivers (e.g. the "only me" option on Facebook). 2) If an adversary is a friend of friend, he can view the victim's information shared with her friend-of-friends or all receivers. However, the adversary cannot view any information that is shared with friends only, or any information that is not shared with any receivers. 3) If an adversary is a stranger, he can access the victim's information that is shared with all receivers. However, the adversary cannot view any information which is shared with friends of friends and friends. Besides the above restrictions, an adversary cannot view a victim's personal information if the adversary is included in the victim's black lists (e.g. "except" or "block" option on Facebook, and "block" option on Googleþ). An adversary may have prior knowledge about a victim. We will specify the exact requirement of such prior knowledge for different attacks in Section 5. Since a user may use multiple OSNs, it is possible for an adversary to infer the user's private data by collecting and analyzing the information shared in different OSNs. We exclude social engineering attacks where a victim is deceived to disclose her private information voluntarily. We also exclude privacy leakage caused by improper privacy settings. These two cases cannot be addressed completely by any technical measures alone.

4 PROPOSED SOLUTION

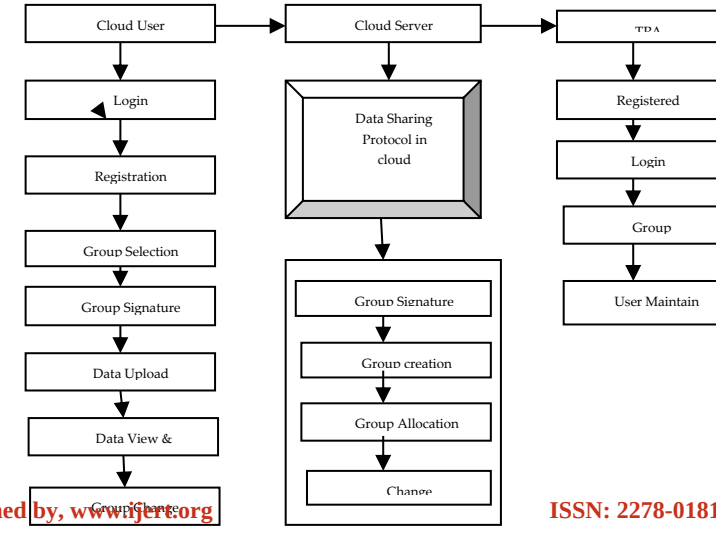
Social network users can also take control of their privacy settings by restricting access to their posts. Users can choose to make their profiles private or limit the audience of their posts to specific individuals or groups. This can help to minimize the risk of unauthorized users accessing their content.

Cloud security must grow and evolve to face these threats and provide a bulwark of defense for the consumers that leverage the

efficiencies and advantages cloud services provide. Cloud services can not only secure data within the cloud, but can leverage the transformative cloud industry to secure the endpoint users that use service.

