A Framework for Privacy and Security on Social Networks Using Encryption Algorithms

Hamideh Jashn[1], Behnaz Mahipour[1], Elaheh Moharamkhani[2]*, Behrouz Zadmehr[3]

[1] Department of Computer Engineering, Science and Research Branch, Isalamic Azad Uuniversity, Khuzestan, Iran
[2] Department of Computer Engineering, Institute of Higher Education Saeb, Abhar, Iran
[3] Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran
Corresponding author: elaheh.moharamkhani@gmail.com

Abstract

One of the most important technologies that has affected our lives today is cyberspace. On the other hand, one of the most important problems of social networks is the disclosure of users' information, i.e. the violation of their privacy. Therefore, protecting the privacy of users is very important, so the use of encryption methods is an important tool in ensuring the privacy and security of shared data users. The proposed framework of this paper is based on AES and RSA algorithms. This framework is designed to be decentralized and takes advantage of the AES and RSA algorithms to provide a framework that prevents unauthorized entities from accessing users' data and messages. Any safe method must be designed in such a way that there is no escape route for attackers and unauthorized entities. Therefore, our focus is on two important parts of secure methods, namely key management and privacy, which the results of this article show, the security assessment proved that our proposed framework is designed to be completely safe and correct, and increased security and efficiency.

Keywords: Social Networks, Privacy, Security, Encryption, Decryption
Article history: Submitted 10-May-2022; Revised 02-Jul-2022; Accepted 14-Jul-2022. Article Type: Research paper

https://doi.org/10.30495/ijsee.2022.1958369.1200

1. Introduction

Today, social networks have gained a lot of popularity among global web users. The use of these networks has penetrated different layers of users. These networks have specific applications and have significant impacts on their target community in each branch in which they operate. Social networks have introduced new methods of social communication. In terms of platform type, social networks can be divided into two categories: online and mobile. Each of these two categories, in terms of architecture and services, may be centralized or decentralized. Schemes that focus on protecting sensitive data, user relationships, and user-centric location. In addition, a clear classification of the types of architectures presented in each mobile and online social network is another key aspect of this research. Several models have been proposed to protect users' privacy. Each of them focuses on one or more users [1]. The main needs of users are to ensure privacy, confidentiality, access control and fairness when exchanging information in a network environment. To maintain confidentiality, there must be an item that ensures that user data and their social relationships are well protected. Components that may violate confidentiality include social media service providers and unfriendly users. Key management and dynamic nicknames are done. Due to the need for encryption and extraction operations due to encryption methods, they usually have high computational overhead and high memory complexity; in some cases, a compromise between the degree of confidentiality and these parameters [2]. In anonymity methods, the use of reconnaissance algorithms and the detection of user mobility patterns can jeopardize confidentiality, because given the time and place data of the collection, you can discover sensitive user data and social relationships. Therefore, anonymity must be unique from user data to complicate the relationships and data of a particular user in terms of access control, users as data owners must be able to control and manage access to their data. This means that only the data owner should be able to grant access to the data to other audiences. In addition, because users' social relationships are different at different times, the user should be able to update and make changes in their relationships at any time [3]. In the case of mobile social networks, there are two types of centralized and decentralized, which can be distinguished from each other based on the type of service to users. In the case of mobile social networks, there is the ability to provide mechanisms based on basic architecture. Of course, it is important to note that access to capabilities to meet the privacy needs of users will lead to time and computational overhead, which should be adjusted according to the importance of user needs. Encryption is one of the techniques, which protects users' privacy in social networks. Available encryption methods for users' privacy protection often differ in terms of their implementation, execution, and management methods. One of the challenges, which is always present in social networks is managing and creating keys and assigning them to users. In this paper, we tried to meet the needed requirements for users' privacy on social networks by providing a framework for social networks. This paper's main contribution is that we introduced an encryption method in social networks, which guarantees high security and privacy in social networks. We also focus on two important sections, which are key management and privacy in social networks, so these two sections are this paper's main contribution. The Keys management is such that we use RSA algorithm encryption in the master key exchange phase in social networks and AES encryption algorithm in the data and message encryption phase in social networks. And the important point is that the master keys of users are not exchanged raw, that is, first the keys are encrypted and then sent to friendly users on social networks, in the framework that we have provided, attackers are prevented from unauthorized access to users' data and messages.

The remaining parts of the paper is structured as follows:

In Section 2, we review the previous works. Section 3 represents is about the structure of social networks. Section 4 we offer a framework of the security and privacy in social networks. Section 5 presents the results and the comparative discussion of the proposed framework, And Section. 6 concludes the paper.

2. Previous work

Bigwood et al. [4] introduced the Persona method. It has a very important feature, which is the power of the user to divide friends into different groups. This method, like many methods, uses cryptography to maintain confidentiality; a technique that encrypts has chosen ABE, which is feature, based.

