ISSN: 2321-7782 (Online)
Volume 3, Issue 9, September 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Security on Mobile Social Networks

A. Vijaya Lakshmi[1]
Research Scholar, Department of Computer Science,
St. Joseph's College(Autonomous),
Trichirappalli, Tamil Nadu, India

Dr. S. Britto Ramesh Kumar[2]
Assistant Professor, Department of Computer Science,
St. Joseph's College(Autonomous),
Trichirappalli,Tamil Nadu, India

P. Joseph Charles[3]
Assistant Professor, Department of Information Technology,
St. Joseph's College(Autonomous),
Trichirappalli,Tamil Nadu, India

Abstract: ***The Mobile Social Networks (MSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of internet users. These MSNs offer attractive means for digital social interactions and data sharing, but also raise a number of issues on security and privacy. While MSNs allow users to restrict access shared data, they currently do not provide any mechanism to enforce security and privacy concerns over data associated with multiple users. Social Networks (SN) Sites are becoming very popular and the number of users is increasing rapidly. As the same as what people usually experience in the daily life, the social relationship in cyberspaces are potentially formed by OSN users' shared attributes, e.g., colleagues, family members, or classmates, which indicates the attribute-based recommendation process would lead to more fine grained social relationships between strangers. It is achieved by using DES Algorithm with MD5 hash.***

Keywords: Security, Privacy, Social Networks, Mobile Social Networks, Data Encryption Standard (DES), Message Digest 5 (MD5).

I. INTRODUCTION

A social network is a social structure made up of a set of social actors (such as individuals or organizations) and a set of the dyadic ties between these actors. The social network perspective provides a set of methods for analysing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures. The study of these structures uses social network analysis to identify local and global patterns, locate influential entities, and examine network dynamics. In recent years, mobile social networks (MSNs) have dramatically expanded in popularity around the world. Many schools have implemented online alumni directories which serve as makeshift social networks that current and former students can turn to for career advice. However, these alumni directories tend to suffer from an oversupply of advice-seekers and an under supply of advice providers. One new social networking service, Ask-a-peer, aims to solve this problem by enabling advice seekers to offer modest compensation to advisers for their time.

II. LITERATURE SURVEY

Aaron et al. **[1]** proposed Secure Social Aware: A Security Framework for Mobile Social Networking Applications in which he presented a framework called SSA, it allows for the interaction of social network information with real-world location-based services without compromising user privacy and security. Through exchanging an encrypted nonce (EID) associated with a verified user location, SSA allows location based services to query the local area for social network information without disclosing user identity or any set of information which could be positively matched to users.

Anna et al. **[2]** proposed PriMa, an effective security and privacy protection mechanism for social networks. PriMa (Privacy Manager) automatically generates access rules for users profile information. PriMa access rules are generated on the basis of users' privacy preferences on their profile data, the sensitivity of the data with respect to the privacy settings of the user such as his privacy preferences for his profile data and the degree to which his profile data is at a risk of being exposed to others, and the risk of disclosing such data to other users.

Hongxin et al. **[3]** have proposed a novel solution for Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks. A systematic conflict detection and resolution mechanism is addressed to cope with privacy conflicts occurring in collaborative management of data sharing in OSNs. Conflict resolution approach balances the need for privacy protection and the user's desire for information sharing by quantitative analysis of privacy risk and sharing loss.

Philip et al. **[4]** devised a model for Preventing Sybil Attacks by Privilege Attenuation for Social Network Services. The Static policy analysis is for verifying if a Face book-style Social Network Services (FSNSs) is Principle of Privilege Attenuation (POPA) compliant. To prevent unprivileged users from colluding with one another to gain access, Denning advocates the Principle of Privilege Attenuation (POPA). Denning's Principle of Privilege. Attenuation (POPA) is formalized as a run-time property, and demonstrated as a necessary. It is a sufficient condition for preventing the Sybil attacks. To prevent Sybil attacks, a group of unprivileged users cannot collude to gain privilege.

Gilbert et al. **[5]** introduced a Practical Attack to DeAnonymize Social Network Users that exploits group membership information that is available on social networking sites. There exists some kind of hierarchy within a group. That is, particular members can hold the role of administrators or moderators, which grants them some special privileges. To determine the group membership of a user, web browser history stealing attacks is used. Thus, whenever a social network user visits a malicious website, this website can launch deanonymization attack and learn the identity of its visitors. The information about the group memberships of a user is sufficient to uniquely identify the user.

