Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 5, 10021-10031

SECURITY AND PRIVACY IN SOCIAL NETWORKS

Seyed Hossein Mousavi[1*]
1. Master's degree, Department of Information Technology, Computer Networks, Karun University of Applied Sciences, Ahvaz, Iran.

Hamid Barati[2]
2. Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran

Abstract

Nowadays, social networks affect the lifestyle of communities in various ways. The possibility of communication between people in cyberspace, information sharing, knowing each other, and quick notifications are advantages of such networks. Besides that, social networks present a set of information to study virtual communities in various fields of science, ultimately leading to knowledge production. Virtual social networks are usually web-based services, including online services, platforms, or sites where people opine, show interests, and share them. The purpose of the study was to examine security and privacy in social networks. The method was descriptive-analytical using library resources. The studies showed that a social network is a social structure with social actors (e.g., individuals or organizations), dual relationships, and other social interactions between the actors. Concerns over privacy in social media are a subset of information privacy that involves the right to privacy in storage, resuscitation, third-party disclosure, and display of information about the Internet. Security and privacy issues on social networks result from a lot of information these sites process every day. Attributes inviting users to participate in messages, invitations, photos, open platform applications, and other applications usually provide access to others' privacy information.

Keywords: Social networks, privacy, profile matching

INTRODUCTION

Issues associated with security and privacy on social networks result from much information that these sites process every day. The attributes inviting users to participate in messages, invitations, photos, open platform applications, and other applications often provide access to others' privacy information. Moreover, the technologies needed to deal with user information might violate their privacy.

A person's life becomes way more public despite social networks. Social media sites allow people to connect with more people using personal interactions. The individuals can connect with users worldwide who may never have the opportunity to meet them in person. This could engrain positive effects. However, this raises many privacy concerns. Information about a person may be published that they do not wish to disclose. Complicating matters in the novel, the author explains that some people “believe that the desire to participate in public spaces - and, as a rule, any act of showmanship and propaganda - is incompatible with a desire for privacy.” When something is published on the Internet, it is accessible to several people and can even be shared beyond supposed friends or followers. Nowadays, many employers consider a person's social media before hiring a person for a job or position.

Social media has turned into a tool that people use to find information about people's lives. People can learn a lot about a person based on what they have published before meeting once. The ability to access privacy is an endless process. “Achieving privacy requires the ability to control social status using complex textual cues, technical affordability, and social dynamism,” Boyd describes. Society is constantly changing; Thus, the ability to

understand social conditions for privacy is constantly changing.

Along with the rise of mobile and online social networks, Internet users make it easier to exchange information. Mobile social network (MSN) is of the new trends in mobile technology that has combined wireless communication with social networking. One of the most known uses and advantages of MSNs is profile matching; this attribute allows users to find the users they are interested in - for instance, in their social life, making friends and finding people with common interests and tastes. Even though this method is widely used and useful in identifying common interests among users, there are several issues to consider.

For matching, the user must disclose their interests and personal information to other users to identify commonalities between them. Some users do not want to reveal all their interests and information to other users in some cases. They only want to disclose their interests fully when they are sure that there is a common interest between them and the intended user. Given the above, the purpose of the study is to examine the security and privacy of social networks.

Theoretical basics

1. Social network

Nowadays, the advancement of technology and the development of mass media have led to many communication changes and different cultural, social, political, economic issues, and so on [1]. Meanwhile, the Internet has its advantages; on the one hand, it raises people's political awareness, and on the other hand, it engages them in political relations since urban public space for dialogue is seldom available. Cyberspace has become an arena for conversation, and its main attribute is the dynamism of this space, which, due to the tools it provides to users, allows people to express their political tendencies better.

Relationships constantly increase between people and create a greater need for communication. This will expand online social network systems (OSNS) like Friendster or LinkedIn and increase the popularity of communication services like instant messaging, web conferencing, and voice on IP (VoIP) systems. Online social networks support interpersonal communication and the creation and completion of human societies and are therefore of interest to software engineers and sociologists [2].

