International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

SOCIAL MEDIA SECURITY

Chander Singh[1], Dr. Devesh Katiyar[2], Gaurav Goel[3]

[1]Student of MCA, Department of Computer Science, DSMNR University, Lucknow, Uttar Pradesh, India
[2] [3]Asst. Professor, Department of Computer Science, DSMNR University, Lucknow, Uttar Pradesh, India

---

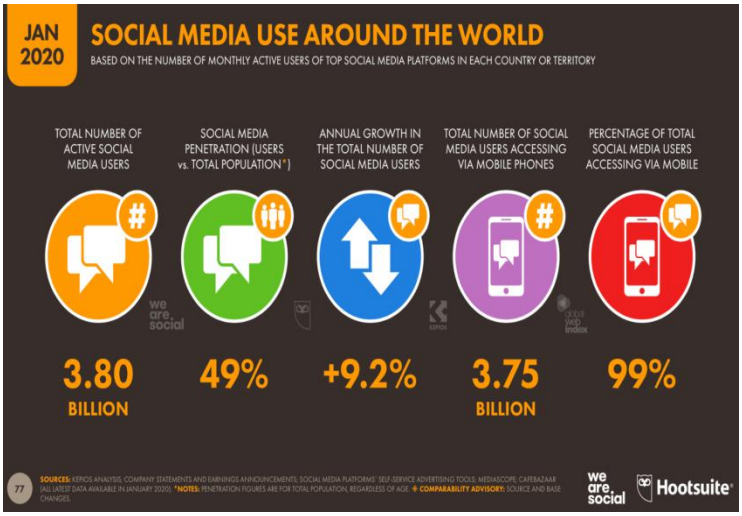
Abstract- *Today, almost everyone in this world uses any of the social media platforms. A social network is a public structure made up of people or associations called nodes, which are associated by at least one particular sorts of interdependency, for example, friendship, normal interest, and interchange of fund, connections of convictions, or information. We send messages, share personal data, like, images & videos and many more. When comes about personal data, the security becomes a topic of great concern. Till now, many steps have been taken to protect the personal and important data from intruders. But still there are some faults in these social media platforms. This paper represents one such problem and provides an adequate solution for this.*

Keywords- Social media; Security; Pin; Password; end-to-end Encryption

1. INTRODUCTION

In this fast moving and stressful world, people use social media platforms for sharing important data and for entertainment. Many internet clients consistently visit a large number of social sites to continue connecting with their companions, share their thoughts, photographs, recordings and talk about even about their everyday life. Social networks can be followed back to the main email which was sent in 1971 where two PCs were sitting ideal alongside each other. We feel really comfortable to use these social media platforms, which help us to connect with friends, families and others. But the more comfortable and attached we become with these sites, the more casual and careless we are to share personal details about ourselves. There is absolutely no doubt that social networks have become a part of every internet user these days and the trend is only set to increase. But even today, many of the internet and social media users face data security issues.

Today most of the people use social media. According to some reports as on January 2020, 49% of the world's population is currently on social media.



People share lots of important data in social media. Many innovations have been done to secure these data. Even today the advancement is in process. But what, when you give limited access to someone or someone hacks the social media account. Will he access only limited data? It totally depends on his moral values and ethics and nothing else.

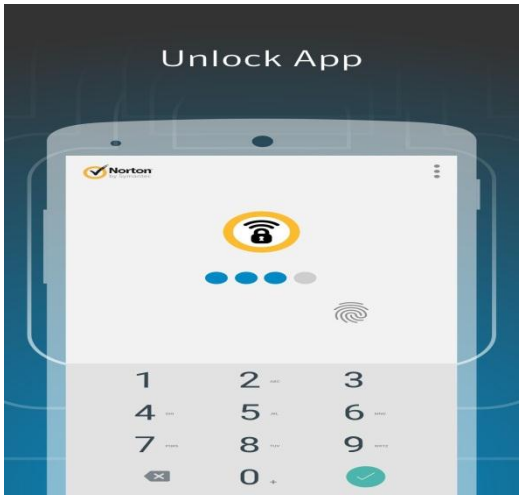
In this paper we will discuss this problem and try to get a solution for this.

