Int. J. Soc. & Nat. Sci. Vol. 1 (II) 30-07, 2025 *ISSN 3079-286X (PRINT)*
*Journal home page: **http://ijsns.com,pk*** *ISSN 3104-4123 (ONLINE)*

An Analysis on Privacy Risks, Attacks and Issues in Mobile Social Networks

Amjad Mehmood Amjad
(COMSATS Institute of Information Technology, Islamabad, Pakistan)

*Corresponding author: *amjad.satti2007@gmail.com*

***Accepted:** 24 May, 2025* ***Published:**30 July,2025*

Abstract

A current trend for social networking websites such as Twitter, Facebook, My Space, is to create mobile application to give their users instant and real-time access from their mobile devices. Mobile Social Networks have become more popular. So it is important to examine the privacy risks, attacks and issues of Mobile Social Networks. In this paper we will make three major contributions. First, we will identify the main privacy risks, attacks and issues in different Mobile Social Network Applications. Second, we will survey or study some of the existing MSN security and privacy mechanisms and approaches. Third, we will make a comparison of these approaches.

Keywords: Social Network, Mobile Social Networks, Mobile Social Network Applications, Privacy.

Introduction

Today the internet has become a primary source of information. Now it is used for different purposes, one of those purposes is social relations. Many people now use social networking. Social networking websites enable the people to share their personal information on the internet. A current trend is to create Mobile Social Network Applications. Mobile Social Networks Applications enable a user to access social network websites such as Myspace, YouTube, Twitter and Facebook through his mobile phone. Different Cell phone manufactures such as Nokia, Virgin Mobile and Motorola have developed their own social networks and provided software that enable the users to use Social Network by their Mobile phones (Wei Dong et. al, 2011). Many Mobile Network Applications such as MamJam, Plazes and Jambo, Rummble, Dodgeball are available in the market nowadays (Racha Ajami et. al, 2012).

Mobile Social Networks that enable users to access social networking websites through their handheld devices (such as PDA or cellular phones), have been increasing day by day. Communication with social network sites by wireless has also increased due to some significant characteristics that it has. The major side effect of Mobile Social Networking is, that is compromises the privacy and anonymity of the users and makes it more easily influenced to spoofing and other attacks. It doesn't matter what type of network Peer-to-Peer MSN system or the client-Server MSN system, the identity of the user is not that anonymous. Peer-to-Peer MSN exposes the user location for all users connected to the system and in Client-Server MSN system, there are also many privacy

issues (Racha Ajami et. al, 2012).

By using Mobile Social Networks users share their knowledge, experience, and some other sensitive information along with personal information. Information that is published by users in an online social network is sensitive in most cases. So the both security and privacy concerns are raised because of this sensitive information (E Novak and Q Li, 2012).

A capability offered by Mobile Social Networks is to know about the physical location of your friends. With this you are able to discover and interact with your friends, family members or other people who are physically near to you. May be you are in a new city and your cellular phone discovers your friend's friend is near to you so that you can talk with face-to-face. These are very exciting applications but they create lot of privacy issues. Online social networks also have these same type of issues, and they become more serious in MSN. So it is important to identify and address these privacy issues (Wei Dong et. al, 2011).

(Racha Ajami et. al, 2012), examine the same privacy issues. Mobile Social Networks offer capability that allows users to discover their friends who are near to them. It also allows users to interact and communicate with discovered friends. For example, you are waiting for train in a railway station and your mobile discovered that one of your friends is near to you, in your physical vicinity and you can interact with him and meet with him. These types of capabilities are an improvement in technology but also create lot of privacy issues. People don't want to reveal their presence and some personal information to any other person. As mentioned earlier that online social networks also have these same types of issues. The wireless medium has a broadcast nature that makes it vulnerable for attackers to attack on MSN. So these issues need to address (Racha Ajami et. al, 2012).

