PREVENTING UNAUTHORIZED USERS FROM VIEWING THE PROFILE PHOTO IN A SOCIAL MEDIA

Jeevithashree DV[1], Pooja Anandani[2], Diksha Mishra[3], Natarajan P[4]

[1,2,3,4] *School of Computer Science and Engineering (SCOPE) VIT University Vellore-632014*

Abstract

Social Networking is one of the most dominant popular innovative technological phenomena which is prevailing these days, with an aid of over a huge number of human population. Many major online platforms such as Facebook, Friendster etc. permits millions of people to design and set up their personal profiles and share their private information with a far-reaching chain of friends, relatives, colleagues, strangers etc. With the vast utilization of these social networking sites, the problem of maintaining the privacy of the information has gained at most attention. Many different approaches have been formulated to encounter such issues. One such approach for managing the privacy is called the 'key management technique'. Thus, this paper proposes a key management system to allow the user to post information that are encrypted such that only the authorized users who are compatible with the corresponding security policy can obtain the key to access the information, thereby providing an efficient way to prevent privacy in a private Social network. Based on the formulated groundwork, an application is constructed which helps in maintaining the privacy of the profile photo.

Keywords- *Social networking, Key management system, Cryptosystem, Privacy, Encryption.*

----------***----------

1. INTRODUCTION

Social networking sites like twitter, Facebook, Instagram have become important part of individual's lifestyle. It is a web service where different individuals share data information, pictures according to their own view point via different types of network. [6]. Many social networking sites which have recently developed have becoming popular in interest to public and also help the individuals to connect to people with their day to day activities. For instance, individuals can connect to their friends with various social platforms like Twitter, Friendster etc., get in touch with the technical society for work or business related activities via LinkedIn etc. The profile information which is

available on the social networks is convenient to get the detailed information of the individual's daily life style and their activities. This may lead to issues which may hinder the personal privacy of an individual. For example, a person's personalinformation might be put in use for some wrong advertisements by some unauthorized users, and so on.Hence privacy plays a very important role in social networking sites. Especially when the users portray their personal information, profile pictures etc.

Consider Facebook social network, the profile picture can be viewed by any random person. This causes major privacy issues which may lead to serious problems. In order to overcome this issue, this paper proposes a key management system. Here the user can view one's profile picture only if he/she is permissible to view with a secret key. If the key is not known to the user by the admin then the picture can neither be downloaded nor viewed. In such scenarios, Cryptography forms the main tool for privacy management. It is nothing but the art of constructing or analyzing protocols which prevents the third parties from reading private messages.

In following paper, the second module is about the literature survey giving brief description about previous works done by researchers. The third module in this paper briefly describes about the proposed model with its corresponding block diagram and flowchart narrating about problem solution. Finally we close the paper with result analysis and conclusion followed by references.

2. LITERATURE SURVEY

Numerous writers have as of now given their contribution in field privacy in social media .This Literature review demonstrates the new goals achieved by different scientists and also the related works achieved by others .This module exhibits our knowledge and ability to solve the problem of Facebook profile picture privacy.

Mohamed Shehab,SaidMarouf ,Christopher Hudel [1] We proposed an expansion that Auth researcher provided in his study that empowers the facilitating of detailed study permission approval by clients while allowing consents to third party applications. They have proposed a procedure that processes consent rating or permission rating taking into account a multi-criteria suggestion model which uses past client choices, and software requests to improve security of the client. They actualized their proposed OAuth augmentation as a program expansion that permits clients to effortlessly configure their security settings during installation of application, gives suggestions on asked for attributes of privacy, and gathers information with respect to client choices. They Investigation on the gathered information showed that the proposed structure efficiently

improved the client awareness and protection identified with third party application approvals.