Lujun et al. **[6]** introduced security and privacy wizards for social networking sites [21]. The goal of the Wizard is to automatically configure a user's privacy settings with minimal effort from the user. Ideally, the wizard should satisfy the following requirements: Low Effort, High Accuracy. A generic framework is developed for the design of a privacy wizard. . This type of interaction is ideal for non-technical users, who have difficulty reasoning holistically about their policy configurations.

Hassan et al. **[7]** have proposed a process towards active detection of identity clone attacks on online social networks. A new attack called Identity Cloning Attack (ICA), which focuses on forging user profiles on OSNs, has been introduced. In this attack, the adversary first tries to find the ways to obtain a victim's personal information, such as name, location, occupation and friends list from his public profile on OSNs or his personal home pages.

III. PROPOSED ARCHITECTURE FOR SECURITY ON MOBILE SOCIAL NETWORK

In a centralized MSN architecture, a centralized server is used to exchange, share, and deliver data between content provider and mobile users. This is a client–server structure in which the mobile user is the client and the centralized server of the content provider is the server. The content created by the content provider is injected to the mobile users via the server. The mobile users can also update and share the content with other users in the MSN via the centralized server. The protocols required by the mobile users and the centralized server are also indicated. The data flow can be via third party application or content provider using Internet services. In this case, third party application may have different services (e.g., map, social networking, and video sharing services). Almost all of the mobile applications used to access the online social networking sites (e.g., Face book) are based on this centralized architecture.

A centralized architecture forms the basis for web based MSN where the mobile users depend on content providers updates (e.g., Facebook server). Designing efficient and effective MSN architecture has always been the focus of the research

community. For example, a general architecture capable of supporting both indoor and outdoor positioning of mobile users in the MSN is proposed using Wi-Fi and cellular networks. The proposed architecture uses mash up (i.e., interconnection of various online social web services) of web services and hence can be easily integrated with the available networks. The middleware service runs on a centralized sever providing simple application programming interface (API) for mobile clients which can interact with the services over the Internet. Similarly, the middleware framework called "RoadSpeak" is proposed for vehicular social networks to provide virtual chat groups for people driving on the road. The idea is to facilitate better communication among people who are physically present in the vicinity but are unable to communicate directly. This overlay middleware runs on a centralized server to manage the profile and activity of the mobile users. The advantages of a centralized architecture include the simplicity of service implementation and the high efficiency of centralized control. However, similar to a client–server structure, a centralized MSN architecture may have a single point of failure and may experience congestion at the server when a large number of mobile users access the services at the same time. MSN is a user-centric mobile communications system in which the methods of social network analysis (SNA) can be applied to analyze the structure and ties among mobile users with the objective of improving the efficiency of publishing and sharing information. The social relationship can be defined by using different social network metrics. Mobility can be used as additional information to analyze the social relationship among mobile users. These social network metrics provide new insights and understanding of social relationship and the interdependencies within the network.