Raji et al. [5] proposed a peer-to-peer social network architecture with privacy and data availability called PESCA. It is a fully distributed social network with privacy enabled for social communication and data availability using diffusion encryption. It also links the availability of user-shared data to controlling user-assigned access to that data. As such, PESCA offers a replica placement strategy to ensure data availability.

Li et al. [6] proposed a lightweight secure data sharing scheme for mobile cloud computing. The design uses feature-based encryption with encrypted text policy (CP-ABE) to control access, but has changed the structure of the access control tree to make it more suitable for mobile cloud environments. This scheme transfers a large part of the centralized computation of the conversion of the access control tree in CP-ABE encryption from mobile devices to external proxy servers. To reduce the cost of cancellation, the user also introduces attribute description fields for lazy implementation, which is a troubling issue in applications based on CP-ABE systems.

Wang et al. [7] proposed a plan to increase the security and privacy of instant messaging for mobile social networking systems. This comprehensive plan for instant messaging security is based on Elliptic Curve Encryption (ECC) and Advanced Encryption Standard (AES). An offline key agreement process between users under the Daffy-Hellman (CDH) computational assumption is designed by short-term periodic key updates. The proposed scheme supports replay attack denial and counterfeit attack denial by using time labels and the Elliptic Curve Digital Signature Algorithm (ECDSA).

Fugkeaw et al. [8] proposed a special access control model with an effective key update function in the data outsourcing environment. This access control is based on combining feature-based encryption with encrypted text policy (CP-ABE) and role-based access control (RBAC). The proposed design is presented in the original CP-ABE design with the aim of improving the management of feature and key updates. In this scheme, the user key is included in the attribute certificate, which is used to decrypt the encrypted text with CP-ABE policy. If any changes include updating or canceling features that appear on the existing key, the key in the feature certificate (AC) will be updated as soon as access is requested. This significantly reduces the overhead of updating and distributing keys to all users simultaneously compared to existing CP-ABE plans.

Qiu et al. [9] proposed a proactive user-centric plan for secure data usage using semantic feature-based access control for mobile cloud computing in the financial industry. This scheme uses a semantic access technique to generate a feature-based data protection perspective. The plan provides a preventive user-centric perspective by avoiding unexpected operations or unexpected parties on the cloud side for the purpose of data protection. The proposed scheme provides a high level of secure stability due to the configuration of data access based on the configuration of user feature restrictions.

Wang et al. [10] review the data storage and sharing system of decentralized storage systems and provide a framework that includes IPFS decentralized storage system, atrium chain block, and feature-based encryption technology (ABE). In this context, the data owner has the ability to distribute encryption keys to data users and encrypt shared data by setting access policies, and this scheme provides precise access control over the data. At the same time, based on the smart contract in Atrium block chain and keyword search in the text of decentralized storage systems, which solves the problem of not returning all the searched results or returning the wrong results in traditional cloud storage systems. They also simulated their design using the Linux operating system and the official Ethereum Rinkeby test network.

Malluhi et al. [11] introduced feature-based decentralized cryptographic schemes with encrypted text policies for devices with low processing resources. They proposed two decentralized feature-based encryption schemes with encrypted text policy. Suggested designs have some nice features like fixed size secret key, fast decryption, optimized size encrypted text and fine access control. These schemes consist of four algorithms including setup, extraction, encryption, and decryption. The problem of key transfer, which is one of the main problems of cryptographic systems, has been solved in the proposed designs. The first design suffers from the bottleneck problem. For this reason, with the expansion of the first plan, they have reached the second plan, which solves the problem of key deposit and supports revocation.

Liu et al. [12] developed a reliable and efficient plan for sharing multimedia messages on the mobile social network. This method supports flexible and fine-grained access control. The encryption algorithm used in this method is feature-based encryption with encrypted text policy. Identity-based cryptography has also been used to anonymize identities on the social network. This method consists of five entities including data owner, data user, and cloud server, proxy and certification authority. In this method, users' messages are encrypted using AES symmetric encryption, and the symmetric key of the AES algorithm is encrypted by feature-based encryption with encrypted text policy. The production of feature-based cryptographic keys is the responsibility of the certification authority, but the data owner does the production of AES symmetric keys. The main drawback of this method is the lack of support for dynamic cancellation at a high rate of group member changes.

Yahiatene et al. [13] proposed a method of privacy in online social networks using distributed feature-based cryptography. In this method, a new framework for protecting privacy in online social networks is presented based on two main concepts, including cloud computing and feature-based cryptography. Cloud computing is used to store outsourced data by a third-party entity. By transferring data to this third party, data control is lost so no one knows where the data is stored. For this reason, this method provides a feature-based encryption scheme with multiple issuance references that provides flexible access control, and only users with the correct keys can access the data. Users protect this method against vulnerabilities; third party presence and social network providers, and is resistant to feature collusion attacks.