A report **"Online as soon as it happens" (online as soon as happens) (Isabella, 2010)** on Mobile Social Networking have been issued by the "EU cyber-security agency ENISA (European Network and Information Security Agency)" (Isabella, 2010). The report describes the SN world and the mobile or cellular phone services which enable a user to access mobile social network by his/her mobile phone. Report also describes some unique security and privacy issues in MSN (Isabella, 2010).

"Another report by professor of computer science, Craig Wills, at US –based Worcester Polytechnic Institute, (WPI) called 'Privacy Leakage in Mobile Online Social Network' has prompted fresh concerns over the security of sites such as Facebook." (Krishnamurthy et. al, 2010)

In this paper we will focus on privacy in MSN. Our goals are to study secured approaches and mechanisms (have been taken to solve security and privacy issues) and take a survey to discuss them briefly and to make a comparison of those approaches and mechanisms.

The major contributions of this paper are: (i) identify the main privacy issues in mobile social networks, (ii) surveys and discuss the main approaches and mechanisms have been taken to solve these issues and (iii) makes the comparison of the discussed approaches and mechanisms.

We will discuss the privacy concerns related Mobile Social Network Application in Section 2. In Section 3 we will discuss some of the existing MSN security and privacy mechanisms and approaches. In section 4 we will compare mentioned and discussed approaches. In Section 5 we will conclude this paper.

Related Work

Mobile Social Network is becoming more popular because of increasing the number of Mobile Online Social Network Applications and ease of use of them from everywhere. Our work is to examine the impact of Mobile Social Network from privacy stand-point. (Lugano, 2008) defined Mobile Social Software (MSS) as "a class of mobile applications whose scope is to support social interaction among interconnected individuals (G. Lugano and P. Saariluoma, 2007) exploiting the media convergence process and the increasing power of mobile devices to offer a variety of services."

Privacy in mobile social networks: "A report by professor of computer science, Craig Wills, at US-based Worcester Polytechnic Institute, (WPI) called 'Privacy Leakage in Mobile Online Social Network' has prompted fresh concerns over the security of sites such as Facebook."(Krishnamurthy et. al, 2010)

(Krishnamurthy et. al, 2010) examine ways by which the new features of mobile Online Social Network interact with existing privacy issues. They said the information on traditional OSNs when combined with new features mobile Online Social Networks cause of privacy leakage. They examine many new privacy issues in the mobile Online Social Networks as well as that result from interaction between traditional Online Social Networks and mobile Online Social Networks. They explain two concepts "presence" and "location". They explore personal information sent on social network websites and the destinations. They discussed three types of destinations include internally, externally or third party. Many mobile online social networks provide privacy settings but the multi-dimensional nature of the issue makes the problem. One of the key feature of presence is explore physical location of user create privacy issue. Information related to the mobile device is another big issue mentioned in this paper. Mobile devices have unique identifier for various purposes. If this unique identifier is leaked, it can be used by a unknown user for an illegal task.

(G. Demiris et. al, 2009) determined that the cameras and image capture devices are increasing the privacy issues. Our work is to identify the newer and latest privacy concerns in MSN to endure users' trust on MSN.

Mobile Social Networks Application and privacy: There are many types of Mobile Social Network Application. (G. Chen and F. Rahman, 2008) categorized 31 applications of Apple Application Store and grouped them into four different categories. i) in first category they grouped "Mobile front-end applications those are similar to desktop applications like MySpace and Facebook that provide interactions among friends only and doesn't support interactions between non-friends"; ii) Sharing Application that allow user to share music, videos, and photos between nearby may be non-friend users; iii) "Neighborhood Exploring Applications" which rely on locations and anonymous interaction and enable users to find, like, dislike, comment, share, and upload multimedia files with the friends as well as all other people that may become your friends in future; iv) applications those designing purpose is mobile communication, the center of attention of some of those is communicating via SMS or electronic-mail (Bluepulse, Avatar) while others allow to display friends' activities, their locations and some sort of comment about visited locations. Our work is to study different new mobile social network applications, privacy settings offer by them and their privacy breaches.