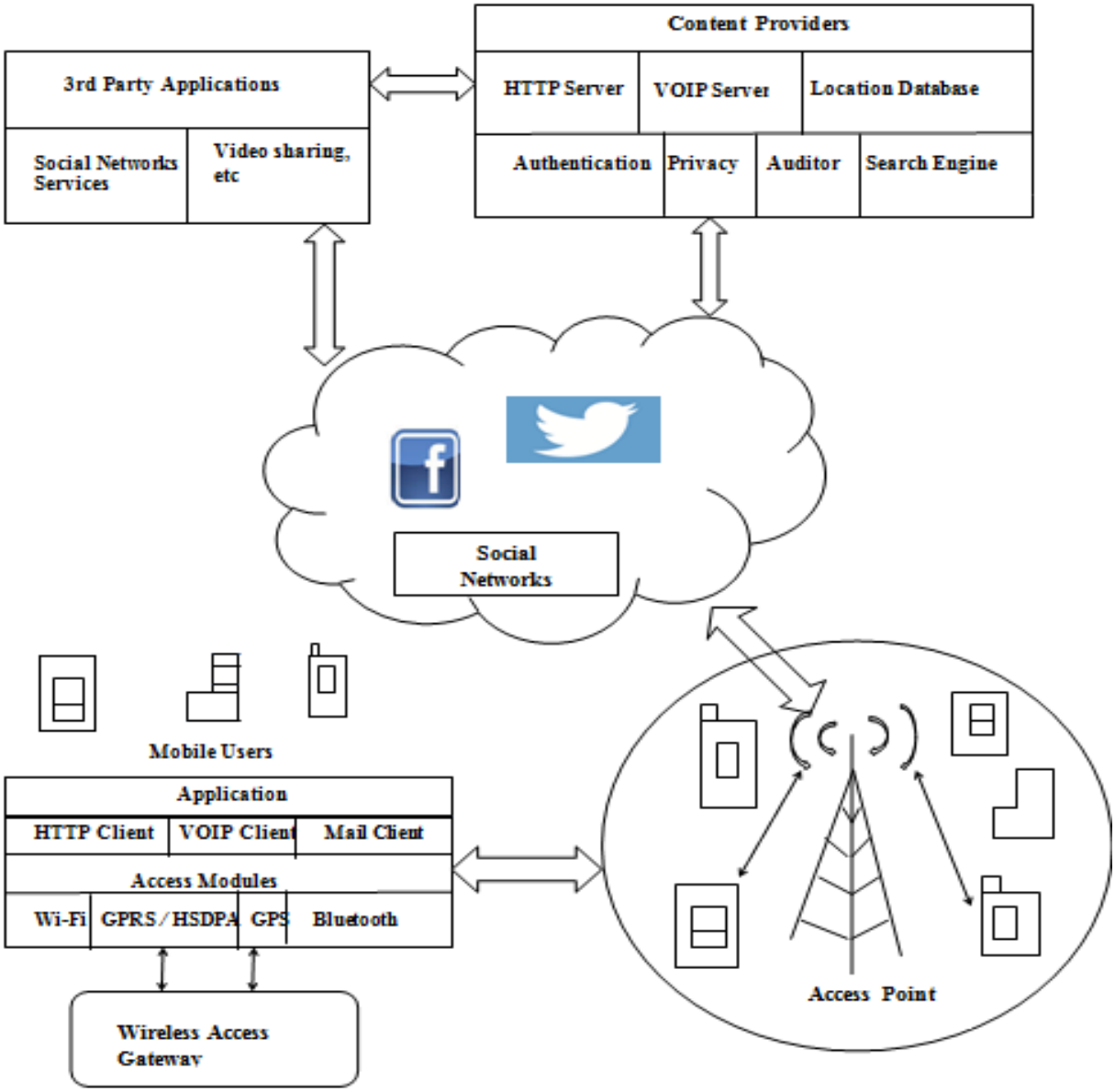

Fig. 1 Architecture for Security on Mobile Social Networks

IV. IMPLEMENTATION

After logging in to the account successfully, users should provide their own unique key to use the various features of framework such as send message to particular user, etc. In order to get the unique key the user need to click on the send message button on the screen.