Qiu et al. [14] propose a hierarchical access control method with scalable data sharing in the cloud. This proposed method is based on key aggregation encryption, and the scalability of the data sharing allows the data owner to share the data with any group of users. In the proposed scheme, the size of each key or encrypted text is fixed and irrelevant to the scale of each user's hierarchical structure. This method improves key management convenience by eliminating key derivation, which is widely used in existing hierarchical key assignment methods. In addition, the proposed design reduces the overhead of user updates by introducing the re-encryption to hierarchical scenarios. This method consists of cloud server, certification reference and hierarchical structure of users.

Chaudhari et al. [15] proposed a fine-grained privacy control framework using searchable encryption. Search encryption in this scheme is based on a single keyword that is used for applications where multiple data owners upload their data to the server and then multiple users can access that data. This method uses feature-based encryption that allows the user to access any selected subset of data stored in the cloud without revealing their access rights to the cloud server. This design is resistant to attack with the selected password in Oracle's random. In the proposed method, in addition to the feature center, also a token generator generates security tokens for users to access data.

Ibtihal et al. [16] used convergent encryption as a service for images outsourced in the mobile cloud-computing environment. This method emphasizes the safe outsourcing of images. For this purpose, in this method, a safe architecture is introduced, which consists of two clouds. The first is the private cloud used for encryption and decryption, and the second is the public cloud used for storage. In this method, the private cloud is implemented using the open source open source software platform, while cryptography is considered as an important service. For encryption, the Paillier fusion algorithm is used, which is specially designed for images. The homogeneity test is performed using the Watermarking DWT algorithm.

Chen et al. [17] proposed methods for sharing social data while maintaining safety in modern large social knowledge systems. In this way, by combining the concepts of information fragmentation with distributed system architecture, they improve traditional social data protection schemes and create a new social data protection scheme. In this proposed method, the protection of social images is used as the basis of the proposed scenario. In this method, two separate social platforms are used to protect the data. The cryptographic algorithm used in this method is of the selected cryptographic type. In this method, the images are protected into two small parts and the large public part is divided, the small part is stored in the first social platform and the large part in the second social platform. When requesting access to this image, a user must receive both pieces from both social platforms.

Zhang et al. [18] proposed a novel blockchain-based privacy-preserving framework for online social networks, called BPP. Combined blockchain and public-key cryptography technique, the BPP framework can achieve secure data sharing, data retrieving, and data accessing with fairness and without worrying about potential damage to users' interest. Specifically, based on blockchain and public key encryption with keyword search technique, a secure, fair and efficient keyword search algorithm is proposed, with which the BBP framework realises privacy preservation of user's query and then obtain accurate query results with assurance and without needing for any further verification operation in online social network.

Garompolo et al [19] presented a disruptive approach, which exploits the availability of a new class of Internet of Things (IoT) devices with autonomous social behaviors and cognitive abilities. Such devices can be leveraged as friendship intermediaries between devices' owners who are connected to a DOSN platform and share the same interest. They demonstrated that clear advantages could be achieved in terms of increased percentage of Interested Reachable Nodes (a specific measure of Delivery Ratio) in distributed social networks among humans, when enhanced with so called Mediator Objects adhering to the well-known social IoT (SIoT) paradigm.

3. Structure of social networks

Social networks can be considered as graphs with nodes (users of social networks), edges (communication between users) and tags of nodes and edges (including attributes related to users and attributes of connections). Due to the structure and relationship between the entities, we see data continuity in these networks. Graphs that represent social networks can be weighted and unweighted, labeled and bad and labeled directional and non-directional, static and poo.

The social network marker is done in the form of (V, E) G. In it, V represents the set of nodes representing the users and E represents the set of nodes that represent the relationship information between users. Social networks are modeled as tagged graphs. These ifs may contain the following information [20, 21].

A) Security and privacy

Security and privacy are completely different. A security issue occurs when a hacker finds unauthorized access to site protection emails. Violation of privacy includes unauthorized access to privacy information and does not necessarily constitute a breach of security. These two types of violations in social networks are so intertwined that, if the site security network is violated. Easy access to personal information is possible. With these interpretations, it can be said that the potential damage is done. It depends on the extent of his involvement in social networks and the amount of information he shares and his willingness to share [22].

