iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 5 **Issue:** VII **Month of publication:** July 2017

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887*
*Volume 5 Issue VII, July 2017- Available at www.ijraset.com*

# Social Network Security Based on Trust Agent and Behavior Induction

Sushma.V[1], Chandrashekhar B.N[2], Dr Sanjay H.A[3]
[1] *MTech,,* [2]*Assistant Professor,* [3]*Professor and HOD, Department Of Information And Science*
*Nitte Meenakshi Institute Of Technology, Bangalore 560 064, Karnataka, India.*

***Abstract:*** ***Social networks are a kind of societal structure that consists of multiple nodes and the relationships among them. Through these relationships, social networks connect all kinds of participants, from casual speaking acquaintances to closely related family members. But while online social networks bring convenience to modern life, they can have negative effects as well. In politics, for example, rumors could be produced and spread on social networks that lead to incidents affecting societal stability; similarly, in e-commerce, false information can be spread over social networks that deceive customers in online shopping platforms. Porn is often distributed via social video sharing and instant messaging platforms, and terrorists have adopted social networks to persuade teenagers to take part in their illicit activities. One way to counter these malicious behaviors is to introduce behavior induction, a process in which a person or group influences the behavior of another person or group through the induction of behavioral attitudes.***
***Keywords: Electronic Commerce(e-commerce), Balanced Incomplete Block Design(BIBD), Transmission Control Protocol(TCP), User Datagram Protocol(UDP).***

## I. INTRODUCTION

There are all kinds of interaction relations between participants in social networks but the most important one is trust. Trust is the measure taken about the acceptance of another party
which is able to perform the act of another party in which the situation of a certain trust value will perform the range[0,1] where one party can take the probability
The issue of the trust which has gained much attention in the field of information technology, researchers mainly focus on a target of entitys security, the relation between participants and the influence on trust relation. The main goal is to obtain the objective results about effective approaches.Trust agents social features can be selected according to participants social features. This encourages participants to trust the agents and then follow the agents designed behaviours.
Social features can describe a context where a participants of social environment will be specified for a particular social environment into independent and dependent social features.
Participants independent social features refer to the personal characteristics which influence his or her interactions, trust and recommendations they typically include the preference and the main role of the impact factor. In social networks the participants can be arranged according to different domains based on the characteristics, the role impact factor is also considered. For example the behavior of a person has experience in a particular domain is more trustworthy than the other who has no knowledge in it.
Some social networks consider only dependent social features such as anonymous social networks which can be called behavior feature-driven social networks some social networks consider both independent and dependent social features which is known as mixed feature-driven social networks.

## II. MODULE DESCRIPTION

### *A. Behavior Induction in Social Networks*

Cloud computing has many security problems to deal with. This project is based on proxy cryptography research results, remote data integrity checking in public cloud and identity-based public key cryptography. In few cases, the cryptographic operation will be dealing with the third party, for example proxy. Here proxy cryptography should be used. Proxy cryptography is important cryptography type. Proxy cryptosystem was proposed by Mmbo et al. in 1996. When the bilinear pairings are considered into the identity-based cryptography, this cryptography becomes efficient and practical. Identity-based cryptography becomes more efficient as it avoids the certificate management, due to this more and more experts will prefer to study identity-based proxy cryptography. An ID-based proxy signature scheme was proposed by Yoon et al. in 2013 with message recovery . Chen et al. demonstrated a proxy signature scheme and a threshold proxy signature scheme using the Weil pairing. Further by combining the proxy cryptography with encryption technique, few proxy re-encryption schemes are proposed. Liu et al.

demonstrated a attribute-based proxy signature. Guo et al. presented a non-interactive CPA(chosen-plaintext attack) which is a secure proxy reencryption scheme, that is resistant to collusion attacks in forging re-encryption keys.

### *B. Trust Agent Feature Selection*

Recent years have witnessed the increased popularity of mobile messaging Apps, such as WeChat and WhatsApp. Indeed, messaging Apps have become the hubs for most activities of mobile users. For example, messaging Apps help people text each another, share photos, chat, and engage in commercial activities such as paying bills, booking tickets and shopping. Mobile companies monetize their services in messaging Apps. Therefore, service usage analytics in messaging Apps becomes critical for business, because it can help understand in-App behaviors of end users, and thus enables a variety of applications. For instance, it provides in-depth insights into end users and App performances, enhances user experiences, and increases engagement, conversions and monetization. However, a key task of in-App usage analytics is to classify Internet traffic of messaging Apps into different usage types as shown in Table Traditional methods for traffic classification rely on packet inspection by analyzing the TCP or UDP port numbers of an IP packet or reconstructing protocol signatures in its payload For example, an IP packet usually has five tuples of protocol types, source address and port, destination address and destination port. People estimate the usage types.