Users trend toward privacy

The amount and type of information that is shared on mobile social networks is depend on the level of trust among the persons those are sharing and to whom they are sharing. (G. Lugano and P. Saariluoma, 2007) elucidated different steps that the users use: i) they decide about trade privacy whether to trade or not. Then they conclude the least damage and calculate the gain from trust. If the damage is lesser than gain the trade will take place otherwise not. At the end users select the set that causes minimal damage. This selection may depend on three things; the sender, the recipient and the message. Sensitivity of data can be asses by asking the user to assign the privacy-sensitivity of each data-item that could be share by mobile devices. When it is done, the application generates profile that consist two steps, public and private as user select. Only the public part is accessed by others and the private part is hidden and cannot be accessed by other users. This application requires effort of user to set privacy sensitivity to each contact and each item (G. Lugano and P. Saariluoma, 2007).

Existing Approaches and Mechanisms (Racha Ajami et. al, 2012) studied some of the existing MSN Security Mechanisms and approaches and compared these mechanisms and approaches according to some characteristics. They examine that if we want to provide appropriate applications for users, it is necessary to think about the privacy issues and include these features into handheld devices such as cellular phones and PDAs. They measured slightly and recognized these issues and address them to make a trust of user on MSN. (G. Demiris et. al, 2009) outlined some most wanted security and privacy issues of encounter-based social networks. They mentioned some common requirements that can be apply to different distributed systems which merge human communication, personal information, and network communication. The security requirements are privacy or unlink ability, authenticity and confidentiality.

The functional requirements are availability and scalability. Their work was similar to SMILE (J. Manweiler et. al, 2009). (Mohaien et. al, 2013) use an approach unlike SMILE. First their design was scalable by nature, second design provided better guarantees of security.

A Survey of different Approaches in Social Network and Mobile Social Networks

We studied some of the existing MSN Security Mechanisms and approaches. We also discussed some Social Network approaches and mechanisms and their features that can be add in Mobile Social Network approaches or mechanisms to improve the privacy of Mobile Social Networks. Here is a brief discussion and evolution of these approaches.

Virtual individual servers (VIS) (Caceres et. al, 2009) are virtual machines that run on a computer infrastructure with high availability utilities and allow users to upload data to Social Network sites. VIS does not depend on the provider's service because it offers users those are able to get full information with the service provider, which make them able to restart usage at whatever time required without concern of the existence of provider. The users of VIS also able to increase or decrease functionality for their convenience but are responsible of managing their own machines and manage to pay for the computing resources used by their VIS. In default situation the anonymity and protection not fully achieved from the service provider,

however, to achieve target of anonymity and security VIS allow the users to install different operating packages and make configuration options as they need. It is not fully flexible mechanism.

The semantic Web-based framework (D. Melinger et. al, 2004) employs the Resource Description Framework (RDF) and the Web Ontology Language (OWL). By using RDF and OWL, it models Social Networks data into different aspects such as modeling of personal relationship, personal information, user resource relationships, and actions. It is flexible because it requires a little involvement form the user. It uses different classes, with their different objects and different methods of encryption, to model information and data, thus the operator protects data and information itself. It is not independent from provider existence. Like a VIS it is also require little involvement from the user so it is flexible.

The proxy based real time protection approach (Tsai et. al, 2010) provides user a secured networking environment. To doing so, it uses the concept of cloud computing. It is a flexible mechanism as semantic Web-based framework because it also requires a little participation from the users. In this approach, whenever a user request for a blacklisted site, he/ she receives a warning message. The operator is responsible for protection itself. It is not independent from provider existence because data rely on the existence of the provider.

The P2P-based SN approach (Graffi et. al, 2009) supports the security requirements in terms of login and `sign-up`, access control and secure communication. In this approach a new user selects a unique user name and password to generate private and public keys. It is also dependent on the provider's existence. It allows authentication of the users easily so it is flexible. Both users and applications communications are authenticated and confidential. It provides access control solutions for both single user and group users. Every message that is sent over the network must be signed and verified respectively by the sender and receiver.