B) Types of attacks on social networks

Recognition attacks on social networks can be identified based on pseudo-traits and using previous knowledge. The enemy exploits weaknesses in the design and implementation of anonymity patterns and launches attacks to violate privacy that is more personal. Attacks on social networks are divided into two categories:

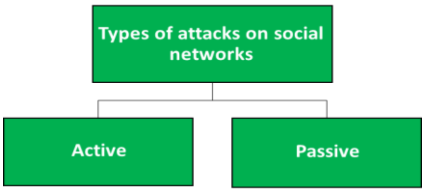

Fig. 1. Types of attacks on social networks

C) Encryption protocols

In general, a cryptographic protocol is a set of mathematical rules and relationships that provide how to combine cryptographic algorithms and use them to provide a particular cryptographic service in a particular application.

D) Cryptographic algorithms

Any mathematical rhythm or function is said to be in use in the cryptographic protocols due to the need for specialization in cryptography. د. The term chronological rhythm model is a comprehensive concept and it is not necessary for every rhythm model in this category to be used directly to store the information used. Rather, the expenditure of work on the relation to the chronograph is considered [23].

E) Security of cryptographic systems

The security of cryptographic systems depends on two main factors:

- The power of the algorithm
- Key length

F) Types of cryptographic systems in terms of key confidentiality

Sophisticated cryptography techniques do not use the same methods of displacement by substitution. Instead, they use a secret key to control for a long period, using complex shifts and alternatives. Cryptographic keys and cryptographic algorithms work together to convert an original text into a cryptographic text. In most cases, the encryption algorithm is fixed and known, and it is the encryption key that generates a unique version of the encrypted information. Some researchers have divided systems into two types, symmetric and asymmetric, in terms of the relationship between cryptographic transformations and decryption.

G) Standard advanced encryption

In order to increase the security of the crypto currency in late 2001, a new model called AES was adopted. Rijndael block chain was proposed as a better rhythm model for 128-bit blocks using 128-92 and 256-bit keys [24].

H) Asymmetric RSA encryption

The RSA algorithm takes its name from the beginning of the name of its inventors. This algorithm uses two general and specific keys for the encryption process. The public key is used to encrypt the message and the private key is used to decrypt the message. In this method, the following three algorithms are used in the cryptographic process:

- Key generation algorithm
- Encryption algorithm
- Decryption algorithm

4. The proposed framework approach for security and privacy in social networks

In this section, we describe our proposed framework in detail and in phasing. The proposed framework is a safe and comprehensive plan that protects the privacy and security of users in online social networks. This method is designed to be decentralized, which eliminates the need for centralized social network server access to content exchanged between users. Concentrated methods cannot protect users' privacy due to unlimited access to social network servers if they can protect users against attackers.

A) Model of the proposed framework

In this section, we will comprehensively show an overview of the proposed framework. This method is designed to be decentralized, which protects the privacy and security of social network users. In this method, users have an AES symmetric master key that encrypts their data using this key. The user key is also encrypted and exchanged by RSA encryption. In fact, the master keys of users are not exchanged raw; first the key is encrypted and then sent to friendly users. The framework consists of three parts, including social network servers, proxy servers, and member users. The role of the social network server is to provide data exchange services, the role of proxy servers is to generate RSA keys, and the role of member users is to send and receive data at the level of the proposed framework. Figure 2 shows this overview.

Table.1.
Description of the proposed framework

Social network server	*Proxy servers*	*Alice*	*Bob*
Generate and exchange data and messages -Generate and store its own symmetric master key -Storing its own public and private RSA keys -Storage of RSA public keys and user friendly	-User registration -Allocation of storage space -Provide interests and data	-Generate public and private RSA keys for users	-Generate and exchange data and messages -Generate and store its own symmetric master key -Storing its own public and private RSA keys - Storage of RSA public keys and user friendly

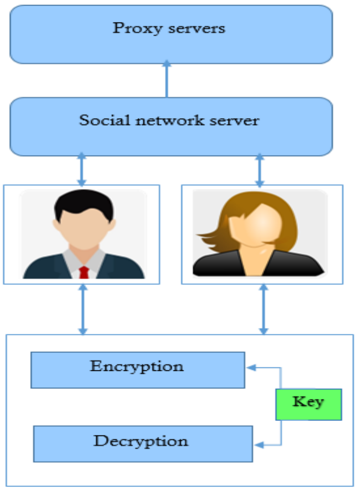

Fig. 2. Proposed framework

B) *Existences of the proposed method*

Each system is made up of a series of entities that execute the structural process of that system. Each of these entities has a series of tasks, maps, and properties. Three entities, including social network servers, proxy servers, and social network member users, play a role in the proposed method. In the following, we will describe the tasks, maps and characteristics of each of these entities:

The tasks of this entity include registering users, allocating storage space, creating an environment for sharing interests and data, communicating with other users, and searching for users. Users communicate with their friends through this server, which is encrypted. Encrypting data and messages prevents the social network server from being informed of the content exchanged between users.

