

WOMEN SECURITY ON SOCIAL MEDIA

Selvarathi C, Arjun K, Ram KumarP, Lokesh E, Saravana Kumar R
Department of CSE, M.Kumarasamy College of Engineering, Karur, India,

Abstract

The purpose of “Women’s Security in Social media” is secured that all women’s in social networks could be safe. Not only women, men’s can also be secured by this feature. Now-a-days most of them are finding a new friend through social networks. The major problems are coming through social networks by anonymous messages. Through the implementation of my new idea we can secure the unwanted message from unknown person. Based on my topic, I added many features to this project. The features that are added in my project is giving a privacy to women’s for hiding profile pictures to unknown person. There is another feature is added that, women can also wish to get friend request from either male or female. The one more important feature is that, they wish to receive friend request from a particular city, state or country. By this technique they can reject friend request from unknown person. The topic focuses on three main areas – privacy, security and a trusted network. This will help women to know how to, login and to set up notifications and the trusted contacts. The user can manage and control a privacy check option in which the user can set the limitations that who can see personal information and what is being shared. Women can live in a trusted community

Keywords: Encryption Standard, Simulation Software and Heidi SQL

1. Introduction

A question arises in my mind constantly – ‘Whether Women are Safe On the Internet and in social medias?’. Here the answer to the question is – Yes, they are! But it requires them to follow few steps as it’s always better to be safe for them. This is a project used to contribute the security for women’s in Facebook. Now-a-days most of them are finding a new friend through social networks. The major problems are coming through social networks. So, I decided to do a project based on the women’s security in social networks. By this project I secured that women can choose the features by allowing friend request from particular person like male or female. It is possible that women can get a friend only with female as well as male. One more feature is that they can able to select the particular location like city or country. Based on this type they can get a friend request from particular location. While women mostly use online social medias to make new connections and share their ideas and items from their personal lives and to get popular in the society, men use social medias means to gather information about business and increase their status.

2. LITERATURE SURVEY

Author: Kumar, Senthil & Kandasamy, Saravanakumar & K, Deepa

[1] According to the authors, their proposed system is by data mining technique which blocks the anonymous person to breach the users privacy. It blocks the users profile for any unknown and does not provide availability for the tagging options. It controls some features like who can message you and who can send the friend request. The authors specified about the breaches and attacks in the sites to safeguard the users details from any unknown persons. This safeguards the user details and their privacy concerns.

Author: Shevchuk, Ruslan & Pastukh, Yaroslav

[2] The model used in the mechanisms is mathematical model calculations by involving a straight forward estimated method for security tools by providing a two steps factor authentication device setup on work on the module. It provides different types of

security like absolute security, adequate security, basic security, satisfactory and unsatisfactory security. A chatbot is developed for the user to ensure and estimate the security level purposes. The security tools involved in this approach are two step factor authentication, Private account, Login notification, security checkups and trusted contacts.

Author: Kumari, Sangeeta & Singh, Shailendra

[3] This system provides access only to the privileged user not to the illegal user. It provides abstraction to the user details and hides the data to the unknown users. It provides big data privacy issues in public social medias. It performs optimized monitoring services like monitoring the employees and the organization. The author explained about the threats and vulnerability attacks. It mainly describes about four threats which are classic threats, modern threats and combination threats. By avoiding these kinds of threats and vulnerability data can be secured properly.

Author: Kumar, Vikas & Nanda, Pooja

[4] Although many advanced technologies came to the existence in the real world but still there is an issues in data leakage and privacy concerns. The information that is fed on the social medias are attacked are stole by some threats are affected by attacks. The approach provides the analytical tool which helps the companies to collect or search on the users data. It provides security to the user by verifying their mobile number and mail id. If any illegal activities happens, it will send the message to the particular user registered with the mobile number. It avoids the data sharing from one organization to other.

3. SYSTEM STUDY

3.1 Existing System

The System design has done after the intensive study. [5-10] The main study is to produce very fast and eliminate errors and give flexible to user. To enter the data, extensions are needed. The need of new system has risen, due to inconsistency of the existing system. Lots and lots of paper works are needed in the existing system. Manual calculations and in adequate information provided by existing system has led to development of proposed system. The main problems covered in the existing system are:

- **Time Consuming**

Now a day's time has become a governing factor in all aspects. The present system consumes a lot of valuable time, whereas the proposed system saves time considerably.