FaceCloak (Luo et. al, 2009) provide full flexibility to users. It's a self-contained architecture. In other words it functions without human intervention and requires no or little involvement by the users. FaceCloak also requires no alteration of the social network authentication features, by visual means. Finally, they enhanced there designs to provide better guarantees of security.

Our goals are to survey different existing mechanisms and approaches that have been taken to address or solved these issues. Make a survey of those approaches, discussed them and make a comparison of them to find and suggest the best one.

It also provides protection of data of users from other users and also from the service provider by encryption. But, it depends on provider existence.

FlyByNight (G. Chen and F. Rahman, 2008) uses client-side JavaScript to encrypt sensitive data. The flexibility of the FlyByNight exists in the ease of use from the users' side. It protects the data of the users from other network users, network administrators, and employees by using encryption keys. It is also dependent on the availability of the service provider.

The U-Control mechanism (Shin et. al, 2009) allows users to manage their privacy level and the sharing of their sensitive personal information in social network sites. It is not flexible for normal users but flexible for experts. It allows experts to control and manage their privacy. It is also dependent on

the existence of social network provider. The operator is responsible itself for protection. The users' data is encrypted against other users on the social networks.

The privacy protection issues in Social Network sites approach (Ho A. et. al, 2009) allows user to determine their require privacy level so it provides more flexibility for skilled users but not flexible enough for normal users. It classifies users based on their characteristics and then provides the privacy for the users as they provide information for social networks. This approach sets the default privacy if the user fails to provide enough information to set privacy. The user can also customize this default setting later if he/she need. Here again the operator is responsible for protection itself as users' data is encrypted against other users on the social networks. It is also dependent on the existence of the provider.

The reputation mechanism (Hogg T., 2009) depends on the peer-to-peer mechanism. It enables users to personalize recommendation via other users according to their reputation or their trusted friends. But, sometime we may not able to recognize reliable users based on their good reputation because some people having good reputation but not reliable and trusted. It's also a dependent mechanism. Operator protection is provided by encrypting and authenticating the information of the users, their messages, and communication.

ReDS (Reputation for Directory Services) (Matthew Wright et. al, 2010) is a framework for using reputation management to improve the security of locating information in Peer-to-Peer. Flexibility of ReDs depends on expertise of the users. However, it requires little configuration from the users. Like reputation mechanism it provides operator protection by encrypting and authenticating the information of the users, their messages, and communication between the communication nodes. So we can easily identify the reliable and malicious nodes. Because it does not provide backup for accounts and information of the users, so the existence of the user depends of the providers' existence.

The Re-Socializing Online Social Network approach (Puttaswamy and Zhao, 2010) is a narrative social networks design which fulfills user requirements. To gain flexibility it uses to schemes Out-Of-Band (OOB) and Coupling to connect other users. A secure message authentication code is used to encrypt information, messages, requests and communications, so the operator is responsible for protection itself. No support for user data. It does not provide independency from provider services.

SMILE (J. Manweiler et. al, 2009) (Mohaien et. al, 2013) tries to allow users for making reliable relationships while protecting them from a number of possible attackers.

In SMILE, users must have an encounter between them for communication otherwise they cannot communicate with each other. They use an encounter key for decryption of data. A user without having a correct key cannot decrypt the message. The benefit of the basic design of SMILE is that it decreases the chances of misuse in the encounter system.More-ever SMILE provides two key features: "k-anonymity and decentralization". It provides authentication but weak.

Encounter-Based Social Network (Mohaien et. al, 2013) provides strong authentication, scalability and guarantees for the post-encounter phase. With strong authentication feature it provides an enhancement in design to provide better guarantees. It reduces the risks of sending extra information to the possible opposition by concealing networking information of users.

Secure friend discovery in mobile social networks (Wei Dong et. al, 2011) is a safe and secure protocol that include three key features: “authentication without long-term link ability, efficient and privacy-preserving proximity pre-filtering and private and verifiable proximity computation”. It uses study of different approaches and real achievement to show its feasibility and efficiency.

