IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Social Chat Application Include Security and Detect the Spam Message

Prof. A.A Shitole[1], Sonam H Anpat[2], Pooja N Bodhale[3], Chaitrali B Gaikwad[4]

Professor, Computer Dept, SEC, Pune, India [1]

Student, Computer Dept, SEC, Pune, India [2, 3, 4]

Abstract: On line social networks (osns) have lately emerged united of the most effective channels for info sharing and discovery due to their potential of permitting users to scan and build new content on the equal time. Whereas this advantage affords customers additional rooms to pick that content material to comply with, it conjointly makes osns fertile grounds for the huge spread of data which may also result in undesirable outcomes. in an effort to make certain the trustiness of content sharing in osns, it is so vital to possess a strategic research at the primary and fundamental problem: the assets of statistics. the usage of thoughts in psychology toguage the unfold of information, incorrect information and information in on-line social networks. Analysing on line social networks to spot metrics to deduce cues of deception can trade the USA to stay diffusion of records. the cognition worried inside the name to unfold information involves respondent 4 major queries viz consistency of message, coherency of message consider capacity of supply and widespread acceptableness of message. we have used the cues of deception to analyse those questions to collect answers for stopping the unfold of records. we've got projected an rule to successfully discover deliberate unfold of fake information which might exchange users to create enlightened choices whereas spreading data in social networks. the computationally within your budget rule makes use of the cooperative filtering property of social networks to live the believability of resources of records.

Keywords: Cognitive psychology, Decryption, Disinformation, Encryption, Misinformation, Online Social Network, spam message.

I. INTRODUCTION

Social networks with its freedom of expression, lack of filtering mechanisms like reviewing and enhancing available in conventional publishing enterprise coupled with high degree of lack of responsibility have become an crucial media for spread of misinformation. summarily, the propagation of different variations of information, viz incorrect information, disinformation and propaganda entails the spread of false or misguided data through facts diffusion technique concerning customers of social networks where all the customers may not be aware of the falsehood within the statistics. a social networking provider (additionally social networking site, sns or social media) is an internet platform this is utilized by human beings to construct social networks or social family members with different folks who percentage similar private or profession hobbies, activities, backgrounds or real-life connections.

Depending at the social media platform, contributors can be able to contact some other member. in other cases, participants can contact absolutely everyone they have got a connection to, and sooner or later anybody that contact has a connection to, and so forth. But privateers of customers need to be maintained whilst communicating through social networking services. when users communicate with every different , their message must be secured. in order to keep these privatives, we should evolved such application that is secure to apply. like smart, unwanted message need to be deleted from messages so that it cannot reason harm to person`s privatizes.

II. LITERATURE SURVEY

• M. Shirali-shahreza, "stealth steganography in sms", proceedings of The third ieee and ifip international conference on wireless and optical Communications networks (wocn), april, 2006.
Which utilized image as cover media and Sms as carrier to transfer the hidden message to the recipient. In this method, a black and white (b&w) image is used to Transfer the hidden message by changing the intensity of Pixels. However, low capacity (27 bytes) is the main drawback Of the mentioned technique, due to the use of only black and White image rather than using full colour.

• M. Shirali-shahreza, and m. H. Shirali-shahreza, " text steganography In sms", international conference on convergence information Technology, pp. 2260-2265, 2007.
Exploited abbreviation or full Form of words such as "u" for the meaning of "you", and "univ" for "university" to hide the secret message in the sms. For example, to hide 01, the abbreviation form of the word (u) Is used to embed value 0, whereas the full form (you) is Utilized for embedding value 1. The main limitation of this Method is very low payload capacity and easy extraction.

DOI 10.17148/IJARCCE.2016.51226

- K. F. Rafat, "enhanced text steganography in sms", international Conference on computer, control and communication, pp. 1-6, 2009.

The static form of the word abbreviation list is Removed by introducing computationally light weighted Exclusive or (xor) encryption.

- M. H. Shirali-shahreza, and m. Shirali-shahreza, "sending mobile Software activation code by sms using steganography", third International conference on intelligent information hiding and Multimedia signal processing, 1, pp. 554-557, 2007.

The image is used to hide software activation code Based on the steganography technique proposed and Then send the image to the recipient through sms.

- M. H. Shirali-shahreza, and m. Shirali-shahreza, "steganography in Sms by sudoku puzzle", international conference on computer systems And applications, pp. 844-847, 2008.

The new Method didn't show any significant improvements to their Previous method rather sending activation code. The use of Sudoku game is another interesting technique proposed by this paper.

- Karlova NA, Fisher KE (2013) “Plz RT”: A social diffusion model of misinformation and disinformation for Understanding human information behaviour. Inform Res 18(1):1–17 [3]Stahl BC (2006) on the difference or equality of information, misinformation, and disinformation: A critical research Perspective. Inform Sci: Int J EmergTransdiscipline 9:83–96. [6]Lewandowsky S, Ecker UK, Seifert CM, Schwarz N, Cook J (2012) Misinformation and its correction continued Influence and successful debiasing. PsycholSci Public Interest 13(3):106–131

The difficulties associated with distinguishing between misinformation, disinformation And true information have been highlighted by most of them.