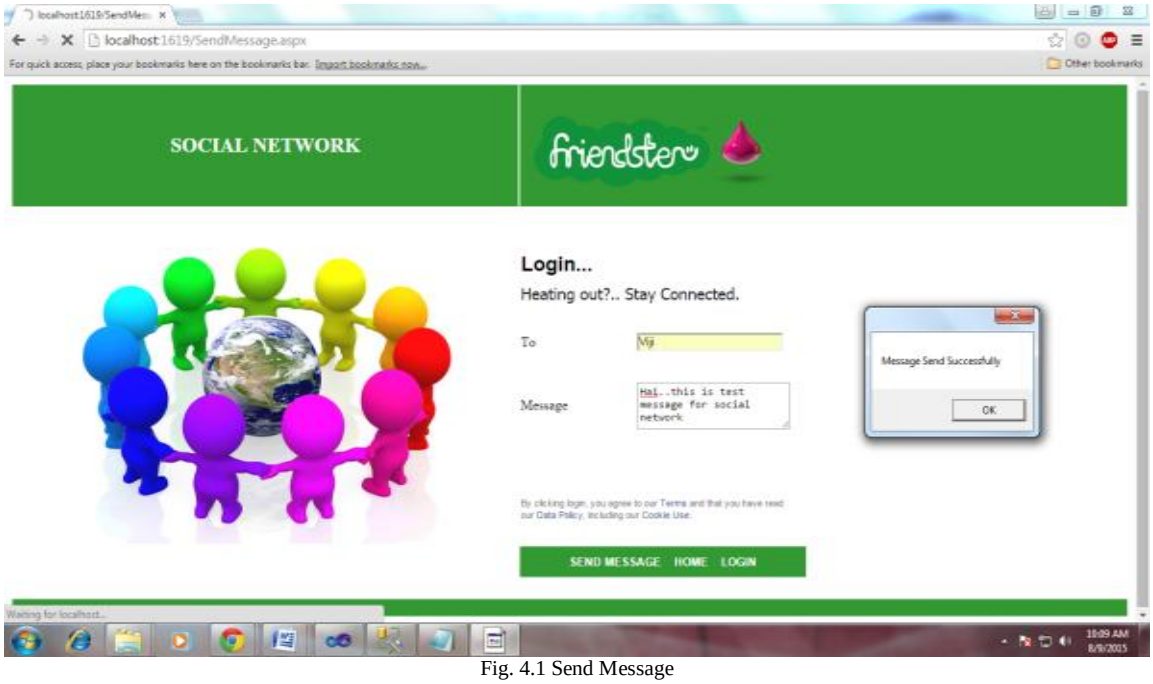

Fig. 4.1 Send Message

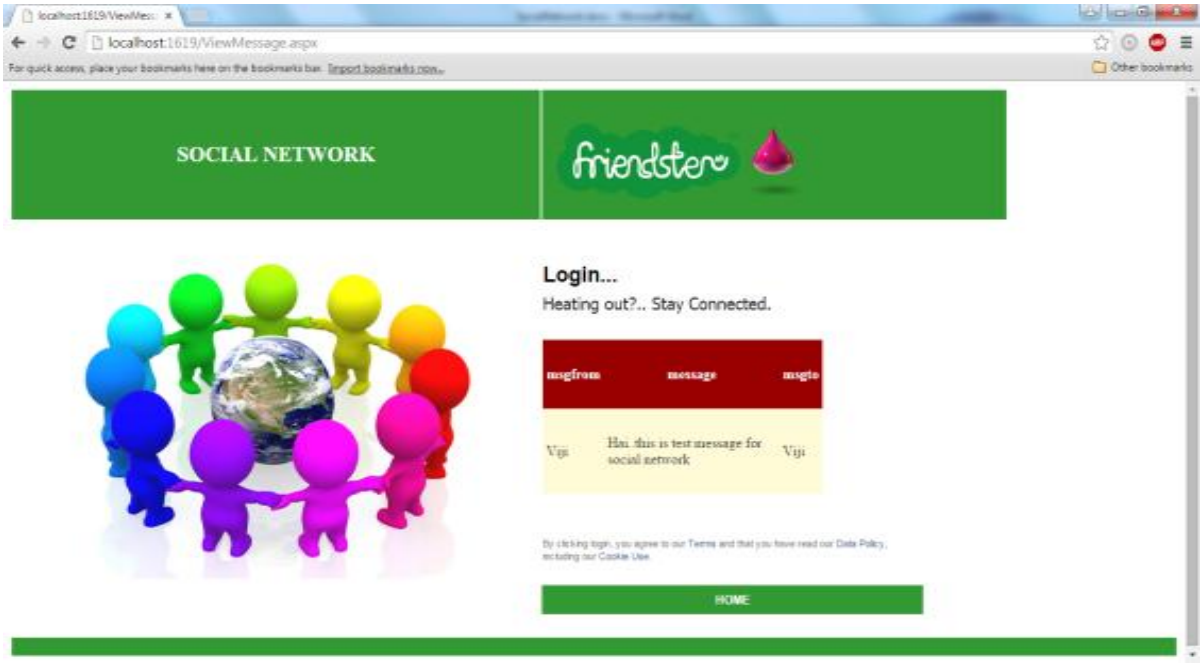

Fig. 4.2 View Message

The encrypted data exchange of messages as well as the personal details of the users of the system is also shown in fig.4.1

The data are encrypted through DES algorithm. DES works on the basis of private and public key. The concept of MD5 is implied when the data is being transferred from user to server and vice versa.