- **Accuracy**

The current system does not guarantee as much accuracy as proposed system. Management needs to ensure as much accuracy as possible for its benefit.

- **Paper**

The current system requires avoidance of paper work for its efficient running. The proposed system reduces much of the paper work by providing other efficient way for sharing data, which also provide for faster data retrieval.

- **Wrong Decision**

Sometimes decisions could be influenced on personnel basis that might hold wrong in case of existing system. But this can be avoided in the case of proposed system.

- **Human Error**

Manual system operations in the existing system almost involve lots of errors. This can be avoided in the case of proposed system.

3.2 Proposed System

The proposed system is designed in such a way that it overcomes the abuse of the existing system. The project along with the proposed system is considered to be very useful while handling the applications. The need of large storage places and other facilities are eliminated. The developed project is user – friendly and it is very easy for the user to handle.

4. ADVANCED ENCRYPTION STANDARD

In the early of 1970 Data Encryption Standard was in existence. [11-14] It is really a small key size of 56 bits or encrypted with 64 bits. Then it was replaced by AES in early 2001. Secured communication is one of the key components of digital world. Banking, Online application, wireless communication and home security needs encryption to log in and perform actions. The data should be protected in a secured way. Advanced Encryption Standard (AES) which is one of the most effective encryption algorithm. It transforms the unprotected or sensitive information into cryptograms. It replaces the cryptograms into normal information using right key. So that the data is secured from intruders or unknown person. The AES algorithm is used in the login page for password encryption. The passwords are stored in the back end sql with the username.

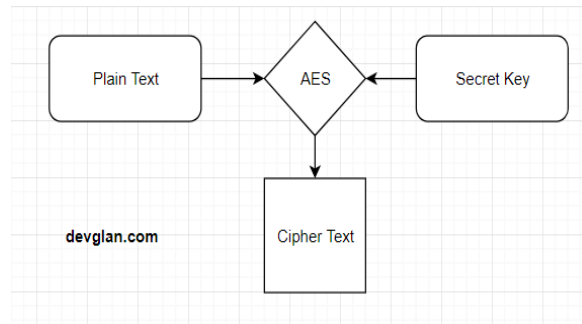


Figure 1: AES Design

5. Simulation SOFTWARE

5.1 Spring Tool Suite

[15-17] Spring Tool Suite (STS) is an eclipse based environment which is used for developing spring applications. It provides an easy environment for the user to implement, run, debug and deploy your applications. The main feature of STS is it validates the projects and provides quick fixes for the applications. It also includes integration for Pivotal tc Server, Pivotal Cloud Foundry, Git, Maven and AspectJ. STS is built as an addition on top of the latest Eclipse releases.

5.2 Heidi SQL

It is an Open source administration tool for MySQL . The user account details like username , password and mail id of the users are stored in back end. It enables you to browse and edit data, create and edit tables, views, procedures, triggers and scheduled events.

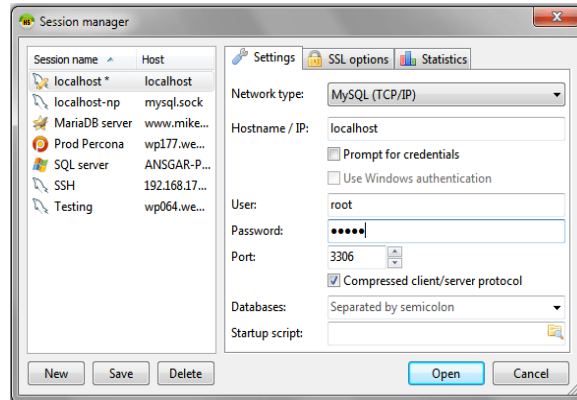


Figure 2: HeidiSQL Session Manager

6. METHODOLOGY

First the user should create a sign-up account to work on which will be stored in the admin database.

Then the user can log on to his account. The user can update his personal details like name, Address, email and location. The Fig 1 explains about flow diagram of the module. The user can set their profile picture from the local computer. There is a separate column for women named women privacy in which the women can set some limitations like whom can send the friend request and who can see their profile. For example if a woman chooses that only female can see the request means for the user she will receive only the female requests and also only female account members can see the profile page of the particular user if the user gave that only female can view her account. It shows the particular person account who matches with the details of the user account. It runs and fetches the details in by SQL commands.