MohamedoShehab ,MoonamoKo , HakimoTouati [2] presented a paper on cross-site association structure x-mngr, permitting clients to connect with clients using different social networking sites like facebook twitter, with a strategy named cross-site permission control , that empowers clients indicate different strategies which helps either to permit/disallow permission to their personal information that they have shared like images,videos across all the social networking site. They likewise propose a partial mapping technique in view of a super intend training technique to map client's personal information crosswise over different digital networking site. They executed their proposed system through a photograph collection in which they share different photohraphs using different social networking site like Instagram and Twitter, Facebook in light of the cross-site permission authority arrangement which is determined through the information holder. They have executed their proposed model and through broad experimentation and they have demonstrated the exactness and accuracy of their proposed techniques.

RalphoGross,AlessandrooAcquisti[3] examined different examples of data revelation in social networking sites and their privacy suggestions. They have investigated the online conduct approximately greater than 5,000 CarnegieoMellon Institution understudies of all those people whoever got involved in prominent in different multimedia sharing sites. They have assessed the quantity of datathey uncover and contemplate their use for the website's security environment. They underlined all possible assaults on different parts for protection, and they also demonstrated, only just an insignificant rate of clients changes the exceedingly security preferences.

Anna C,MohamedShehab, Federica Paci they have demonstrated the issue of collective implementation ruleof security strategies on common information by utilizing a unique approach of gaming. Specifically, they have suggested an answer that offers mechanized approaches to share pictures based on particular individuals' ownership. Expanding upon the Clarke-Tax system, they have depicted a basic method that advances honesty, and that prizes clients who advance co-ownership. They have incorporated their configuration with implementation procedures that provides freedom to the clients from the procedure of individually choosing confidentiality or security options for every photo.

MuhammadoUmaroChaudhry,YasiroSaleem, MuhammadoMunwar, MuhammadoYasir [5] in this paper they have proposed a crytographic structure to execute social networking site client's protection by taking out the interruption of the unapproved access. Taking into account the designed system, where the application is constructed which keeps running on the social networking site at the client's backend. This designed system encodes the information that is shared by user on social networking site and only authorized users will have the capacity to decrypt that content that is shared, accordingly accomplishing security objective.

3. PROPOSED MODEL

In the following module detailed study of proposed model is explained with a block diagram along with a flow chart to give precise knowledge of the concept of problem definition.

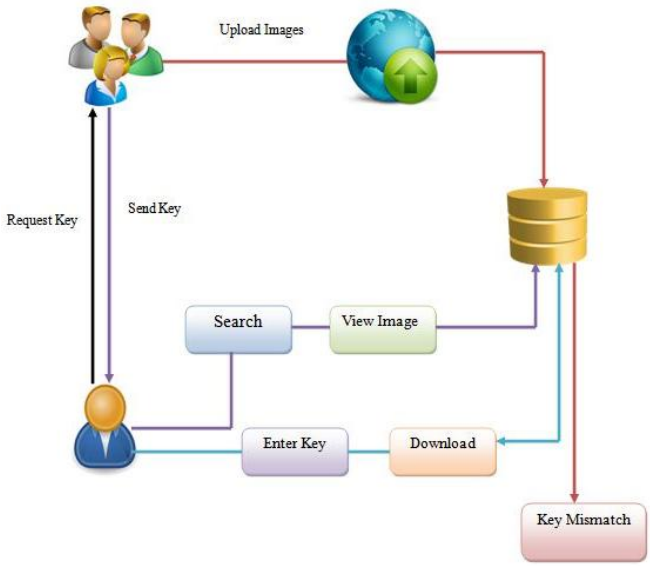

Figure 3.1: Block Diagram

The block diagram(Figure 3.1) is explained as below:
Back End: When users create their profile, they upload their profile image on to the social media. These images are stored in the database.

FrontEnd: Now suppose a user want to search for a person whose name is 'A', the user first searches for the person 'A' and then tries to view the image.Since,key management technique is used, a dialogue box appears before he/she downloads the image, which asks the user to enter the secret key. For the person to download and view the image he must know the secret key of person 'A'. If the user knows the secret key then he/she can enter the secret key and view the image.