- Ratkiewicz J, Conover M, Meiss M, Goncalves B, Patil S, Flamini A, Menczer F (2010) Detecting and tracking the Spread of astroturf memes in microblog streams. Arxiv preprint arxiv:1011.3768. [8]Ratkiewicz J, Conover M, Meiss M, Goncalves B, Patil S, Flammini A, Menczer F (2011) Truthy: mapping the spread of Astroturf in microblog streams. In: Proceedings of the 20th International Conference Companion on World wide Web. ACM, Hyderabad, India, pp 249–252

The Cognitive factors which decide the credibility of messages and their consequent acceptance by users can be effectively modulated INOSNS as seen during US elections.

- Lewandowsky S, Ecker UK, Seifert CM, Schwarz N, Cook J (2012) Misinformation and its correction continuedinfluence and successful debiasing. PsycholSci Public Interest 13(3):106–131

Significant contributions towards successful debiasing of misinformation

- Mendoza M, Poblete B, Castillo C (2010) Twitter under crisis: Can we trust what we RT? In: Proceedings of the First Workshop on Social Media Analytics. ACM, 2010: Washington DC, USA, pp 71–79

Reliability of Twitter under extreme circumstances

- J. Singh, R. Ruhl, and D. Lindskog, " Secure GSM OTA SIM cloning attack and cloning resistance in EAP- SIM and USIM ", International Conference on Social Computing (SocialCom), pp. 1005–1010, 2013.

Phone Cloning allows an attacker to intercept incoming messages and send outgoing messages as though the phone is the original one.

III. EXISTING SYSTEM

1) In existing system we can see that there are too many spam or unwanted messages comes into our inbox. For ex. in whatsapp, some unwanted messages send by users which we don’t want to read or save. There is a no option to automatically remove a message and images.

2) In another scenario, sender sends a message to receiver/recipient and receiver/recipient read it. There is a no any mechanism to decrypt a message at receiver side.

IV. ARCHITECTURE DIAGRAM

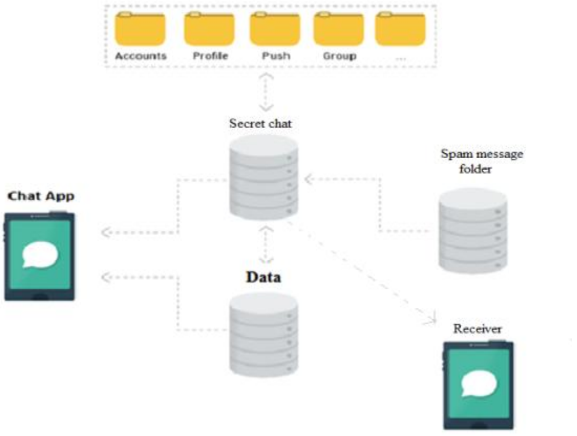

Fig: Social chat

V. PROPOSED SYSTEM

1) We develop a system which detect and remove a spam or unwanted messages, images automatically without disturbing user. System detects a spam messages and send it into spam folder. User don’t waste time for removing these data and also save the time of user.

2) Second main purpose of these system is, provide a two way authentication for users when they communicate. For ex. when a sender wants to send a message to another user

DOI 10.17148/IJARCCE.2016.51226

then he/her encrypts a message with his/her own private key and send to receiver. If receiver has private key which provided by the sender then only he/her can decrypt it.

Advantages:

1) Security: provides a strong authentication for both users.
2) Automatically removes a spam/unwanted messages so it's less time consuming.
3) Save storage space of device.

VI. CONCLUSION

We will develop a chat application which provides function like strong securities as well as removing spam/unwanted messages.

REFERENCES

[1] M. Shirali-shahreza, "stealth steganography in sms", proceedings of The third ieee and ifip international conference on wireless and optical Communications networks (wocn), april, 2006.

[2] M. Shirali-shahreza, and m. H. Shirali-shahreza, " text steganography In sms", international conference on convergence information Technology, pp. 2260-2265, 2007.

[3] K. F. Rafat, "enhanced text steganography in sms", international Conference on computer, control and communication, pp. 1-6, 2009.

[4] M. H. Shirali-shahreza, and m. Shirali-shahreza, "sending mobile Software activation code by sms using steganography", third International conference on intelligent information hiding and Multimedia signal processing, 1, pp. 554-557, 2007.

[5] M. H. Shirali-shahreza, and m. Shirali-shahreza, "steganography in Sms by sudokupuzzle", international conference on computer systems And applications, pp. 844-847, 2008.

[6] N. P. Nguyen, G. Yan, M. T. Thai, and S. Eidenbenz, "Containment of viral spread in online social networks," in WEBSCI, 2012.

[7] T. N. Dinh, D. T. Nguyen, and M. T. Thai, "Cheap, easy, and massively effective viral marketing in social networks: Truth or fiction?," in Hypertext, 2012.

DOI 10.17148/IJARCCE.2016.51226