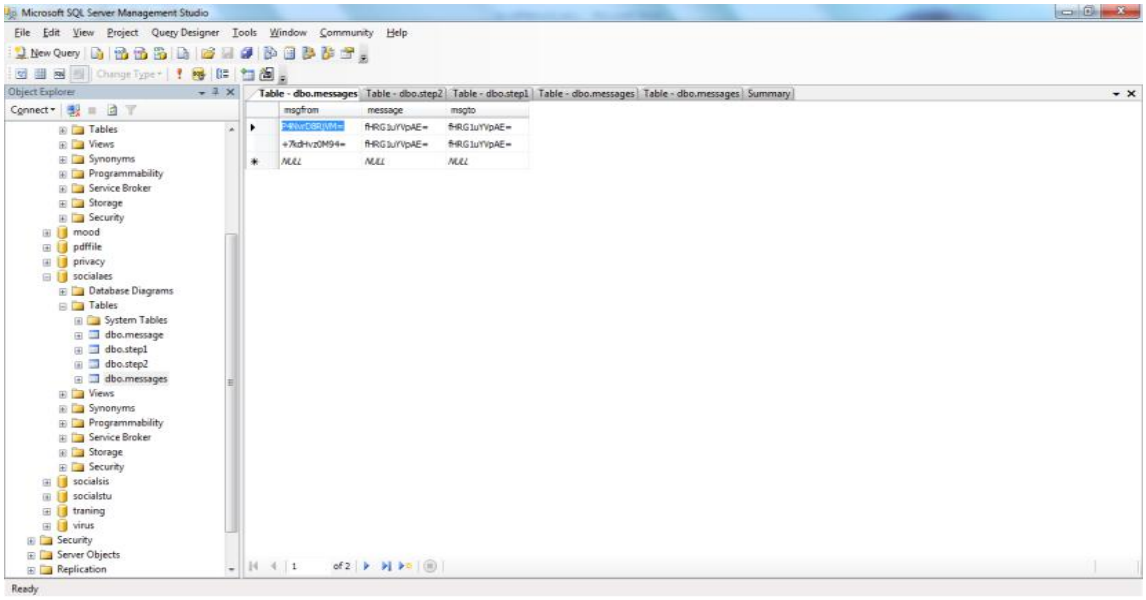

Fig 4.3 Encrypted data stored in database

V. CONCLUSION

The most common computer authentication method for a user is to submit a user name and password consisting of text, numbers or together even with special characters. The vulnerabilities of this method have been well known for attackers to guess, because the users often create memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. The use of strong passwords reduces the risk of unauthorized access, and difficult task of trying to break the entire password. The empirical studies have proven that human are better at memorizing cipher passwords compared to plain passwords. This work gives an idea of having a secured effective authentication system, which provides strong and easily remembered cipher passwords with dynamic security level. The major advantage of this proposed framework is to large password space over alphanumeric passwords.

References

1. Aaron Beach, Mike Gartrell, Baishakhi Ray, Richard Han, "Secure Social Aware: A Security Framework for Mobile Social Networking Applications", in Proc. IEEE International Conf. on 2012, pp. 439-446.
2. Anna Squicciarini, Federica Paci, Smitha Sundareswaran, "PriMa: An Effective Privacy Protection Mechanism for Social Networks", in Proc. of IEEE 3rd International Conf. on 2011.
3. Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen, " Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks", in Proc. of ACM International conf. on 2007, Vol.4, Issue 8, pp.538-542
4. Philip W. L. Fong, "Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems", in Proc. of IEEE International Conf. on 2008.
5. Gilbert Wondracek, Thorsten Holz, Engin Kirda, Christopher Kruegel, "A Practical Attack to De-Anonymize Social Network Users", in Proc. of IEEE, 2011.
6. Lujun Fang and Kristen Le Fevre, "Privacy Wizards for Social Networking Sites", in Proceeding of IEEE 3rd International conf. on 2011.
7. Lei Jin, Hassan Takabi, James B.D. Joshi, "Towards Active Detection of Identity Clone Attacks on Online Social Networks", in Proc. ECDC of 7th International Conf. on 2013, pp. 1- 12.

AUTHOR(S) PROFILE

A. Vijaya Lakshmi received her Master's in Computer Science from Bharathidasan University, Tiruchirappalli, India. Currently, she is a M.Phil Scholar in the department of Computer Science, St. Joseph's College, Tiruchirappalli affiliated to Bharathidasan University, India. Her main area of research is Security in Mobile Social Networks. She has presented two papers in the National Conference. She has atteneded several national and international conferences and workshops.

Dr. S. Britto Ramesh Kumar is an assistant professor of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli. His research interests include software architecture, wireless and mobile technologies, information security and Web Services. He has published many journal articles and book chapters on the topics of Mobile payment and Data structure and algorithms. His work has been published in the International journals and conference proceedings, like JNIT, IJIPM, IEEE, ACM, Springer and Journal of Algorithms and Computational Technology, UK. He awarded as a best researcher for the year 2008 at Bishop Heber College, Tiruchirappalli. He guides 8 Ph.D. research scholars and has completed a minor research project. He visited the countries like China, South Korea and Singapore.

P. Joseph Charles is currently works as an assistant professor in department of information technology, St. Joseph's College (Autonomous), Tiruchirappalli. His areas of interest include context aware web services, information retrieved, etc. He has published nearly twenty research papers in international and national journals. Among three papers were scopes indexed.