If the key is not known by the user, the user sends a request to the person 'A' for requesting for the secret key. Then the person 'A' sends the acceptance along with the secret key to the user via email. Once the user receives this secret key he/she can enter in the dialogue box and view the image.
The flow chart (Figure 3.2) describing the same is given below:

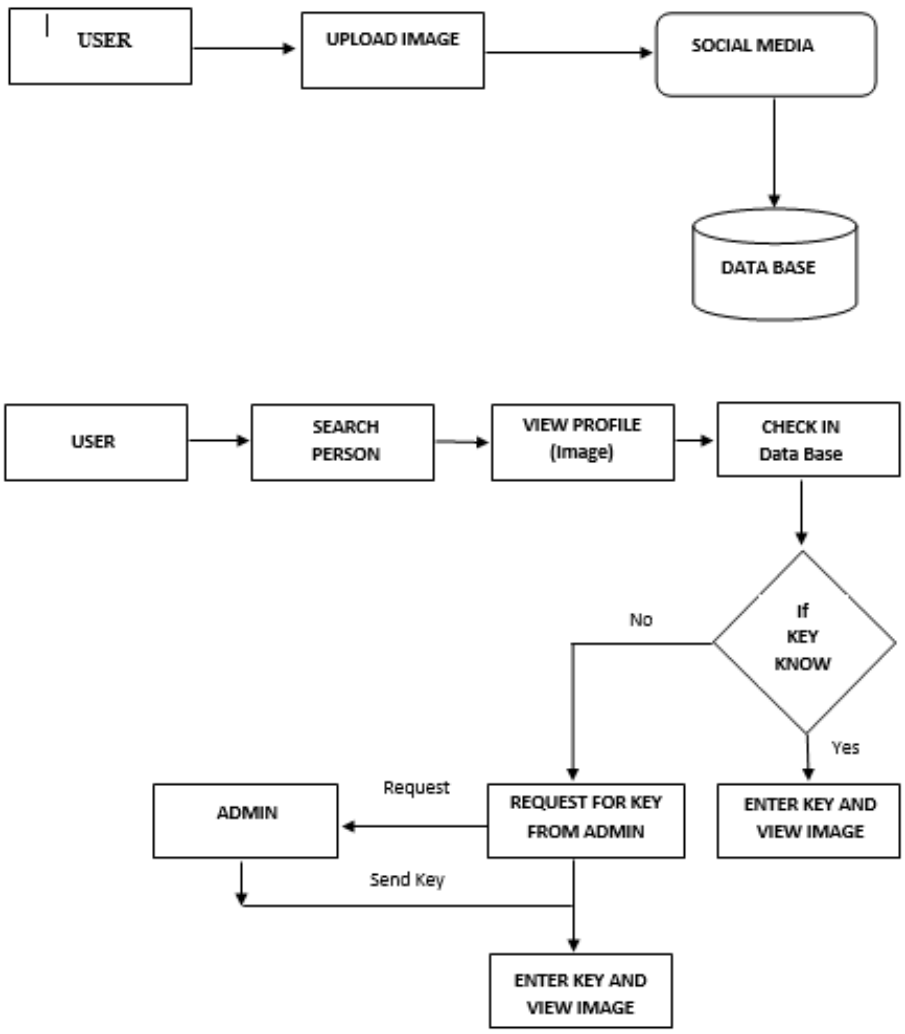

Figure 3.2 : Flow Chart

This technique basically helps in providing authentication before a person's profile picture is being downloaded and viewed, and hence provide privacy.

4. RESULT

The following are the snap shots of the output of our proposed model.

