ADVANCE ANDROID BASED CHAT APPLICATION USING DATA MINING TECHNIQUES

[1]syeole196@gmail.com
[2]prafulla.wagh@yahoo.com
[3]nikhilsomani29@gmail.com
[4]roshanwakode159@gmail.com

[1]Bachler of engineering , Computer, Sinhgad College of engineering vadgoan, Maharastra, India
[2]Bachler of engineering , Computer, Sinhgad College of engineering vadgoan, Maharastra, India
[3]Bachler of engineering , Computer, Sinhgad College of engineering vadgoan, Maharastra, India
[4]Bachler of engineering , Computer, Sinhgad College of engineering vadgoan, Maharastra, India

ABSTRACT

online social networks have recently emerged as one of the most effective channels for information sharing and discovery due to their ability of allowing users to read and create new content simultaneously. while this advantage provides users more rooms to decide which content to follow, it also makes OSNS fertile grounds for their wide spread of misinformation which can lead to undesirable consequence . In order to gaurantee the trust worthiness of content sharing in OSNS, it is thus essential to have a strategic investigation on first and foremost concern the sources of misinformation.

The paper explores the use of concepts in cognitive psychology to evaluate the spread of misinformation, disinformation and propagana in online socialnetworks. Analysing online social networks to identify metrics to infer cues of deception will enable us to measure diffusion of misinformation. We have used to cues of deceptioin to analyse these quetions to obtain solutions for preventing the spread of misinformation. This system have proposed an algorithm to efficiency deliberate spread of false information which would enable users to make informed decisions while spreading information in social networks.

I INTRODUCTION

Social networks with its freedom of expression, lack of filtering mechanisms like reviewing and editing available in traditional publishing business coupled with high degree of lack of accountability have become an important media for spread of misinformation.

A social networking service (also social networking site, SNS or social media) is an online platform that is used by people to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections. Depending on the social media platform, members may be able to contact any other member. In other cases, members can contact anyone they have a connection to,

and subsequently anyone that contact has a connection to, and so on. But privacy of users should be maintained while communicating through social networking services. When users communicate with each other , their message should be secured. In order to maintain these privacy, we have to developed such application which is safe to use. Like wise, unwanted message should be deleted from messages so that it cannot cause harm to user's privacy

II LITERATURE SURVAY

On using Emoticons and Lingoes for Hiding Data in SMS, 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET) 2015. - An investigation on the suitability of hiding secret message in SMS.The hidden data are represented as lingoes and emoticons which are frequently used by users in SMS and chat. Sources of Misinformation in Online Social Networks: Who to suspect? 847, 2014. - The Aims to identify the top k most suspected sources of misinformation. two effective approaches namely ranking-based and optimization-based algorithms. to cope with the incompleteness of collected data as well as multiple attacks, which mostly occur in reality.

Detecting misinformation in online social networks using cognitive psychology april, 2006. -evaluates the spread of misinformation, disinformation and propaganda in online social networks. 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) Isused to embed value0, where as the full form(you)is Utilized for embedding value 1. The main limitation of this Method is very low payload capacity and easy extraction. 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. 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 Emerg Transdiscipline 9:83–96. [6]Lewandowsky S, Ecker UK, Seifert CM, Schwarz N, Cook J (2012) Misinformation and its correction continued Influence and successful debiasing. Psychol SciPublicInterest13(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 USelections.

III EXISTING SYSTEM

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. 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 PROPOSED SYSTEM

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.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 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.