WhozThat (A. Beachet at. al, 2008) attempts to make a social communication by using MSN technology. To achieve this, it implements 2 steps protocol. In first step two cellular phones share the WhozThat unique identities. In second step they consult with the online SN with the share identities. The identities can be shared via Bluetooth, WiFi or internet. Cellular phones which are participating in communication must have the WhozThat identity sharing protocol. Each cellular phone is required to advertise an identifier of mobile’s owner. Another good thing is that this software can be extended and many other applications can be included into basic mechanism. (A. Beachet at. al, 2008)

Dodgeball(N. Ziv and B. Mullth, 2006) combines location service with SN. It’s combination of SN, cellular phone messages and mapping software. It allows users to create a public profile and making friends. It also allows users to know about the friends of friends and having a list of “crushes”. It allows users to inform their friends that are 10blocks away from them. When a user sends a message to all his/her friends, Dodgeball inform the user if one of his friends is near (10block in radius) to him/her. Dodgeball also allow you to know about some of the “crushes” if they are in a radius of 10blocks of your place. If you want about a place, send the name of the place to Dedgeball, it will return you the address of that place. (N Ziv and B. Mullth , 2006).

MANET (Stefan Stieglitz and Christoph Fuchß, 2011) is a new technology allows data transferring between cellular phone. It allows users to interact face to face with persons from his virtual network. It incorporates exchanging of information between cellular phone’s users. Users are allowed free exchanging of data, user doesn’t need new devices, software download is voluntarily and without any cost arbitrarily activation and deactivation of users.

Anonymous Identifiers (AIDs) (Beach et. al, 2009) enables users to connect secretly and hides their identities. Its design is not fully flexible. It does not require much involvement from users. Just in the beginning of setting stage, users need to set identifiers and passwords for security purpose. To maintain anonymity of the users the approach provides protection of information of the users and their identities from malicious users. It depends on the SN provider existence to maintain information of users and to complete the primary setting steps.

A survey on privacy issues in MSNs (Venkata Sai and Y. Li, 2020) introduces MSNs, categorize privacy issues based on their affected aspects, summarize related threats within those categories, classify existing privacy-preserving solutions from recent research, and provide information on relevant datasets and data generation tools for future studies in the field.

User Motivation based Privacy Preservation (UMPP) model (Venkata Sai et. al , 2021) is novel approach to address privacy issues in LBSNs. (Hussam et. al , 2023) proposes AI as a key solution to improve security and privacy issues within MSNs.

(Chandana et. al , 2025) highlights key issues, including user data vulnerability, ethical

challenges in content moderation, and the role of policies and regulations. They proposed a system to enhances privacy through stronger settings, decentralized identity management, homomorphic encryption, and federated learning. They also explore how artificial intelligence is shaping content moderation and legal frameworks. (Chandana et. al, 2025)

Online Social Networks (OSNs) have become a central part of daily life, widely used for communication and information sharing. However, the rapid spread of personal content such as photos, videos, and audio raises serious security and privacy risks, as attackers can exploit this information for malicious purposes.

(Akash Shah et. al, 2024) address these gaps by categorizing threats into traditional, advanced persistent, and targeted types, while also providing protective measures and highlighting ongoing research challenges to ensure OSN user safety. (Akash Shah et. al , 2024)

(A. Ometov et. al, 2017) investigate whether modern mobile devices can be compromised, testing existing security algorithms against side-channel attacks. Findings reveal that while basic equipment yields limited results, advanced techniques and neural networks may significantly improve data extraction. They also suggest protective measures to mitigate such threats and ensure user privacy. (A. Ometov et. al , 2017)

(Ali S. et. al , 2018) highlight key security and privacy challenges in OSNs and offers practical recommendations for users to safeguard their data while engaging on such platforms. (NaliniPriya and Asswini, 2015) reviews major security challenges in OSNs and examines existing models aimed at protecting user data and ensuring secure interactions. (NaliniPriya and Asswini, 2015).

