# Securing Cloud Data under Key Exposure

M Somasekhar[1], Prof. Abdul Baki[2]

***Abstract*- Social networks area unit a form of social group structure that consists of multiple nodes and therefore the relationships among them. Through these relationships, social networks connect all types of participants, from casual speaking acquaintances to closely related family members. However whereas on-line social networks bring convenience to fashionable life, they'll have negative effects yet. In politics, as an example, rumors might be made and unfold on social networks that cause incidents affecting social group stability; similarly, in e-commerce, false info may be touch social networks that deceive customers in on-line looking platforms. porn is commonly distributed via social video sharing and instant messaging platforms, and terrorists have adopted social networks to influence teenagers to take half in their illicit activities. a way to counter these malicious behaviors is to introduce behavior induction, a method during which a person or group influences the behavior of another person or cluster through the induction of behavioral attitudes.**

***Index Terms*- Electronic Commerce (e-commerce), Balanced Incomplete Block Design(BIBD), Transmission Control Protocol(TCP), User Datagram Protocol(UDP).**

## INTRODUCTION

There is a unit all types of interaction relations between participants in social networks however the foremost vital one is trust. Trust is the live taken regarding the acceptance of another party which is in a position to perform the act of another party true of a precise trust price can perform the range [0,1] where one party will take the chance The issue of the trust that has gained a lot of attention within the field of data technology, researchers in the main concentrate on a target of entities security, the relation between participants and also the influence on trust relation. the most goal is to get the target results regarding effective approaches. Trust agents social options may be elite in keeping with participant social options. This encourages participants to trust the agents so follow the agents designed behaviors. Social options will describe a context wherever participants of social atmosphere are given for a selected social environment into freelance and dependent social options. Participant's freelance social options talk to the private characteristics that influence his or her interactions, trust and recommendations they usually embody the preference and also the main role of the impact issue. In social networks the participants may be organized in keeping with completely different domains supported the characteristics, the role impact issue is additionally considered. as an example the behavior of someone has expertise in a very specific domain is a lot of trustworthy than the opposite UN agency has no data in it. Some social networks think about solely dependent social options like anonymous social networks which may be known as behavior feature-driven social networks some social networks think about each freelance and dependent social options that is understood as mixed feature-driven social networks.

## PROPOSED SYSTEM

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 encryption 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 We Chat 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 represents 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.

ARCHITECTURE DIAGRAM

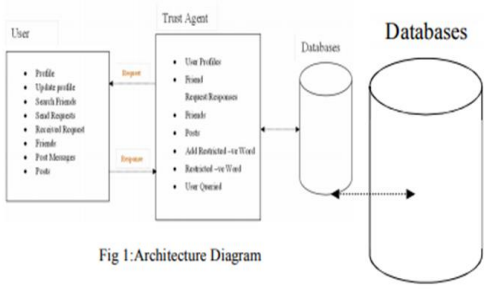


Fig 1:Architecture Diagram

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 these responds to the trust agent and then the waiting state will be converted to authorize 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.

## CONCLUSION

Social networks are a sort of social group structure that consists of multiple nodes and also the relationships among them. Through these relationships, social networks connect all types of participants, from casual speaking acquaintances to closely related members of the family. However whereas on-line social networks bring convenience to modern life, they'll have negative effects moreover. In politics, for instance, rumors may be made and unfold on social networks that cause incidents affecting social group stability; equally, in e-commerce, false info is contact social networks that deceive customers in on-line shopping platforms. Creative activity is often distributed via social video sharing and instant messaging platforms and terrorists have adopted social networks to steer teenagers to require half in their illicit activities. a method to counter these malicious behaviors is to introduce behavior induction, a method during which someone or cluster influences the behavior of another person or cluster through the induction of activity attitudes.

## REFERENCES


[1] Albert, R., Barabasi, A.: Statistical mechanics of complex networks. Reviews of Modern Physics 74(1), 47-97 (2002).

[2] Garton, L., Haythornthwaite, C., Wellman, and B.: Studying online social networks. Journal of Computer-Mediated Communication 3(1) (1997).

[3] Ye, S., Lang, J., Wu, and F.: Crawling Online Social Graphs. In: Proc. of the 12th International Asia-Pacific Web Conference, pp. 236-242. IEEE (2010).

[4] Kleinberg, J.: The small-world phenomenon: an algorithm perspective. In: Proc. of the 32nd annual symposium on Theory of computing, pp. 163-170. ACM (2000).

[5] Gjoka, M., Kurant, M., Butts, C., Markopoulou, and A.: Walking in Face book: a case study of unbiased sampling of OSNs. In: Proc. of the 29th conference on Information communications, pp. 2498-2506. IEEE (2010)

[6] Mislove, A., Marcon, M., Gummadi, K., Druschel, P., Bhattacharjee, and B.: Measurement and analysis of online social networks. In: Proc. of the 7th SIGCOMM conference on Internet measurement, pp. 29-42. ACM (2007)

[7] Han, J., Kamber, M., Pei, J.: Data mining: concepts and techniques. Morgan Kaufman Pub (2011)

[8] Adamic, L., Adar, E.: Friends and neighbors on the web. Social networks 25(3), 211-230 (2003)

[9] Blondel, V., Gajardo, A., Heymans, M., Senellart, P., Van Dooren, P.: A measure of similarity between graph vertices: Applications to synonym extraction and web searching.Siam Review pp. 647-666 (2004)

[10] Jeh, G., Widom, and J.: Simrank: a measure of structural-context similarity. In: Proc. Of the 8th SIGKDD international conference on Knowledge discovery and data mining, pp. 538-543. ACM (2002)

[11] Batagelj, V., Doreian, P., Ferligoj, A.: An optimization approach to regular equivalence .Social Networks 14(1-2), 121-135 (1992)

[12] Blondel, V., Gajardo, A., Heymans, M., Senellart, P., Van Dooren, P.: A measure of similarity between graph vertices: Applications to synonym extraction and web searching.Siam Review pp. 647-666 (2004) network. In: Proc. of the 2nd International Conference on Social Computing, pp. 249-256 (2010)

[13] Mislove, A., Marcon, M., Gummadi, K., Druschel, P., Bhattacharjee, B.: Measurement and analysis of online social networks. In: Proc. of the 7th SIGCOMM conference on Internet measurement, pp. 29-42. ACM (2007)

Author's Profile:
Mr. M.Abdul Baki working as an Assoc.professor in Emeralds Advanced institute of computer since, Tirupati, A.P.
T. Jyotheeshreceived the PG degree from Sri Venkateswara College of Engineering& Technology,Chittoor, A.P.
K. Sudhakar received the PG degree from Sri Venkateswara College of Engineering & Technology, Chittoor, A.P