5 Security Analysis

Data Confidentiality. For data objects that are not under any SDS constraint, confidentiality is guaranteed because we follow [8] for these data objects. The SDS monitor can just be regarded as an external user who does not have sufficient attributes. Considering data objects that are under the SDS constraints, we introduced the following concepts: the SDS monitor, the SDS constraint specific dummy attributes, and additional partial decryption by the SDS monitor. Therefore, we mainly analyze the effect of the corresponding changes regarding the data confidentiality. An external user ut whose attributes do not match the tree access structure in the ciphertext cannot produce a valid token for partial decryption. This results in the fact that the proxy server cannot extract the expected value $e(g, g)rt\tau s$ with the invalid token without knowing rt and τ, which are unique secrets to the user. Assuming that the unauthorized user ut directly fetches the ciphertext from the cloud storage server without using the token, he/she cannot compute $e(g, g)rts$ because his/her attributes do not match the access tree. Moreover, he/she cannot cast off the session keys KS and KSDS embedded in the ciphertext component $C=M\cdot\tilde{K}\ S\cdot K\text{SDS}\cdot e(g, g)\alpha s$ because KS is only shared by the data owner and the proxy server, and KSDS is only shared by the data owner and the SDS monitor. The proxy server, similar to other external unauthorized users, not only does not have sufficient attributes to decrypt the ciphertext but also cannot cast off KSDS embedded in the ciphertext component $C=M\cdot\tilde{K}\ S\cdot K\text{SDS}\cdot e(g, g)\alpha s$ because KSDS is only shared by the data owner and the SDS monitor. The KGC cannot decrypt the ciphertext because the session keys KS and KSDS are embedded in the ciphertext component $C=M\cdot\tilde{K}\ S\cdot K\text{SDS}\cdot e(g, g)\alpha s$. In addition, KS is shared only by the data owner and the proxy server, and KSDS is shared only by the data owner and the SDS monitor. The KGC cannot determine KS and KSDS because of the session key secrecy property of the key agreement [20]. Assuming that the KGC can access the partially decrypted ciphertext $CT'=(\tilde{C}', C=hs, A, H1(K\theta i,j))$, where $\tilde{C}'=C/\tilde{K}\ S=M\cdot K\text{SDS}\cdot e(g, g)\alpha s$ from the proxy server, it still cannot cast off KSDS because KSDS is only shared by the data owner and the SDS monitor. Moreover, the KGC cannot cast off τ from $A=e(g, g)rt\tau s$ to obtain the expected value $e(g, g)rts$ because τ is a unique secret to the user. The SDS monitor cannot decrypt the ciphertext for two reasons. First, it cannot cast off τ from $A=e(g, g)rt\tau s$ to obtain the expected value $e(g, g)rts$ because τ is a unique secret to the user. Second, the SDS monitor does not know β, rt, or $g\alpha$ to obtain the expected value $g(\alpha+rt)/\beta$ because β and $g\alpha$ are private keys of the KGC and because rt is a unique secret to the user. In addition, the SDS constraint specific dummy attributes themselves do not disclose any information about the content of the data object because they are completely independent of the content of the data object. Collusion Resistance. For both ordinary data objects and the data objects that are under the SDS constraints, collusion resistance is guaranteed. The ciphertext component $C=M\cdot\tilde{K}\ S\cdot K\text{SDS}\cdot e(g, g)\alpha s$ is different from that in Hur's scheme for the data that are under an SDS constraint, but this does not affect collusion resistance. The random value rt, which is unique to each user in the users' private keys, prevents several users from combining their private keys to produce a token to decrypt the ciphertext unless one of the users has sufficient valid attributes to produce a token to achieve $e(g, g)\alpha s$. SDS Constraint. The data object that is under an SDS constraint must pass through the SDS constraint checkpoint, the SDS monitor, because the session key KSDS is embedded in the ciphertext component $C=M\cdot\tilde{K}\ S\cdot K\text{SDS}\cdot e(g, g)\alpha s$. Neither the proxy server, the KGC, nor the user can cast off KSDS because KSDS is only shared by the data owner and the SDS monitor. When the SDS monitor receives the partially decrypted ciphertext from the proxy server, the SDS monitor checks if the user's current data access violates an SDS constraint by comparing $H1(K\theta\iota,J)$ in the ciphertext to the precomputed values $\Theta i,j=H1(K\theta i,j)$, $j=1, 2, \ldots, ni$, $i=1, 2, \ldots, m$, where $K\theta i,j=e(g\alpha, H(\theta i,j)\sigma)$, $j=1, 2, \ldots, ni$, $i=1, 2, \ldots, m$, for SDS INFO(a) $i=\{\theta(a)\ i,1, \theta(a)\ i,2, \ldots, \theta(a)\ i,ni, ki\}$ $1\le i\le m$, and it checks if $|H\text{ Attr}(ut, \text{SDS}(ua)\ \iota)\cup\{\theta\iota,j\}|=k\iota$. If the SDS monitor determines that the current data access violates an SDS constraint, the SDS monitor destroys the data immediately. We consider that the duty of access control policy enforcement and the duty of SDS constraint policy 10 Security and Communication Networks enforcement should be separated into two different entities. Therefore, we add an SDS monitor to the system architecture instead of only using the proxy server to perform both duties. Performing this separation follows the access control principle of separation of duty.