Comparison of approaches of Social Network and Mobile Social Networks:

We studied and analyzed different existing SNs and MSNs Security Mechanisms and approaches. Here is a brief discussion and evolution of these approaches base on their performance in respect to the following challenges and constraints: User's anonymity, Flexibility, Operator protection, Level of privacy and security, Authentication and Provider's existence in-dependency.

Table 1

Comparison of approaches of SN and MSN

Name of Approaches/ Architectures / Mechanisms	Features	User Anonymity	Flexibility	Security and Privacy Level	Operator Protection	Dependency	Authentication Level
Virtual Individual Servers (VIS)	Virtual machines that allow users to upload data to Social Network sites.	Not Fully achieved/ dependent on user setting	Some	Not Fully achieved/ dependent on user setting	Not Fully achieved/ dependent on user setting	Yes	-
Semantic Web Based Framework	Uses RDF & WOL to model SN data models Social Networks data into different aspects.	Not Addressed	Yes		Yes	No	-
Proxy based real time protection	Detects security Threats, and blacklisting the none-secure websites.	Not Addressed	Yes	Can detect the websites security threats	Yes	No	-
FaceCloak	Self-contained architecture that function automatically	Not Addressed	Yes	Not fully achieved, attacker can take control over the user browser	Yes	No	`-
FlyByNight	Uses client-side JavaScript to encrypt sensitive data. Protect user data.	Not Addressed	Yes	Yes, encrypt text but not achieved image encryption	Yes	No	-
U-Control mechanism	Enables users to control their privacy level	Not Addressed	Some	Allow users to control privacy levels	Yes	No	-
Privacy protection issues in SN sites	Allows user to determine their require privacy level	Not Addressed	Some	Help users to determine their require privacy level	Yes	No	-
Reputation Mechanism using SN Sites	Personalize recommendations according to reputation of other users or trusted friends.	Not Addressed	Some		Yes	No	-
ReDS	Use reputation management for improving the security	Not Addressed	Some		Yes	No	-

Name of Approaches/ Architectures / Mechanisms	Features	User Anonymity	Flexibility	Security and Privacy Level	Operator Protection	Dependency	Authentication Level
Home Network Social Application	Allows home devices to actively participate in SN sites.	Not Addressed	Some		No	No	-
SMILE	Provides k-anonymity and decentralization.	Yes	Some	Not guarantee of full security	Some	No	Weaker
encounter-based social network	Provides strong authentication, scalability and guarantees for the post-encounter phase	Yes	Yes	Yes	Yes	No	Strong
Secure Friend Discovery in Mobile Social Networks	Provides privacy and verifiability	Not Addressed	Some	Yes	Yes	No	Yes
MANETs	Provides repository organization and message storing.	Not Addressed	Some	Yes	Yes	No	Yes
AIDs	Provides secret connection for mobile users and conceal their identities.	Yes	Some	-	Yes	No	-
Re-Socializing Online Social Networks	Is a narrative social networks design which fulfills user requirements.	Not Addressed	Some	-	Yes	No	-
Privacy-Enablig Social Network	Protect users' information and users' privacy against the SN operator.	Yes	Yes	-	Yes	No	-

Conclusion

Due to increasing popularity of social network and especially mobile social networks, it has become important to examine the impact of Mobile Online Social Networks from a privacy standpoint. In this paper, we surveyed and discussed some existing Social Network and Mobile Social Network mechanisms and approaches. We hope that this paper will help other researchers to design a fully secure mechanism for Mobile Social Networks. Because this research has made a comparison of different approaches so it is easy to design a new approach by having the weak points in mind of discussed approaches. As seen in this research, that it is necessary to consider the privacy issues though adding such features into handheld devices (such as mobile, PDAs,) to provide proper application to the users.