Proxy servers are responsible for generating users' RSA keys. In the proposed framework, there are a number of proxy servers that play a hierarchical role. In fact, this hierarchy includes a central proxy server and several subset proxy servers. The central proxy server has the task of connecting users to different proxy servers so that the computational load is distributed over all proxy servers.

The tasks of users in the proposed framework include producing and sharing content, exchanging messages and data with other users, and sharing interests. Also in the proposed method, users have a symmetric master key that the user generates this key and no entity other than authorized users have access to this key.

C) *How to connect social network server and central proxy server*

The social network server and the central proxy server are directly connected to each other. However, neither has access to data stored in the other. Proxy servers used to generate RSA keys also communicate directly with social network users. When two users want to exchange messages and data, the social network server sends the unique ID of these users to the central proxy server. The central proxy server then forwards their request to one of its affiliate proxy servers, and the affiliate proxy server generates the RSA keys for those users. This operation is performed due to the computational load of key generation.

D) *Encryption keys of the proposed method*

In any secure framework that uses cryptographic algorithms, there are a number of cryptographic keys that are generated, exchanged, and stored by its entities. How these keys are stored guarantees security and privacy. In the proposed framework, there are three cryptographic keys, which are as follows:

This key is used to symmetrically encrypt and decrypt user data and messages. The user generates this key individually and without the cooperation of other entities. This key is only available to users who are authorized by the key owner. Social network servers, proxy servers and unauthorized users cannot access this key. The symmetric master key is exchanged encrypted using the RSA algorithm.

Subsystem proxy servers that are used to encrypt users' master keys create this key. Disclosure of the RSA public key does not pose any security issues, so it does not need to be maintained. After requesting users from the proxy server, this key is provided to them. This key is the third and last key of the three keys in the proposed method. Subscriber proxy servers generate this key and make it available to users. This key is provided to users securely and the social network server is not aware of its content.In the following, we describe the phases of the proposed framework:

Phase 1: Registration of users in the social network

In this phase, users register their identity information and characteristics in the social network server. Each user must have a unique ID to register. This ID can be a mobile phone number or email. In the proposed method, this unique identifier is the user's mobile number. The steps for registering users' names in the social network of the proposed framework are as follows:

Algorithm 1: Registration of users in the social network

```
Start
    User: Register_PhoneNumber ();
    OSN: Send_To_User (Authenticate Code);
    User: Send_To_OSN (Authenticate Code);
    OSN: Verify (Authenticate Code);
    OSN: Send_To_Proxy (User's PhoneNumber);
    Proxy: Save (User's PhoneNumber);
Finish
```

Phase 2: Exchange phase of the master key users in the social network

In the proposed framework, each user has a symmetric master key that encrypts their data and messages using this key and sends it to friends. This key guarantees the privacy and security of social network users, so it must be exchanged completely safely and correctly. If this key is exposed, the privacy of the user's data and messages will be compromised. To this end, in the proposed framework, we provide a safe and correct method of key exchange that prevents unauthorized entities from accessing this key. To facilitate the description of this phase of the proposed method, we name the first user Alice and the second user Bob.

Here, in order to better understand this phase, we describe its implementation process in Algorithm 2 as pseudo-code.

Algorithm 2: Exchange phase of the master key users in the social network

```
Start
    Alice: Send_To_OSN (Key Exchange Request)
    Bob: Send_To_OSN (Key Exchange Request)
    OSN: Send_To_Proxy$_{Cent}$ (ID$_{Alice}$, ID$_{Bob}$)
    Proxy$_{Cent}$: Select_Proxy$_{Sub}$ ()
    Proxy$_{Cent}$: Send_To_Proxy$_{Sub}$ (ID$_{Alice}$, ID$_{Bob}$)
    Proxy$_{Sub}$: Generate_RSA_Keys ();
    Proxy$_{Sub}$: Send_To_Users (RSA Keys);
    Alice: RSA_Encryption (Key$_{Alice}$)
    Bob: RSA_Decryption ()
    Bob: Save (Key$_{Alice}$)
    Bob: RSA_Encryption (Key$_{Bob}$)
    Alice: RSA_Decryption ()
    Alice: Save (Key$_{Bob}$)
Finish
```

Phase 3: Phase of encrypting data and messages in social network

The data and messages generated in the proposed method must be exchanged in encrypted form so that unauthorized entities cannot read or access them. For this purpose, users' data and messages are first encrypted and then sent in the proposed framework using the symmetric AES algorithm. To facilitate the description of this phase of the proposed method, we name the first user Alice and the second user Bob, who is the sender of the Alice data and the recipient of that Bob.

Here, in order to better understand this phase, in algorithm 3, we describe its implementation process in pseudo-code.