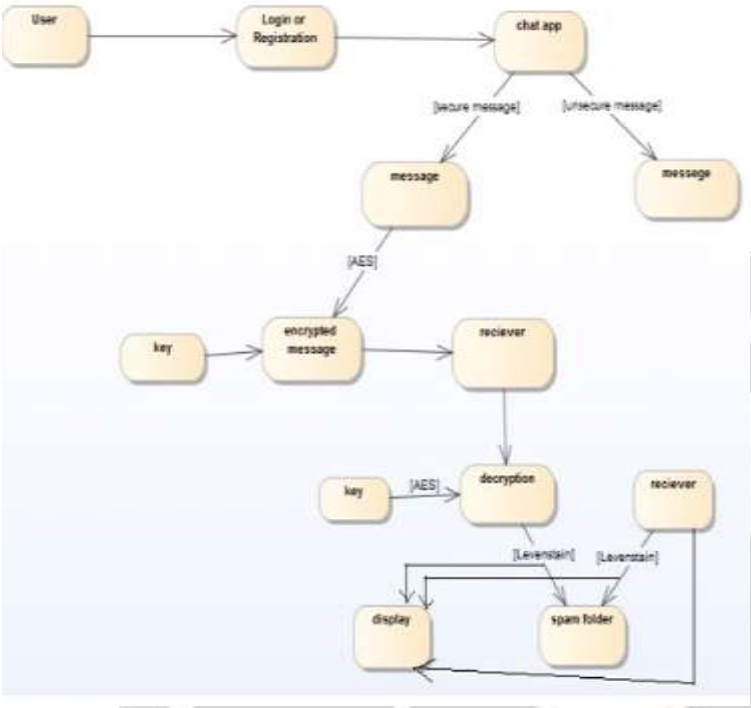

Fig. Architecture Diagram

Module description:

We use AES algorithm for encryption and decryption of messages . we give chance to the user for encryption and decryption of messeges by using key.We use Lavenstein algorithm for spam removal.

User
user can chat with other user .The chat may be normal or encrypted.For spam removal user can add his own words in interactive page and if some another user send message and if that message contains that word in interactive page then that word go in spam folder.

Database
Database contain the user information like name,phone no ,emailid,user chat.

Server
we use wamp sever here. Device and sever can be connected with each other with the help of internet nwtwork.

V METHOD

AES algorithm:

In project, AES algorithm is used for encrypt the message using private key and decrypt the message using same key. AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). The features of AES are as follows • Symmetric key symmetric block cipher • 128-bit data, 128/192/256-bit keys • Stronger and faster than Triple-DES • Provide full specification and

design details • Software implementable in C and Java AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Inproject,Levenshteindiatancealgorithmisusedforpatternmatchingandisusedtocountand measure the number of iterations required to convert one string to another.i.e. two strings will be match for spam identifying purpose. Levenshtein distance (LD) is a measure of the similarity between two strings, which we will refer to as the source string (s) and the target string (t).

levenshtein (source, target : STRING): INTEGER – Minimum number of operations to turn source into target local distance : ARRAY2[INTEGER]

i, j,del,ins,subst :INTEGER

do

createdistance.make(source.count,target.count)

fromi:= 0untili > source.countloop

distance[i,0] := i;i:= i+1

end

fromj := 0untilj >target.countloop

distance[0, j] := j; j := j+1

end

fromi:= 1untili > source.countloop

fromj := 1untilj >target.countinvariant

loop if source [i] = target [j] then distance [i, j] := distance [i -1, j -1] else deletion := distance [i -1, j]

SCOE, Dept. of Computer Engineering 19 Year 2016-17

insertion := distance [i , j - 1] substitution := distance [i - 1, j - 1] distance [i, j] := minimum (deletion, insertion, substitution) + 1 end j := j + 1 end i := i + 1 end Result := distance (source.count, target.count) End.

VI CONCLUSION

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

VII ACKNOWLEDGEMENT

Every work is source which requires support from many people and areas. It gives us proud privilege to partially complete the project "ADVANCE ANDROID BASED CHAT APPLICATION USING DATA MINING TECHNIQUES " under valuable guidance and encouragement of my guide Prof. T.P. Vaidya. I am extremely grateful to our respected H.O.D.(Computer Dept.) Prof. M. P. Wankhade for providing all facilities and every help for smooth progress of seminar. I would like to thank all the Staff Member of Computer Engineering Department for timely help and inspiration for completion of the seminar.

VIII REFRENCES

[1] M.Shirali-shahreza,"stealthsteganographyinsms",proceedingsofThethirdieeeandifip international conference on wireless and optical Communications networks (wocn), april, 2006.M.

[2] 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,andm.Shirali-shahreza,"sendingmobileSoftwareactivationcode bysmsusingsteganography",thirdInternationalconferenceonintelligentinformationhiding and Multimedia signal processing, 1, pp. 554-557, 2007.

[5] 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.

[6]N.P.Nguyen,G.Yan,M.T.Thai,andS.Eidenbenz,"Containmentofviralspreadinonline 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.