REFERENCES

Wei Dong; Dave, V.; Lili Qiu; Yin Zhang, "Secure friend discovery in mobile social networks," infocom, *2011 Proceedings IEEE* , vol., no., pp.1647,1655, 10-15 April 2011 doi: 10.1109/INFCOM.2011.5934958

Racha Ajami, Nabeel Al Qirim, Noha Ramadan, "**Privacy Issues in Mobile Social Networks"** Procedia Computer Science, Volume 10, 2012, Pages 672–679

E Novak, Q Li" A Survey of Security and Privacy in Online Social Networks" - College of William and Mary Computer Science …, 2012 - cs.wm.edu

European Network and Information Security Agency (ENISA), "Online as soon as it happens", 2010, Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu

Krishnamurthy, Balachander and Wills, Craig E." Privacy leakage in mobile online social networks" USENIX Association, Berkeley, CA, USA 2010

Beach, A.; Gartrell, M.; Han, R., "Solutions to Security and Privacy Issues in Mobile Social Networking," *Computational Science and Engineering, 2009. CSE '09. International Conference on* , vol.4, no., pp.1036,1042, 29-31 Aug. 2009 doi: 10.1109/CSE.2009.243

Von Arb, M.; Bader, M.; Kuhn, M.; Wattenhofer, R., "VENETA: Serverless Friend- of-Friend Detection in Mobile Social Networking," *Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and* Mobile Computing, , vol., no., pp.184,189, 12-14 Oct. 2008n doi: 10.1109/WiMob.2008.52

Lugano, G., Mobile social networking in theory and practice, First Monday, Volume 13, Number 11 (2008).

Tasch, H., Bakel, T., Location Based Community Services for a new Type of Web Communities, IADIS International Conference Web Based Communities, Lisbon (2004).

G. Chen and F. Rahman, Analyzing privacy designs of mobile social wetworking applications, In Proceedings of the IEEE/IFIP International Symposium on Trust, ecurity and Privacy for Pervasive Applications (TSP), Shanghai, China, 2008.

G. Demiris, O. D. Parker, J. Giger, M. Skubic, and M. Rantz, Olderadults' privacy considerations for vision based recognition methods ofeldercare applications, Technology and Health Care, vol. 17, 2009.

G. Lugano , P. Saariluoma, To Share or not to share: supporting the user decision in Mobile Social Software applications, In Proceedings of the User Modelling conference, Corfu, Greece, 2007.

D. Melinger , K. Bonna, M.Sharon, M.SantRamet, Socialight: A Mobile Social Networking System, In Proceedings of the 6th International Conference on Ubiquitous Computing, Nottingham, England, 2004.

P. N. Puttaswamy and B. Y. Zhao, Preserving privacy in location-based mobile social applications, in Hotmobile'10 Proceedings of the Eleventh Workshop on Mobile Computing

Systems & Applications, Ohio, USA, 2010.

J. Manweiler, R. Scudellari, Z. Cancio, and L. P. Cox. We saw each other on the subway: secure, anonymous proximity-based missed connections. In HotMobile '09: roceedings of the 10th workshop on Mobile Computing Systems and Applications, pages –6, New York, NY, USA, 2009. ACM.

Mohaien, Abedelaziz; Kune, Denis Foo; Vasserman, Eugene Y.; Kim, Myungsun; im, Yongdae, "Secure Encounter-Based Mobile Social Networks: Requirements, Designs, and Tradeoffs," Dependable and Secure Computing, IEEE Transactions on , vol.10, no.6, pp.380,393, Nov.-Dec. 2013 doi: 10.1109/TDSC.2013.19

Caceres, R., et al. "Virtual Individual Servers as Privacy-Preserving Proxies for Mobile Devices," In Proc. of MobiHeld'09,2009

Luo, W., Q. Xie, and U. Hengartner, "FaceCloak: An Architecture for User Privacy on Social Networking Sites," in Proc. of PASSAT-09, pp. 26-33, August 2009.