### *C. Trust Agent-Based Behavior Induction*

Second, a traffic-flow of M observations (packets in this study) usually contains two sequences: an M size sequence of packet lengths representing the data transmission of service usages and an (M-1)-size sequence of time delays representing the time intervals of consecutive packet pairs. In terms of the packet length, as shown in, different service usages have different global characteristics (e.g., distribution properties such as mean and variance of packet lengths, etc.) and local characteristics (e.g., packet-level features such as forward or backward variances at important observation positions, etc.). For example, texts are more frequently used, shorter in time, and smaller in data size comparing to stream video call, therefore any traffic intervals with flow rate lower than certain thresholds are likely determined as text streams. Aside from global characteristics, local (i.e., packet-level) characteristics are from the fact that the packet lengths of different usage types vary over observation positions in the sequence of packet lengths. For example, shows the process that a mobile user sends out a text message, and thus generates a pulse in traffic, followed by another pulse representing a text reply. Also, Figure shows that, in stream video call, most packets are fully loaded (i.e., close to 1500 bytes) in the sequence of packet lengths. In terms of time delay, different in-App usages adopt different design logics and control flows for function implementation and different network protocols for packet transmission, and thus show unique characteristics of time delay distribution. For example, shows that, for location sharing, most of packets are sent in the initial phase. However, for short video, data transmission is completed.

### *D. Symmetric Key Distribution Method*

Balanced incomplete block design (BIBD) is a combinational design methodology which is used in key pre-distribution schemes. BIBD will arrange v distinct key objects of a key pool into b different blocks where each block will represent a key ring assigned to a node. In this design each BIBD design is expressed with a quintuplet where v is the number of keys, k is the number of keys in each key ring, r is the number of nodes sharing a key, b is the number of key rings. Each pair of distinct keys occur together in exact blocks. Further, BIBD design can be expressed with the equivalent tuple as it always holds with the relationship.

## II. ARCHITECTURE DIAGRAM

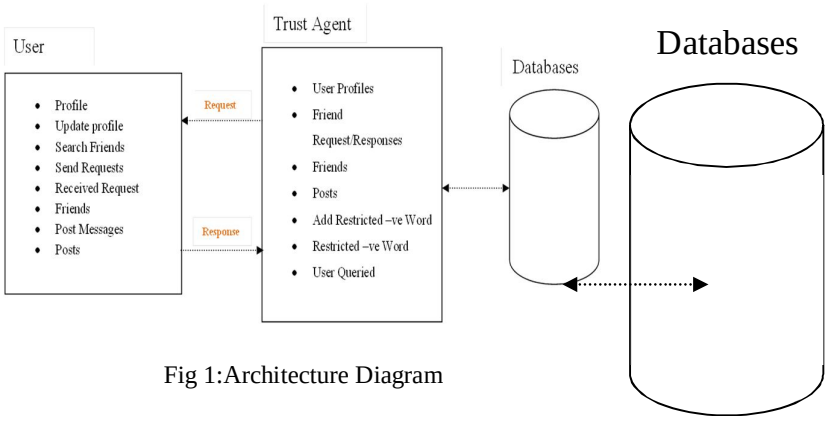



Fig 1:Architecture Diagram

The implementation of architecture diagram states that all the information of the user and the trust agent will be stored in a database. It consists of all the data which is created by the user and also the trust agent. The user accepts the request which is obtained from the trust agent where it will be in a waiting state then thuser responds to the trust agent and then the waiting state will be converted to authorized that means the request is accepted and responded by both user and trust agent.