2. LITERATURE REVIEW

Much work have been done till date and more is being and to be done to make the data secure in social media. Some of the works that are being used at present time are:

2.1 *PIN:*

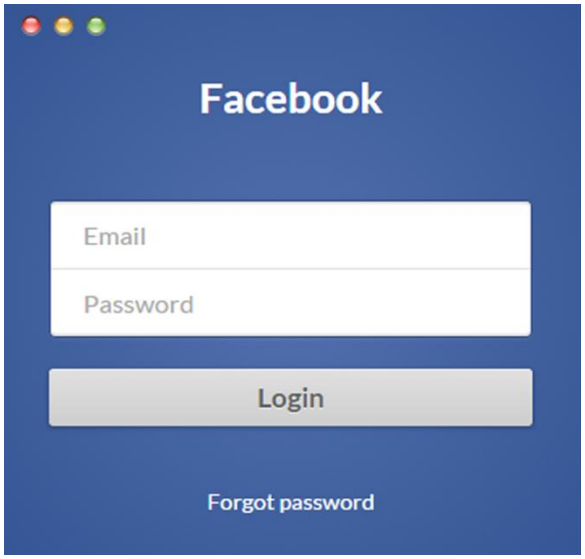
In this method a four digit code is used for security. Many applications are available on internet which helps to set pin and passwords for other apps (includes social media apps). Eg. Norton app lock.



But the problem of this method is that the password can be retrieved by anyone by hit and trial method.

2.2 Password:

To end up this problem password could be used as there is no limitation for number of characters or digits. The password can be created using multiple characters and digits. Many social media websites like facebook, uses login method for security. In this, the user has to enter the loginId (mostly email ID or mobile number) and a password.



2.3 *Encryption:*

Some social media platforms provided encryption for messages. Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Some social media platforms like whatsapp, presently using end-to-end encryption technology. In end-to-end technique, the data sent by the sender moves from sender's end to receiver's end in encrypted mode. The data is decrypted only after the receiver receives it.

3. DRAWBACK

Even after these security options, there is still chances of data theft. Any expert might access to the social media account. Sometimes we intentionally give access to friends or any known person to social media. We want that they access only limited data, or the data that we want to share with them. But at that time, access is in their hands. They can access the account to any extent. At present situation we can't do anything for this. But we can take a step forward to improve security for highly confidential data. In this paper we have discussed a method to secure that "highly confidential" data.

4. THE PROPOSAL SYSTEM

To trounce the above discussed drawback, a technique can be used in which a pin or password could be set for individual/ each chatting, message or post which are highly confidential. This will give a double security to the important data. If anyone gets access to the victim's social media account, even then he/she will not be able to access that data for which another password has been set.

5. CONCLUSION

In this modern and fast growing world, where almost half of the population is active on social media, the security issues can never be ended. But we can reduce the security risks to a minimum level. The above discussed method can be useful to increase security level and can surely make the data more secure.

REFERENCES

[1] International *Journal* Engineering And CS Issuing Date: 03-03-2015, Page No. 10810 to 10814

[2] EsmaAimeur, SebastienGambas, Ai Ho "Towards a Privacy-enhanced Social Networking Site" 2010 International Conference on Availability, Reliability and Security.

[3] Chander Singh, Dr. Devesh Katiyar "Fingerprint Based Security" International journal of scientific research in engineering and management (IJSREM) Volume: 04 Issue: 04|April-2020

[4] https://www.varonis.com/blog/social-media-security/

[5] https://www.smartinsights.com/wp-content/uploads/2019/02/

[6] https://us.norton.com/internetsecurity-privacy-5-tips-for-social-media-security-and-privacy.html

[7] https://apkpure.com/norton-app lock/com.symantec.applock

[8] https://buzzfeedng.com/tech/facebook-com-login-facebook-login-page-facebook-homepage-how-to-facebook-login-with-a-mobile-device/

[9] https://www.businesstoday.in/buzztop/buzztop-feature/how-does-whatsapp-end-to-end-encryption-work/story/307998.html

BIOGRAPHIES

Mr. Chander Singh, he is student of "M.C.A. Department of Computer Science, DSMNRU Lucknow, Uttar Pradesh, India". He has completed B.C.A. from Lucknow University in 2018.

Dr. Devesh Katiyar, he is Assistant Professor at Department of Computer Science, DSMNRU Lucknow, Uttar Pradesh, India". His research areas are: Software Engineering, Data Mining & Data

Mr. Gaurav Goel, he is Assistant Professor at Department of Computer Science, DSMNRU Lucknow, Uttar Pradesh, India". His research areas are: Digital Image Processing, Machine Learning, Wireless Sensor Network, and Artificial Intelligence