Tsai, D.T., A.Y. Chang, , S. Chung, Y.S. Li, "A Proxy-ased Real-time Protection Mechanism for Social Networking Sites," in Proc. ICCST 2010

Graffi, K., P. Mukherjee, B. Menges, D. Hartung, A. Kovacevic, R. Steinmetz, "Practical Security in P2P-based Social Networks," in Proc. IEEE 34th Conference on Local Computer Networks (LCN 2009)

Zürich, Switzerland, pp. 269-272, October 2009. "A Framework for Enabling User-controlled Persona in Online Social Networks," in 33rdAnnual IEEE International Computer Software and Applications Conference, pp. 292–297, 2009.

Ho, A., A. Maiga, E. Aïmeur "Privacy Protection Issues in Social Networking Sites" in proc. AICCSA 2009, p. 271-278, 2009.

Hogg, T., "Security Challenges for Reputation Mechanisms using Online Social Networks," in Proc. AISec'09, pp. 31 – 34, November 2009.

Matthew Wright, Apu Kapadia, Mohan Kumar, and Apurv Dhadphale "ReDS: Reputation for Directory Services in P2P Systems" in CSIIRW '10, Oak Ridge, Tennessee, USA, 21–23 April 2010.

Manweiler, R. Scudellari, and L. P. Cox. SMILE: encounter-based trust for mobile social services. In E. Al-Shaer, S. Jha, and A. D.Keromytis, editors, ACM Conference on Computer and Communications Security, pages 246–255. ACM, 2009.

Beach, M. Gartell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan,B.Surendar,M.Terada,andR.Ha n. WhozThat? Evolving an ecosystem for context-aware mobile social networks. IEEE Network, pages50 55,July 2008.

Tong. Analysis of some popular mobile social network system. Helsinki University of Technology,2008.

Ziv and B. Mullth. An exploration on mobile social networking: Dodgeballas case in point. Proceedings of the international conference on mobile business,2006.

Stefan Stieglitz, Christoph Fuchß, Challenges of MANET for Mobile Social Networks, Procedia Computer Science, Volume 5, 2011, Pages 820-825, ISSN 1877-0509, http://dx.doi.org/ 10.1016/j.procs. 2011.07.112

Ajami, Racha and Ramadan, Noha and Mohamed, Nader and Al-Jaroodi, Jameela, Security challenges and approaches in online social networks: A survey, IJCSNS, pages1-8,2011

M. V. Venkata Sai and Y. Li, "A Survey on Privacy Issues in Mobile Social Networks," in IEEE Access, vol. 8, pp. 130906-130921, 2020.

A. M. V. Venkata Sai, Kainan Zhang, Yingshu Li, "User Motivation Based Privacy Preservation in Location Based Social Networks", 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/ SCALCOM/UIC/ATC/IOP/SCI), pp.471-478, 2021.

Hussam N. Fakhouri, Sadi Alawadi, Feras M. Awaysheh, Faten Hamad, Sawsan Alzubi, Mohammad Naser AlAdwan, "An

Overview of using of Artificial Intelligence in Enhancing Security and Privacy in Mobile Social Networks", 2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC), pp.42-51, 2023.

Chandana D M, Sankalp M R, Sheela Kathavate, Aruna S, "Inspection of Ethical and Privacy Concerns in Online Social Networks", 2025 International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF), pp.1-6, 2025.

Akash Shah, Sapna Varshney, Monica Mehrotra, "Threats on online social network platforms: classification, detection, andprevention techniques", Multimedia Tools and Applications, 2024.

Ometov, A. Levina, P. Borisenko, R. Mostovoy, A. Orsino and S. Andreev, "Mobile Social Networking Under Side-Channel Attacks: Practical Security Challenges," in IEEE Access, vol. 5, pp. 2591-2601, 2017.

Ali, S.; Islam, N.; Rauf, A.; Din, I.U.; Guizani, M.; Rodrigues, J.J.P.C. Privacy and Security Issues in Online Social Networks. Future Internet 2018.

G. NaliniPriya and M. Asswini, "A survey on vulnerable attacks in online social networks," International Confernce on Innovation Information in Computing Technologies, Chennai, India, 2015.