Algorithm 3: Phase of encrypting data and messages in social network

```
Start
    Alice: Generate_Data ()
    Alice: AES_Encryption (PT)
    Alice: Send_To_Bob (CT)
Finish
```

Phase 4: Phase of decoding data and message in social network

In the previous phase, the data and messages generated by the users were encrypted and then sent. The recipient user must decrypt this data so that it can be read. For this purpose, the data-decoding phase must be performed.

Finally, in order to better understand this phase, in algorithm 4, we describe its implementation process in pseudo-code.

Algorithm 4: Phase of decoding data and message in social network

```
Start
    Bob: Recovery (Key$_{Alice}$)
    Bob: AES_Decryption (CT)
    Bob: Save (PT)
Finish
```

E) Changing and updating the user's master key

If the user feels that their master key has been exposed or compromised, they may want to change the key. For this reason, the user must notify all authorized users after changing their master key. Therefore, when communicating with friendly users, the master key exchange phase must first be re-run. This action allows the user's friends to be informed of his updated key and use it in new communications. Here the key exchange phase is performed with a slight difference. In this way, this phase is done one-way, because there is no need for the second user to send his key to the first user. Because in previous communications, it sent its master key to the first user, and now, since it has not changed, it does not need to be exchanged.

5. Simulation and performance evaluation

A) Evaluation of key management of the proposed method

In security methods that use cryptographic algorithms, the security of the entire system is compromised if the key is not generated, exchanged, and stored securely. For this purpose, in the proposed framework, cryptographic keys are managed securely and correctly, which ensures that the privacy and security of users in the social network are fully protected. To prove this claim, we now examine the three keys of the proposed method in terms of how the key is generated, exchanged, and accessed:

The subset proxy server creates this key at the request of the owner user. Disclosure of this key has no security restrictions and is easily made available to friendly users. Alice's friends, for example, are aware of her public key and use it to exchange secure keys.

The proxy servers of the subset make this key, like the previous key,, except that it should not be disclosed under any circumstances. The only virtual entity to which it has access is the key user. For this purpose, after generating this key by the subsystem proxy server, it will be provided only to the user who owns it. Therefore, none of the entities in the proposed method has access to it. This key is not exchanged in any way and is reserved by its owner. Therefore, the privacy of users' RSA private keys is not compromised under any circumstances.

The most important security element is the proposed method of this key. Each user's master key is generated by him. The user uses this key to encrypt his data. This key is first encrypted by the RSA algorithm during exchange and then sent. For this purpose, it is exchanged in a completely safe way. Therefore, this key is not accessible by unauthorized entities.

Table.2.
Key management case evaluation of the proposed method

Keyname	***Key manufacturers***	***Authorized units***	***Unauthorized units***	***role of the key***	***Key exchange***
PubK	Subset proxy server	All users	-	Encrypt key users	It is sent to users by a subset proxy
PrvK	Subset proxy server	The user owns the key	All users, social network servers and proxy servers	Decrypt key users	It is sent by the subset proxy to the user who owns it
Key$_{User}$	The user owns it	Key owner and user friends	Unauthorized users, social network servers and proxy servers	Encrypt and decrypt user data and messages	It is exchanged encrypted by the RSA algorithm

B) Evaluation of privacy in the proposed method

Privacy in social networks is one of the most important concerns of users in these systems. For this reason, their privacy is maintained when a completely safe and correct method is provided. The substantiate this claim, we further examine the access of each authorized and unauthorized unit to user data

A social network server needs access to their master key to access users' data. Because the users' master key is exchanged encrypted by the RSA algorithm, it needs to have the destination user's private RSA key to decrypt it. Now, since its owner holds the destination user’s private RSA key, the social network server is unable to decrypt it. Therefore, users' privacy is fully protected against unauthorized access to the social network server.

Proxy servers also require access to the user's master key to access user data. Because the RSA algorithm and the proxy encrypt the user’s master key server generates user's RSA keys, it is assumed that it can access the user's master key. However, because users pass their master key encrypted through the social network server, the proxy server cannot track and decrypt it. Therefore, proxy servers are also unable to access user data. So users' privacy is protected against unauthorized access to these servers.

Unauthorized users can only access user data if they know their master key. Therefore, if the user does not send their master key to them, unauthorized users will not be able to access this key. In addition, if the user owns the data, has already sent his / her master key to the user and now does not want to read his / her new data to that user, by performing the update phase of the master key, he / she will prevent this unauthorized access. Therefore, users' privacy is protected from unauthorized access.