Figure 4.1: User enters his/her user Id and Password

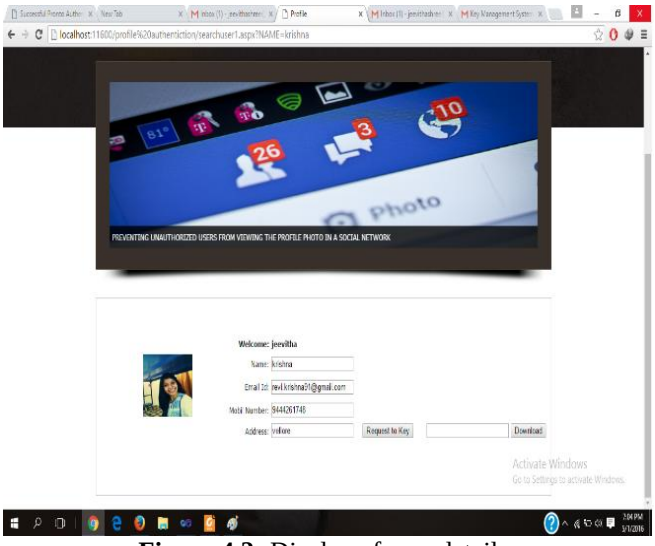

Figure 4.2: Display of user details

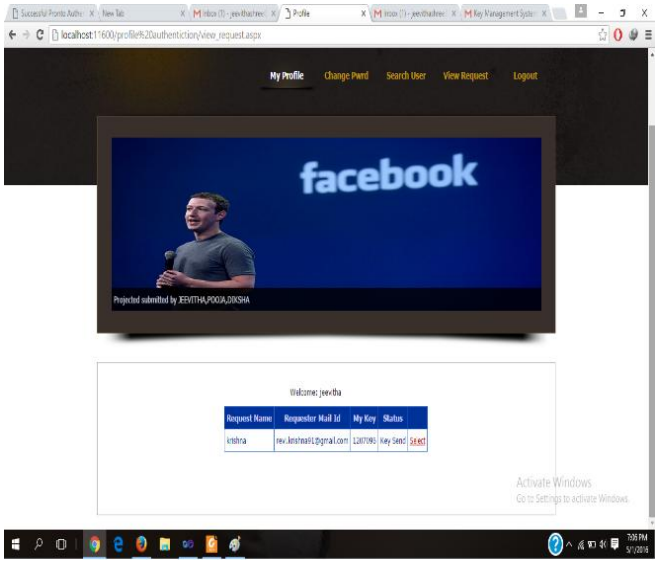

Figure 4.3: The receiver gets a notification that the requestor requires the key to view the profile pictures.

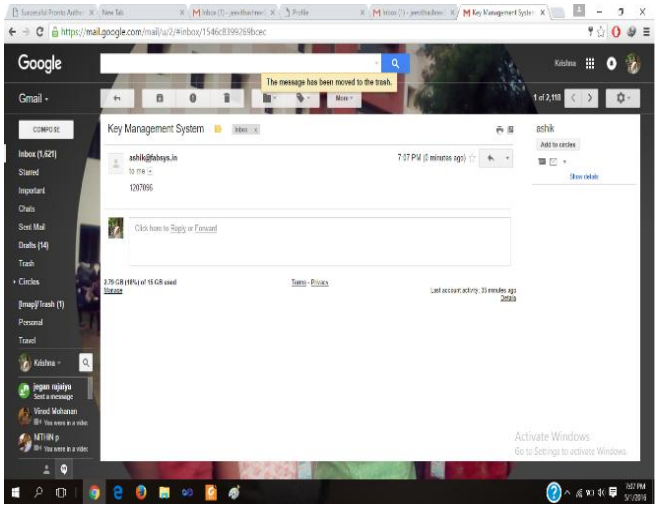

Figure 4.4: The requestor gets a mail which contains the secret key.