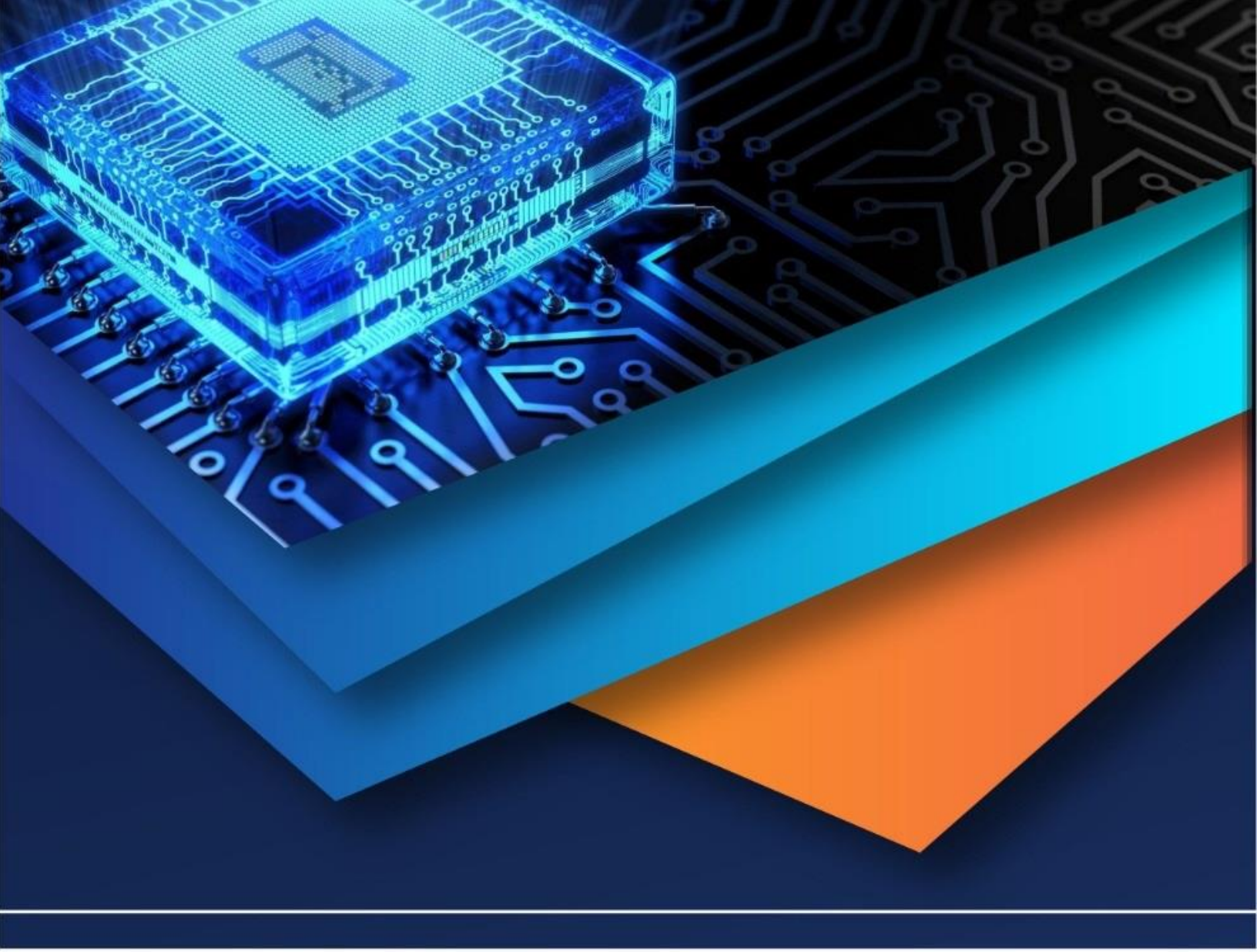
Restricted words must be added to the trust agent where it avoids all the restricted words and the bad comments which will not be displayed and also informs that these are the words which are not used by the servers.

## III. CONCLUSION

The attacks that are demonstrated will raise a number of questions which are important, about the level of privacy that users can expect from these services. Exact plaintext content cannot be revealed, the results obtained in the project indicate that rich metadata can be learned about a user and their social network with high accuracy. At the same time, a closed-world study should be considered, as it is believed that it realistically represents a serious privacy threat, there are aspects of real world usage that may impact the results, such as texting shorthand or previously unobserved languages. In the recent research of widespread metadata gathering and given the unusually broad impact of these attacks on an international user base, it looks reasonable to consider that the issues raised in this paper pose a realistic threat that should be taken seriously by messaging services.

## REFERENCES

[1] A. Mislove et al., "Measurement and Analysis of Online Social Networks," Proc. Internet Measurement Conf.,2007,pp.29-42.
[2] X. Cheng et al., "BTM: Topic Modeling over short Texts," IEEE Trans. Knowledge Data Eng., vol. 26,no. 12, 2014,pp. 2928-2941.
[3] M. Jiang et al., "Inferring Lockstep Behavior from Connectivity Pattern in Large Graphs," Knowledge Information Systems: An Int'l j., vol.45,no.3, 2015;doi:10.1007/s10115-015-0883-y.
[4] P.-R. lei, " A Framework for Anomaly Detection in Maritime Trajectory Behavior," Knowledge Information Systems: An Int'l j., vol. 45 , no.3,2015; doi:10.1007/s10115-015-0845-4.
[5] F.D. Malliarors, V. Megalooikonomou, and C. Faloutsos, "Estimating Robustness in Large Social Graphs," Knowledge Information Systems, vol.45,no. 3,2015, pp. 645-678.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)