6 ANALYSIS OF POTENTIALLY VULNERABLE USERS

A user's personal information in OSNs could be leaked to adversaries who acquire necessary capabilities to perform the attacks, which have been discussed in Section 5. The effectiveness of the attacks can be affected by users' and their friends' sharing behaviors in OSNs. To investigate the users who can be vulnerable to these attacks, we conducted an online survey and collected users' usage data on Facebook, Googleþ, and Twitter. In this section, we first describe the design of the online survey. We then present the demographic data collected in the survey. Based on the survey results, we analyze how widely the users in OSNs can be vulnerable to the corresponding attacks. 6.1. Methodology The participants to our online survey are mainly recruited from undergraduate students in our university. We mainly focus on young students in our survey because they are active users of OSNs. Our study shows that they are particularly vulnerable to the privacy attacks. Each participant uses at least one OSN among Facebook, Googleþ, and Twitter. The survey questionnaire consists of four sections including 37 questions in total. In the first section, we gave an initial set of demographic questions and a set of general questions such as participants' awareness on privacy and what OSNs (i.e. Facebook, Googleþ, and Twitter) they use. All the participants need to answer the questions in the first section. In the following three sections, questions about participants' knowledge and privacy attitude towards Facebook, Googleþ, and Twitter are raised, respectively. Each participant only needs to answer the questions which are relevant to them in these three sections. 6.2. Demographics There are 97 participants in total, among which 60 participants reported being male, and 37 reported female. Our participants' age ranges from 18 to 31, with an average of 22.7. All of the 97 participants are Facebook users, among whom 95 participants have been using Facebook for more than 1 year, and 2 have been using Facebook for less than 1 month. About a half participants (41/97) are Googleþ users, among whom 23 participants have been using Googleþ for more than 1 year, 13 have been using Googleþ for about 1 monthe1 year, and 5 have been using Googleþ for less than 1 month. Similarly, about a half participants (40/97) are Twitter users, among whom 36 participants have been using Twitter for more than 1 year, 3 have been using Twitter for about 1 monthe1 year, and 1 has been using Twitter for less than 1 month. 6.3. Attacks to PP set To obtain the undisclosed personal information in a victim's PP set, adversaries could exploit the inferable personal particulars and cross-site incompatibility to launch two corresponding attacks as discussed below. 6.3.1. Inferable personal particulars As discussed in Section 5.1.1, due to inferable personal particular (Exploit 1), a victim and most of his/her friends may share common or similar personal particulars. Our study results show that 71% of the Facebook users are connected with their classmates on Facebook; 78% of the Googleþ users are connected with their classmates on Googleþ; and 73% of the Twitter users are connected with their classmates on Twitter. Via Exploit 1, an adversary could perform Attack 1 and infer a victim's personal particular from the personal particulars shared by most of her friends. To perform Attack 1, two types of knowledge are required: a large portion of users stored in the victim's SR set and their personal particulars. The protection of the victim's SR set could help prevent the adversary from obtaining the victim's relationships. Unfortunately, our study shows that 22% of the Facebook users, 39% of the Googleþ users, and 35% of the Twitter users choose the “Public” privacy rule or the default privacy rule4 for their social relationships, which means that these users share their social relationships with the public. Moreover, the OSNs users may connect to strangers. According to our study, 60% of the Facebook users, 27% of the Googleþ users, and 30% of the Twitter users have set up connections with strangers, which leave their SR set information vulnerable to Exploit 4 (unregulated relationship recommendation) as discussed in Section 5.2.2. The privacy rules for personal particulars of the victim's friends can be set to prevent the adversary from obtaining the second type of knowledge required in Attack 1. However, the victim's personal particulars can be exposed to threats if his/ her friends publicly share their personal particulars. In our study, 43% of the Facebook users, 44% of the Googleþ users, and 48% of the Twitter users share their personal particular publicly because they choose the “Public” privacy rule or the default privacy rule.5 6.3.2. Cross-site incompatibility Users may use multiple OSNs at the same time. According to our survey, 54 out of 97 participants use at least two OSNs as shown in Fig. 7. And 27 participants publish their posts in more than one OSN at the same time as shown in Fig. 8. If a user publishes personal information in multiple OSNs, he/she may set different privacy control rules vulnerable to Exploit 2, i.e. cross-site incompatibility.

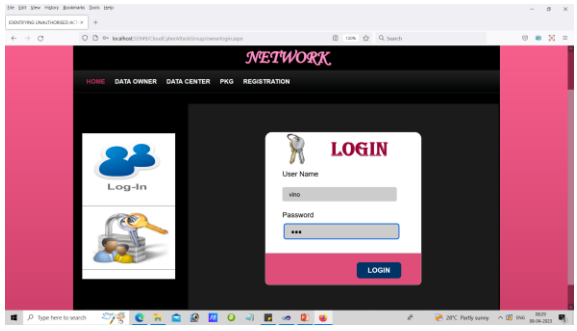
7 FUTURE ENCHANCEMENT

Improved User Permission Controls: To provide users with more granular control over who can view and download their content, as well as the ability to restrict screenshotting.