Social Networks (SNs) have become significant components of the information society. Although social network analysis (SNA) emphasizes interpersonal communication, SNA results provide more information about individuals themselves. There are many different social networks [3]. All approaches to the social network are rooted in the concept of society, emphasizing the nature of communication between individuals, not just individuals. Carol Marx said that society is not just a collection of individuals but the sum of the relationships where these individuals confront each other [4]. The one starting the studies on modern social network theory was Stanley Milgram. In 1967, he carried out an experiment where 60 people from Nebraska were asked to send letters to their colleagues in Boston. This has to be only done by giving this letter to a person whom these people knew by name. The experiment result was that people in America form a social network and are connected to this network with six degrees of separation, a message on the network that is delivered in an average of six steps [5].

The main idea behind the social network is that various people or organizations form network nodes, and the nodes between nodes represent the connections between different people. A social network indicates how actors interact with each other, which can be maintained through one or more other relationships. Moreover, the social network has access to its own options (people who are directly connected to it) and other options (my friends' friends).

Social network nodes are not independent. Some characteristics are defined specifically for network members, such as demographics and interest data about people. However, none of the SNA methods sample people independently. Actors are connected via relationships characterized by content, direction, and strength. Content indicates the source being exchanged, meaning that in computer communications (CMC), information can be considered the source. Direction determines whether the relationship is directional or directionless. The relationship between employees and their supervisor is directional. Employees work for the supervisor, which is the relationship between employees and the boss.

Social networks can be divided into several groups with various criteria. Social networks should be: private (meeting or business networks, friends' networks, graduates, leisure clubs), indirect (online communication, address books, e-mail), joint activities (authors of scientific articles, event organizers), local networks (people living nearby), families, employee networks, hyperlink networks (the link between home pages) [6].

Using these different social networks, they can be classified based on the type of relationship that connects the two people. In this case, social and business relationships can be distinguished. Business connections include social networks of people connected because of what they do but do not share their personal lives at the same time. These can be called professional networks. Company employees create an employee social network that can be a good sample. Those organizing a conference or other event together create a social network of organizers. These people are connected because they work together, and their participation usually has consequences like papers, conferences, books, etc. On the other hand, social relationships show relationships with an emotional background. Relatives are a group of people who make up our family, but usually, not everyone is in touch with all of their family members.

The classification of social networks could be based not only on the type of communication that happens in the network but also on the type of communication channel between members that are used to exchange resources, it could be individual or using a device (virtual, with a computer, mobile, post) (Figure 1) [7].

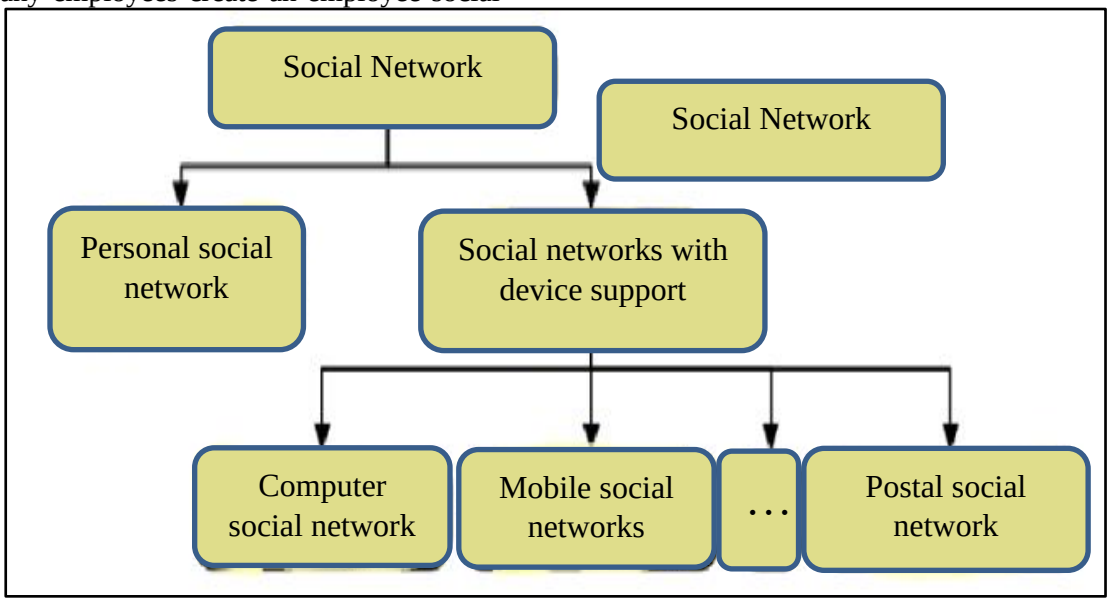

Figure 1. Division of social networks based on the type of communication channel [7]