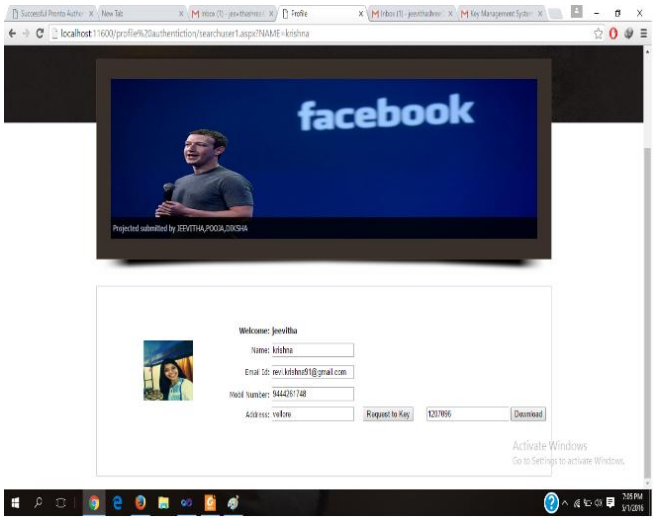

Figure 4.5: The key is put in order to view the profile picture.

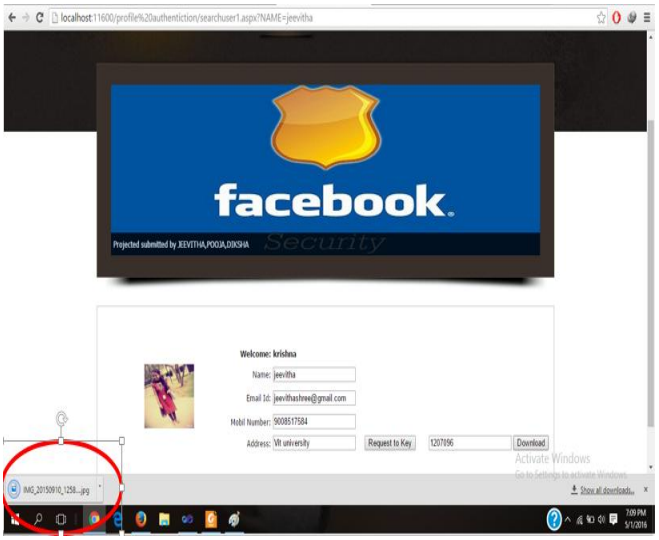

Figure 4.6: The profile photo gets automatically downloaded and the requestor can view the image.

CONCLUSION

1. Social networking sites are one of popular trends in youngsters as well as mid age people. It is easy for an individual profile to be associated with several other persons straightforwardly, and a large number of others through the system's ties. In this large number of friends some are actual friends some are completely strangers. And so, profile pictures and individual personal information is shared openly and publicly given.
2. In this paper, we presented a plan where different information is shared among different social networking sites,so we propose a key management strategy to provide security to user from unauthorized data. Using this key management technique,only the authorized users who fulfill the necessary security policy can get the key to obtain the data.Therefore this strategy helps to keep clients' profile pictures confidential and safe.

REFERENCE

[1]. Mohamed Shehab,SaidMarouf ,Christopher Hudel. “ROAuth: Recommendation Based Open Authorization” Symposium on Usable Privacy and Security (SOUPS) 2011, July 20–22, 2011.

[2]. Mohamed Shehab • MoonamKo • Hakim Touati “Enabling cross-site interactions in social networks” Springer-Verlag2012 : 12 January 2012.

[3]. Ralph Gross,AlessandroAcquisti. “Information Revelation and Privacy in Online Social Networks (The Facebook case)” ACM Workshop on Privacy in the Electronic Society (WPES) WPES’05, November 7, 2005

[4]. Anna C,MohamedShehab, Federica Paci. “Collective Privacy Management in Social Networks” International World Wide Web Conference Committee (IW3C2). WWW 2009, April 20–24, 2009

[5]. Muhammad Umar Chaudhry, YasirSaleem, Muhammad Munwar Iqbal, Muhammad Yasir. "User privacy protection in online social networks: secure file sharing on facebook" ISSN 1013-5316; CODEN: SINTE 8

[6]. W. Luo, Q. Xie, and U. Hengartner, "Facecloak: An architecture for user privacy on social networking sites," in CSE (3). IEEE Computer Society, 2009, pp. 26–33.