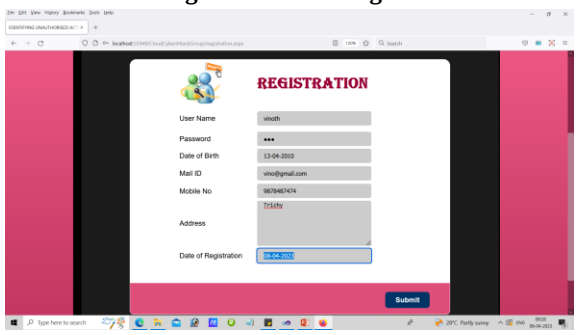
AI-Based Detection: Using artificial intelligence (AI) algorithms to automatically detect and flag instances of unauthorized access or activity, such as unusual download or screenshot patterns.

Blockchain-Based Security: A more advanced approach could be to incorporate blockchain technology into the social network's security architecture. This would create a decentralized, tamper-proof record of all user activity on the platform, making it more difficult for unauthorized parties to access or manipulate content.

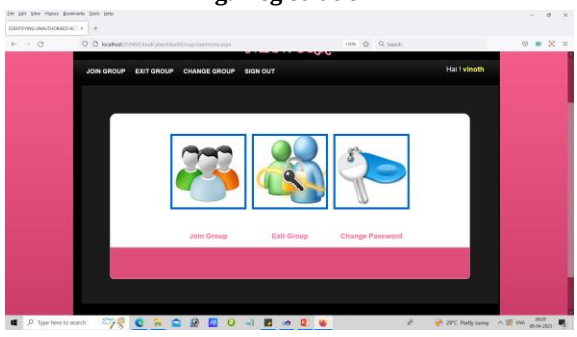
8 RESULT AND DISCUSSION



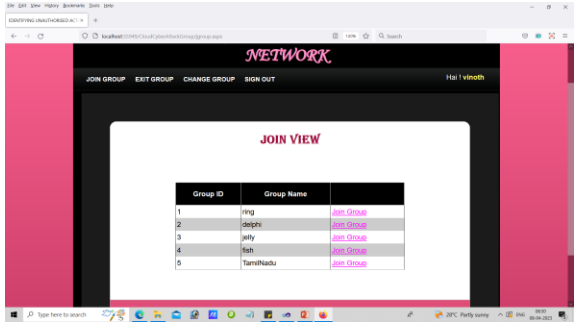
Fg. Cloud User Login



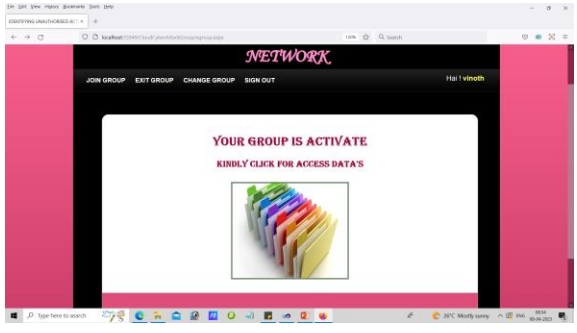
Fg. Registration



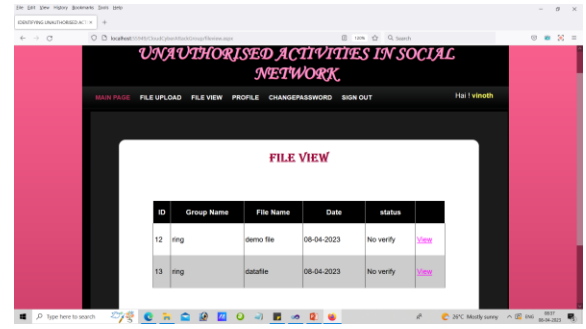
Fg. Clould Main Page



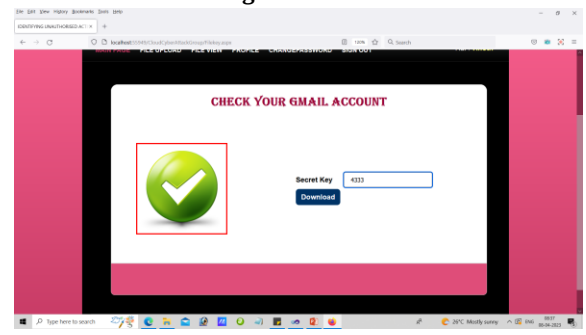
Fg. Group Joining



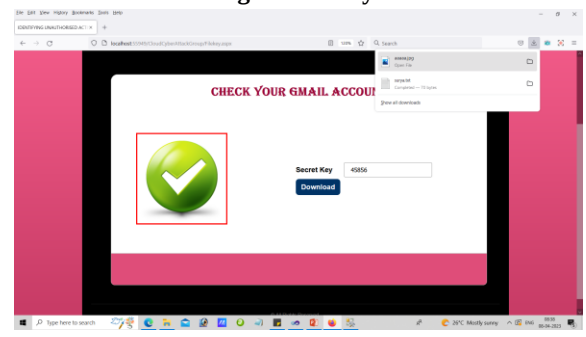
Fg. Group Activation



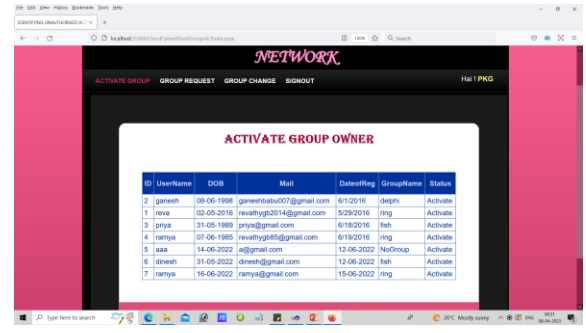
Fg. File View



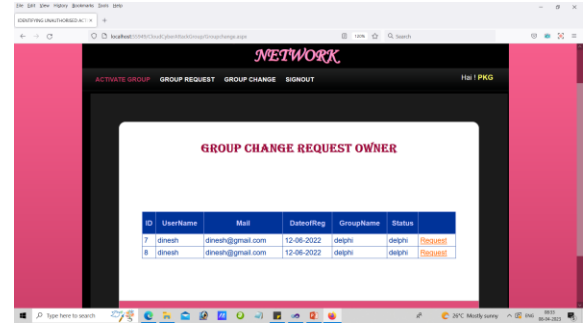
Fg. Enter Key



Eg File Download



Fg. Activate Group



Fg. Group Change Request

9 CONCLUSION

In conclusion, the objective of identifying unauthorized activities in social networks related to downloading or taking screenshots of user's posts is critical in ensuring the privacy and security of user's data. By identifying and preventing such activities, social media platforms can protect their users from potential privacy violations and reputational harm. This objective requires a combination of technological measures, such as limiting the ability to download or take screenshots, and user education on best practices for protecting their data. Overall, identifying and addressing unauthorized activities in social networks is an essential step towards creating a safe and secure online environment for users.