Personal social networks are more vulnerable, whereas decision-support social networks (DSSNs) suffer from limited social presence. In personal networks, not only words and information are important, but also the physical context, non-linguistic expressions, and visible information about social characteristics. These components did not take place in DSSN. In contrast to personal SN, DSSN enables the communication between people in various parts of the world. This classification likens the previous one (Figure 1). It does not exclude a situation in which two people communicate with each other in more than one way, say, two people who both send e-mails to each other and meet each other. Proposed classifications are not the only possible cases. However, they say there will be many possible classifications for social media.

2. Online social networks

Online social networks can be defined as a collection of people connected to a computer network. Online social networks facilitate new connections and facilitate communication between people in various places and at various times. This makes relationships feel like real relationships. Nonetheless, this becomes an important advantage when people cannot meet but can communicate in other ways (e.g., sending email) [8]. On online social networks, on the other hand, people will miss the opportunity to study some verbal (tone of voice) and non-verbal (body language) components of the exchange.

The relative lack of social presence makes it possible to develop an organized community with a common interest, not a common neighborhood. According to one of the divisions of social networks, they can be called computer-supported social networks (CSSNs). This group includes two distinct subsets of simultaneous and asynchronous online social networks.

The asynchronous network enables asynchronous communication between two people or from person to group. An example of this is e-mail. When person x sends an email to person y, a relationship is established between these people. However, if the x person only has the y address of the y person, but they never send each other emails, then there will be no boundary between them. Internet groups, as opposed to email, which support communication between two people or a small group of people, give everyone on a particular social network the ability to read all the messages provided by all network members. Their capabilities are similar to real-world bulletin boards [9].

The second group is social networks with the support of computer networks, chats, instant messengers, and VoIP systems. In this type of network, communication between users is simultaneous, meaning that both users must be online to communicate. In chat systems, people exchange messages and wait for the other party to respond. In instant messaging, two people or a limited group of people will communicate with each other and exchange messages.

3. The role of online social networking systems

In addition to being a reference for providing many of their cultural, social, scientific, and other needs, virtual social networks allow members to perform their activities in this virtual space simultaneously as performing other social activities via computer or mobile phone. Thus, the attractiveness of virtual social networks on the one hand and the ease of activity in this category of communities, on the other hand, causes the relationship between membership and presence in virtual social networks and lifestyle changes of employees of member organizations as a serious question for researchers in the field of culture. The concept of lifestyle, which has become one of the fundamental concepts in social analysis today, is one of the new and important fields of study that has attracted the attention of a considerable number of researchers in recent years [10].

Figure (2) reveals the activities and conditions that must be established to establish a new relationship between two users. At first, user x searches for someone whose profile characteristics and preferences are proper. After finding the user, an invitation is sent to the selected user. If the selected user responds positively to this request, the relationship is established and could be maintained by the users and expanded (Figure 2). However, if the request is not accepted, the selected user has not responded. Thus, user x must be looking for a new friend or start another search.