C) Assessing the safety of the proposed method against attackers

In secure data exchange methods, attackers reveal the privacy of users' data. This violates the privacy and security of users. Therefore, any secure data exchange method must be designed to be resistant to these attacks. The proposed method is designed in such a way that it resists such attacks in the best way and maintains the privacy and security of users. We will first describe each of these attacks below, and then prove by reason why the proposed framework is resistant to them. The attackers' attacks are as follows:

The attack takes place in a way that the attacker intercepts the data being transmitted, eavesdrops on it through the transmission channel, and retransmits important information such as username and password or changing the information. Because in the proposed method, the master key is exchanged encrypted, this attack is not executable in our framework.

The middle attack occurs when an attacker is placed between two nodes and exchanges information in such a way that both parties are not aware of his existence. In the proposed framework, due to the correct and safe execution of the key management method, the middle man attack is not executable. This is because the attack is executed when the key management is designed to be simple and poorly designed.

A booster is a program or device that can read or monitor network transactions. If the packets are not encrypted, the scanner can get an overview of its contents and try to exploit them. User information and data are exchanged in encrypted form. In the proposed scheme, because the data is exchanged in full-encrypted form, this attack is also not executable in our method.

In this attack, one person or program will introduce itself as another. In our method, due to the use of the public key's RSA key, it is not possible to use the forgery attack and receive the master key. Because if the attacker wants to forge the user's identity, it is not possible to decrypt and access the user's master key due to not knowing the RSA's private key. Therefore, the proposed method is also resistant to this attack. Now that we have shown the reason for the resistance of the proposed method against these attacks, in Table 3, we will compare the proposed framework with the methods presented in Articles [25] and [26] on a case-by-case basis.

Table.3.
Comparison of the proposed framework in terms of attack resistance with other articles

Method name	*Resistance to Spoofing Attack*	*Resistance to Sniffer Attack*	*Resistance to Man-in-middle Attack*	*Resistance to Replay Attack*
Ref [25]	-	✓	✓	-
Ref [26]	-	✓	✓	-
Proposed method	✓	✓	✓	✓

Here we evaluate its efficiency by implementing the cryptographic algorithms used in the proposed method. Next, we first measure the key exchange phase and then the data exchange phase.

D) Experimental settings

We used the Java language to implement the proposed method algorithms. We used the programming library [27] to implement the RSA and AES algorithms. Table 4 describes the mobile specifications and the implementation environment of the proposed framework algorithms on a case-by-case basis.

Table.4.
Mobile specifications and implementation environment of the proposed method algorithms

Operating system	*CPU frequency*	*Cache*	*Processor*
Android 8.1	1.4 GHz	1 GB	Exynos 7570 Quad
Used libraries	***Programming language version***	***Programming language***	***IDE environment***
JPBC and Cryptox	1.8	Java	Eclipse Indigo

E) Discussion

In the proposed method, users exchange their master keys securely using RSA encryption. For this reason, in order to exchange the master keys of users, one time is spent for encryption and one time for decryption of RSA. The total encryption and decryption time are the time used for the exchange. We also note that we have spared no time generating RSA keys by proxy servers. Next, we first show the encryption and then the decryption of RSA in the form of a graph, and finally we depict the key exchange diagram, which is the result of the total time of both diagrams. We also compare with RC2, RC4, 3DES and DES algorithms the results of which show the high performance of our prosed framework. And we use RSA-2048 encryption to encrypt users' master keys, which are 128, 192 and 256 bits based on the type of AES algorithm chosen.

This diagram is the sum of RSA encryption and decryption times, which is the result of key exchange time between users, because users have to perform an RSA encryption and decryption operation to exchange the key in order to access the key. The master result of these two graphs is the key exchange diagram or the same diagram (5), which shows the time spent on the master key exchange between social network users.