10 ACKNOWLEDGMENT

This research work was partially supported by the Faculty of Computer Science and Information Technology, University of Malaya under a special allocation of the Post Graduate Fund for RP036-15AET project. Imran's work is supported by the Deanship of Scientific Research, King Saud University, Saudi Arabia through Research Group No. 1435-051.

11 REFERENCE

[1] A. C. Squicciarini, M. Shehab, and J. Wede, "Privacy policies for shared content in social network sites," The VLDB Journal, vol. 19, no. 6, pp. 777–796, Dec. 2020.

[2] Y.-P. Guan, Z.-Q. You, and X.-P. Han, "Reconstruction of social group networks from friendship networks using a tag-based model," Physica A: Statistical Mechanics and

its Applications, vol. 463, pp. 485 – 492, 2020

[3] J. Qiu, Y. Li, J. Tang, Z. Lu, H. Ye, B. Chen, Q. Yang, and J. E. Hopcroft, "The lifecycle and cascade of wechat social messaging groups," in Proceedings of the 25th

International Conference on World Wide Web, ser. WWW '16, 2020, pp. 311–320.

[4] R. Krishnan, R. Sandhu, J. Niu, and W. H. Winsborough, "A conceptual framework for group-centric secure information sharing," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09. New York, NY, USA: ACM, 2021, pp. 384–387.

[5] Y. Li, Y. Li, Q. Yan, and R. H. Deng, "Privacy leakage analysis in online social networks," Computers & Security, vol. 49, pp. 239 – 254, 2021. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814001588