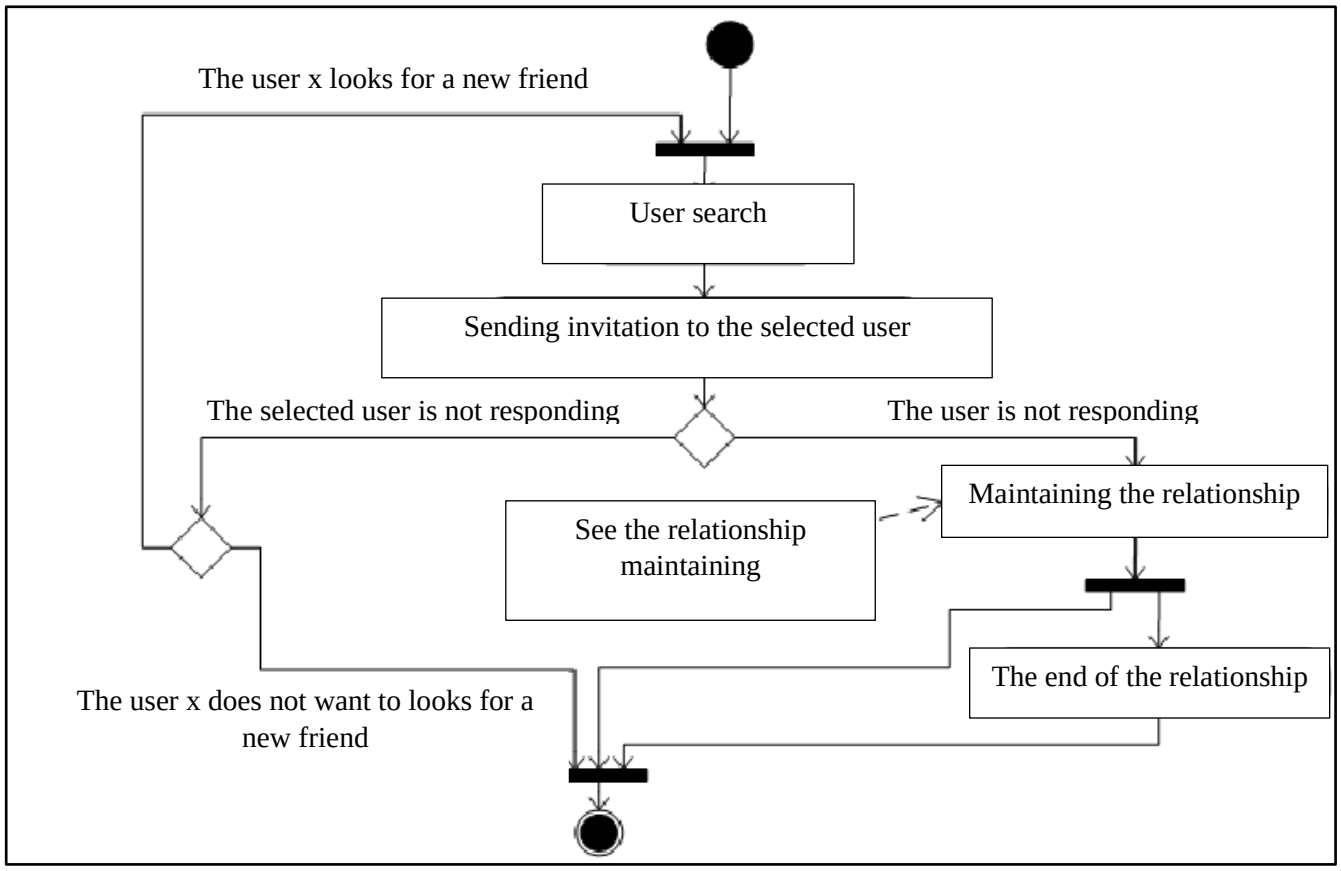

Figure 2. The process of starting a new relationship [10]