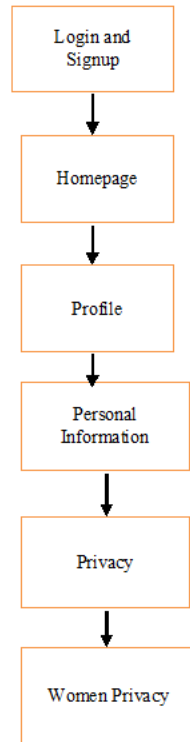


Figure 3:Module Flow Diagram for Women

Privacy

Using HeidiSql we can monitor the details of the users. If a user details matches with all other in this site it will bring first 1000 members to the existence of the user.

7. CONCLUSION

Our problem statement is to create a safe and secured platform in social media for women by rejecting anonymous request and messages. So, this web page paves the way for that. It will really help women to safe guard their profile in social medias.

REFERENCES

1. Kumar, Senthil&Kandasamy, Saravanakumar& K, Deepa. (2016), “**On Privacy and Security in Social Media – A Comprehensive Study. Procedia Computer Science**”, 2016, PP 114-119.
2. Shevchuk, Ruslan & Pastukh, Yaroslav. (2019). “**Improve the Security of Social Media Accounts**”. PP- 439-442. 10.1109/ACITT.2019.8779963.
3. Kumari, Sangeeta & Singh, Shailendra. (2015). “**A critical analysis of privacy and security on social media** “, pp 602-608
4. Kumar, Vikas& Nanda, Pooja. (2019). “**Social Media to Social Media Analytics: Ethical Challenges** “. International Journal of Techno ethics, pp 57-70.
5. Tse, Daniel & Lee, D.C.K. & Gong, H.H. &Sae, P.M. & Lam, J.W. & Lu, D.Z. (2014). “**Strategies in securing the social media**”, pp 141-150
6. Michael Fire, Roy Goldschmidt and Yuval Elovici,” **Online Social Networks: Threats and Solutions**” IEEE Communication Surveys & Tutorials, Fourth Quarter 2014, pp.2019-2036
7. Mohamed Bourimi, Ricardo Tesoriero, Pedro G. Villanueva, FatihKaratas and Philipp Schwarte, "**Privacy and Security in Multi-modal User Interface Modeling for Social Media,**" IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing2011, pp.1364-1371

8. Jong P. Yoon, Christopher M. Frenz, Zhixiong Chen and David Wang, "**Privacy-Preserving Mobile Accesses for Virtual Private Social Media**", IEEE Eighth World Congress on Services, 2012, pp.192-198
9. Santosh Krishna Putchala and Krishna Bhat and Anitha R, "**Information Security Challenges in Social Media Interactions**", IEEE, July 2013, pp.1-4
10. .PramodJagtap, Anupam Joshi, Tim Finin and Laura Zavala, "**Preserving Privacy in Context-Aware Systems**,"Fifth IEEE International Conference on Semantic Computing, 2011, pp.149-153.
11. P. Santhi, S.Thilagamani," A Survey on Audit Free Cloud Storage via Deniable Attribute Based Encryption", IRA-International Journal of Technology Engineering, Vol.5,No.1,PP.1-5,2016.
12. P.Pandiaraja,P.Viajayakumar,V.Vijayakumar,R.Seshadhri,"Computation efficiency Attribute based broadcast group key management for secure document access in public cloud" ,Journal of international Science and Engineering,Vol.33,No3,PP 695-712.
13. P.Pandiaraj, P.Vijayakumar, "Efficient Multikeyword search over Encrypted data in untrusted cloud environment",Second International conference on Recent trends and challenges in Computational Model(ICRTCCM -17,PP 251-256)
14. N.Deepa, P.Pandiaraja, "Hybrid context aware recommendation system for e-health care by Merkle Hash tree from cloud using evolutionary algorithm", Journal of soft Computing springer PP 1-13.
15. K Sumathi, P Pandiaraja,"Dynamic alternate buffer switching and congestion control in wireless multimedia sensor networks",Journal of Peer-to-Peer Networking and Applications,Springer US,PP 1-10.
16. S. Saravanan, T. Abirami, P. Pandiaraja,"Improve Efficient Keywords Searching Data Retrieval Process in Cloud Server",2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW),IEEE Explorer ,PP 219-223.
17. P.RajeshKanna,P.Pandiaraja "An Efficient Sentiment Analysis Approach for Product Review using Turney Algorithm",Journal of Procedia Computer Science Elsevier ,Volume 165 ,Issue 2019 ,PP 356-362.