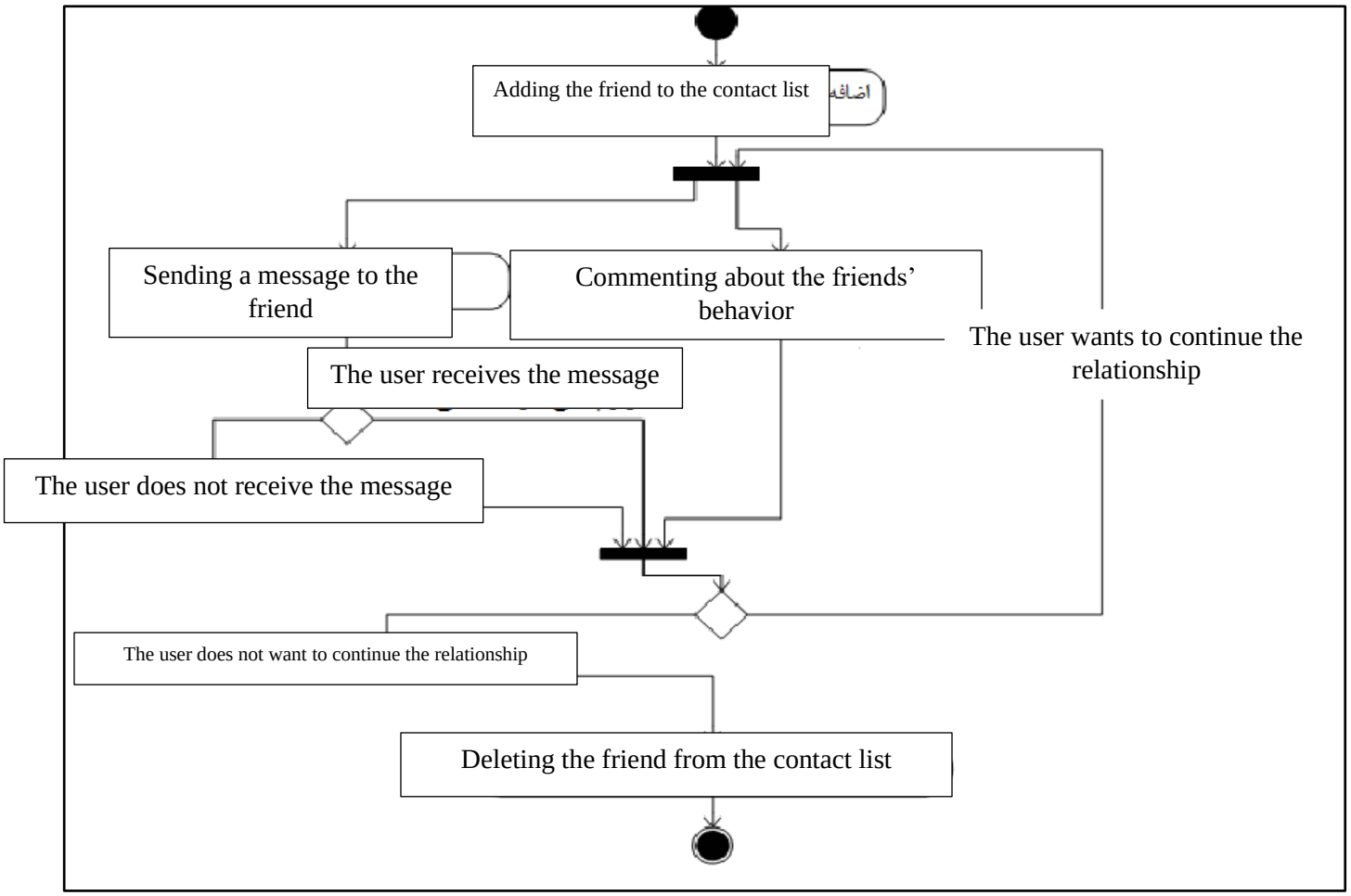

Figure 3. Relationship maintenance process [10]

When the selected user responds to user x's friendship request, a relationship is established and can be maintained by sending a message to a friend or commenting on behavior on a social network (Figure 3). When user x wants to delete his friend, he has to remove him from his contact list. However, user x is not friendly to the user removed from the contact list. If the deleted person does not remove user x from the contact list, there is still an undirected relationship between this person and user x.

4. Attributes of social networks

Each social network can be defined by a set of attributes providing information about the overall structure of the network, such as domain, density, access, and connectivity, as well as about users - centrality and roles. The scope of a social network can be accessed via characteristics like size and heterogeneity (composition). Small homogeneous groups are good for conserving existing resources, yet large, heterogeneous networks are good for gathering and exchanging new information. Traditional workgroups, families, and urban communities are examples of homogeneous networks, and online communities belong to large, heterogeneous networks. Virtual communities belong to the most heterogeneous group because they connect people with cultural and religious backgrounds. Density is the ratio of nodes in a network to all the existing nodes. Once network density is known, the speed of information dissemination between actors and the extent to which actors have high levels of social capital or social constraints are specified [11].

One of the network attributes is access, determining the x player available to the y player when there is a set of connections that make it possible to track from x to y. Moreover, it is not important how many people are between x and y. Access determines whether there is a connection between the two actors, whereas the connection shows that user x will be able to reach y in several possible ways. If there are various paths for connecting two actors, then the high connectivity of some of the attributes that describe SN are the roles assigned to them based on the behavior of the members. The similarities between the behaviors of individuals have made it possible to differentiate the set of rules of each network. These maps can be determined empirically by finding rules in relationship patterns (structural equality). Groups and sub-structures must be analyzed to understand the possible behavior of the network. The phenomenon maintained in networks is that categories and connections are weak and strong. The category is created by a group of actors very closely related. The formal definition says that the category is the maximum number of actors with possible connections between them. This definition is very difficult and can be relaxed in two ways: the concept of categories N and K networks. The first case defines a category as a set of actors connected to other actors belonging to this set at a distance equal to or less than N and the second allows a cast member to determine if an actor is connected to all members of the K category. The communications that connect people on a social network are often divided into strong and weak categories. However, like the centrality problem, strong and weak communication definition relies on the context. Overall, weak communication can be defined as communication that involves the combination of intimacy, disclosure, providing mutual services, much kindness between close friends or colleagues [12].

5. Privacy

Privacy design is done for mobile social networking applications based on four steps: stepping, construction, accessibility, and goals. Stepping discusses the type of information that is collected from the mobile device. Most mobile social networking uses show a dialog asking you to access user location information. Construction metrics discuss what happens to users' information after collection. This relies on the application, the location of the information left on the user's device, or the external sending to another. Even for applications that store information locally, in some places, it transfers it to a larger network or system for additional processing and better use of services.

Furthermore, for services such as neighborhood services, information is sent externally. The issue of accessibility is about who can access users' information after collection, which is different in each application. Neighborhoods in the programs exploit the information stored in the service provider and allow access to users who have no control over the distance between

themselves and the people who can discover their location. Ultimately, Demirs et al. indicated that privacy concerns are heightened by cameras and video recorders with targeted questions about how the information will be used later. Moreover, they figured out that participants emphasized the need to control the system by enabling it to be turned on or off and to determine who had access to the collected information.

6. Cryptographic algorithms

Even though cryptography has evolved tremendously since Shanon's earliest works in the late 1940s and early 1950s, cryptography has evolved with cryptography, and few algorithms have retained their value over time. Hence, the number of algorithms used in practical computer systems and smart card-based systems is very small [13].

Literature review

Green et al. (2011) suggested a new way to reduce the overhead of the decoding process and called it Outsourcing the Decryption. This approach allows a cloud server to convert "Attribute-based with encrypted text policy" text to plain encrypted text using a user-provided key. This significantly reduces the decryption overhead on the user side, but there is no guarantee that the transfers made by the server are correct [14].

Lai et al. (2013) added the concept of verifiability to outsourced decoding to ensure that the external server carried the outsourcing calculations correctly [14]. Check Ability to review enables the user to review the accuracy of the information transmitted by a third party. In this scheme, they encrypted a random value added to the encryption and decryption algorithms and used it to Check Ability. The main problem of this method is that the length of the encrypted text doubles because of the addition of a random value to the attribute-based cryptographic prototype and increases the computational costs of encryption and decryption compared to the prototype too [15].

Hur et al. (2013) suggested an attribute-based cryptographic scheme with an encrypted text policy for data sharing in smart grid systems. In this scheme, users create tokens for decryption and send them to the server. These tokens are generated to outsource decryption calculations to external servers, reducing the huge amount of decoding computational load. The main problem with this scheme is the permanent validity of the tokens. Non-expiration of tokens makes the plan vulnerable to denial-of-service (DOS) attacks. Moreover, it lacks a way to cancel users [16].

Bayat et al. (2014) enhanced the proposed Hur scheme [47] and provided two security issues for that scheme: invalidating users and resisting DOS attacks. In this scheme, a timestamp is added to the token produced by the user, which saves the validity time of the token. This makes it impossible to launch DOS attacks if the token is stolen by an unauthorized user [17].

Chow et al. (2016) suggested a scheme for constructing Multi Authority Attribute-based Encryption (MA-ABE) with efficient decoding and falsification. This scheme uses a central reference with several issuing references to generate the key. Decryption is outsourced in this scheme, and most of the computational load is decrypted by the server, and the rest of the encryption is done by the user. When a user reports that a decryption key has been compromised, all of that user's keys must be canceled [18].

Yang et al. (2014) proposed a scheme for attribute-based access control with multiple export references in the cloud environment. The architecture of this design has a Central Authority (CA) and several issuing references. Data encryption is carried out based on the public keys issued by various issuing authorities and universal public parameters issued by the central authority, preventing the data from being decrypted. Moreover, a version number is assigned to each attribute to invalidate the attributes. When an attribute is revoked, only the components associated with the revoked attribute are updated in the private key and encrypted text, which reduces the over-encryption overhead [19].

Nabeel et al. (2014) suggested a two-layer encryption-based method for data loaded in the cloud environment and called it two-layer encryption (TLE). In the TLE method, the access control policy is divided into two sub-categories, constituting the primary access control policy. This segmentation is carried out so that the least number of attributes are assigned to the data owner, and also the data remains highly confidential from the point of view of the cloud [20].

Jung et al. (2015) suggested a Semi Anonymity access control with cryptography according to completely anonymous attributes for cloud environments. This scheme protects not only data privacy but also the privacy of identities. This scheme, called Anony Control, decentralizes central reference to limit identity disclosure [21].

Wang et al. (2015) provided a useful protocol for maintaining privacy on online social networks. Friendship with some of the common attributes is one of the most popular applications in MSNs. Nonetheless, protecting users' privacy while finding a friend is a major security issue for such applications. In this paper, according to the definitions of privacy level, a new system is presented that helps users find their friends without finding private information. A user (called initiator) can find the best friend among the candidates and only intersect the traits exchanged with the best ones, while other users only know the intersection size of the attributes. The analysis and simulation results reveal that the proposed protocol is efficient with the ability to resist semi-honest and destructive attacks, besides providing higher compatibility efficiency [22].

Conclusion

In the world today, social networks have a key role in the relationships between people around the world. Thus, it has turned into an integral part of most people's lives. Nonetheless, the base of the emergence of these networks is to facilitate and shorten the communication path between people in society. In Iran, too, this not-so-emerging phenomenon is increasing its enthusiasm day by day. In the not-so-distant past, people may have had little knowledge of the nature and use of these networks, but these days, in everyday life, we see a diverse range of people talking and exchanging information about these networks. Various classes in society talk about it: young and old, literate and illiterate, men and women. Many people are against them and consider the existence of these networks as a cause of social harm and moral corruption for the classes of the society, and they want to close, close and filter them. On the other hand, others see them as manifestations of a new civilization and find their existence not only useful but necessary for social solidarity. Some are very opposed to them and consider the existence of these networks as a cause of social harm and moral corruption for the classes of society and want to close, close, and filter them, and on the contrary, others consider them as manifestations of a new civilization and their existence. Not only useful but also necessary for social cohesion. The widespread use of this phenomenon has many positive and negative consequences on our lives and, in some cases, has imposed inevitable consequences on us. This has been to the extent that some of the common terms in these networks will be part of the conversational culture of people in our society. The results of other studies indicate that the capacity of social networks at various individual and social levels could be benefited to identify problems and determine their solutions, establish social relationships, manage organizational affairs public policy, and guide people on the path to achieving goals. In addition to the myriad benefits of the Internet, there are disadvantages that a lack of familiarity with cyberspace can do for families. The family is the center of individual identity formation in all cultures. No individual can be defined apart from his family, and the family is the main building block of the individual and personality. The sacred center of the family is the best place for physical and mental education.

Social networks are of the spaces attracting a large audience. OSNs are usually web-based services that include online services, platforms, or sites where people can express their opinions and interests and share them with others. These networks have created a space where users can compensate for the limitations and obstacles of the real-life space and have created an opportunity for interaction, communication, and message transmission. However, security and privacy must be considered as well.

REFERENCE

1. Scott, J. Social Media Analysis, 1991, London Publications (Sage), translated by Fereshteh Nikofar.
1. Boyd DM & Ellison NB. Social network sites: Definition, history, and scholarship. Journal of Computer

Mediated Communication, 2008. 13(1): p. 210-230.
2. Scott.J, Stokman.F. “social networks”. International encyclopedia of the social & behavioral sciences, 2015, pp.473-477.
3. Stokman.F. “Networks:social”. International encyclopedia of the social & behavioral sciences, 2001, pp.10509-10514.
4. Griffiths.M, Kuss.D, Demetrovics. “Social networking addiction: an overview of preliminary findings”. Journal of behavioral addiction, 2014, pp.119-141.
5. Cornwell.B, Schafer.M. “social networks in later life”. Journal of handbook of aging and the social sciences, 2016, pp.181-201.
6. Brnads.U. “social network algorithms and software”. International encyclopedia of the social& behavioral sciences, 2015, pp.454-460.
7. Din.N, Yahya.S, Suzan.R, Kassim.R. “online social networking for quality of life”. Journal of social and behavioral sciences,2012, Vol.35, pp.713-718.
8. Heidemann.j, klier.M, probst.F. “online social networks: a survey of global phenomenon”. Journal of computer networks, 2012, Vol.56, Issue.18, pp.3866-3878.
9. Musial.K, kazienko.p. “social networks on the internet”. Journal of social network, 2013, Vol.16, issue.1, pp.31-72.
10. Amini Siahmezgi, R., and Rezapour, A.R. 2009, Community Recognition in Social Networks Using Data Mining Algorithms, The First Conference on Computer Science, Electrical Engineering, Communication and Information Technology in the Islamic World, Mashhad, Be Andish Company Avaran Tadbir Ghohestan.
11. Ebrahimzadeh, S., Rezaei Sharifabadi, S., and Masoumeh Karbalaei Agha Kamran, 2009, The Impact of Social Networks as a Source of Information on Information and Behavior Behavior, Fifth International Conference on Web Research, Tehran, University of Science and Culture.
12. Liwandouw.V, Wowor.D. “the existence of cryptography: a study on instant messaging”. Journal of computer science, Vol.124, pp.721-727, 2017.
13. M. Green, S. Hohenberger, and B. Waters, “Outsourcing the Decryption of ABE Ciphertexts,” *Proc. 20th USENIX Conf. Secur.*, pp. 34–34, 2011.
14. Junzuo Lai, R. H. Deng, Chaowen Guan, and Jian Weng, “Attribute-Based Encryption With Verifiable Outsourced Decryption,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 8, pp. 1343–1354, 2013.
15. J. Hur, “Attribute-based secure data sharing with hidden policies in smart grid,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2171–2180, 2013.
16. M. Bayat, H. R. Arkian, and M. R. Aref, “A revocable attribute based data sharing scheme resilient to DoS attacks in smart grid,” *Wirel. Networks*, vol. 21, no. 3, pp. 871–881, 2014.
17. S. S. M. Chow, “A Framework of Multi-Authority Attribute-Based Encryption with Outsourcing and Revocation,” *Proc. 21st ACM Symp. Access Control Model. Technol. - SACMAT ’16*, pp. 215–226, 2016.
18. K. Yang and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, 2014.
19. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in public clouds,” *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2268–2280, 2014.
20. T. Jung, X.-Y. Y. Li, Z. Wan, and M. Wan, “Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption,” *IEEE Trans. Inf. forensics Secur.*, vol. 10, no. 1, pp. 190–199, 2015.

21. Y. Wang, J. Hou, Y. Xia, and H. Z. Li, ``Ef_cient privacy preserving matchmaking for mobile social networking," against malicious users," *Concurrency Comput., Practice Exper.*, vol. 27, no. 12, pp. 2924_2937, 2015.