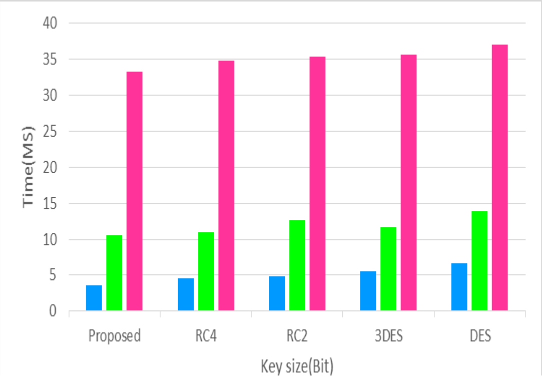

Fig. 3. Time to encrypt users' master keys

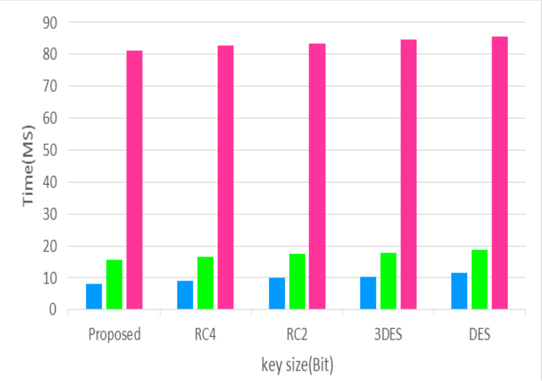

Fig. 4. Time to decrypt users' master keys

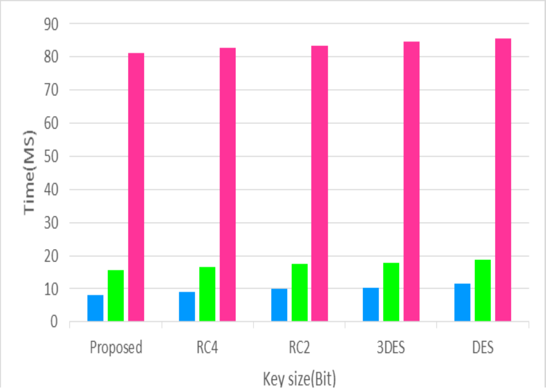

Fig. 5. Time to exchange users' master keys

In this section, we evaluate data exchange between users in terms of efficiency. The data is first encrypted by the sender with the AES algorithm and then decrypted by the receiver. For this reason, in the proposed method, the data exchange time between users will be the sum of the AES encryption and decryption time. Therefore, in separate diagrams, we first plot the AES encryption time, the AES decryption time, and finally the data exchange time diagram. For evaluation, we used data with a size of 0.001, 0.01, 0.1, 1 and 100 MB. In this diagram, we have depicted the time of data exchange between social network users. In this social network, the proposed method, when data is to be exchanged, is first encrypted AES symmetrically and then decrypted symmetrically at the destination, so when the time is spent exchanging data between source and destination Is the product of the sum of AES symmetric encryption and decryption times. Therefore, we have plotted the data exchange time in a separate graph, which is the sum of the AES encryption and decryption time.

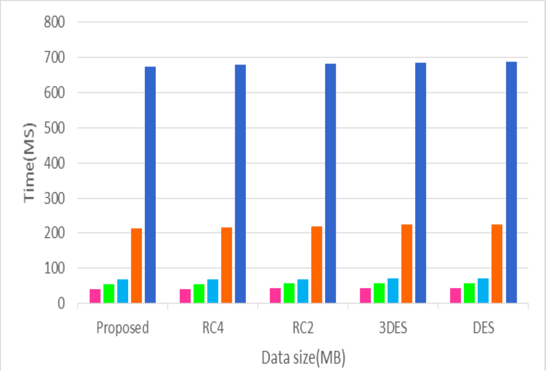

Fig. 6. Symmetric encryption time of data

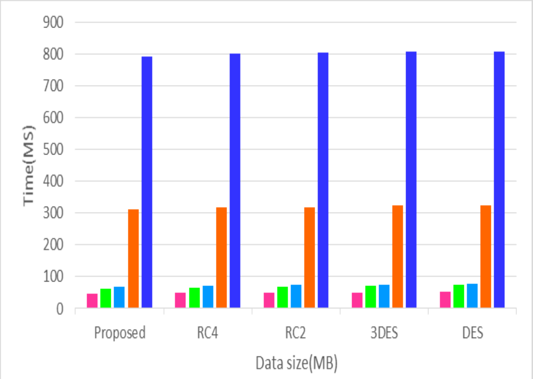

Fig. 7. Symmetric decryption time of data

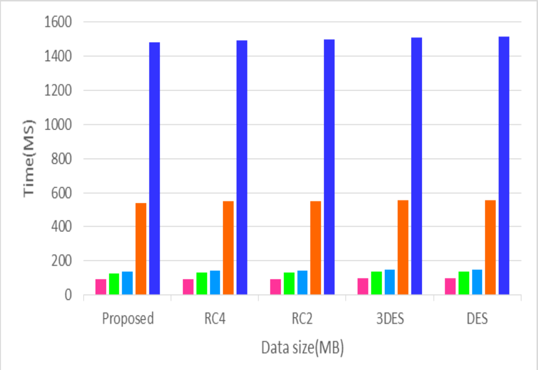

Fig. 8. Data exchange time

6. Conclusion

In this article, we present a completely safe and correct way to protect the privacy and security of users in social networks. In this framework, using the advantages of AES and RSA algorithms, we provide a framework that prevents unauthorized entities from accessing users' data and messages. Any safe method must be designed in such a way that there is no escape route for attackers and unauthorized entities. To this end, we have targeted from the beginning two important parts of secure methods, namely key management and privacy, in which proper and secure key management is the most important element of a security method. In the proposed method, we exchanged users 'master keys using RSA encryption, which prevents attackers and unauthorized entities from accessing users' master keys. Protecting users' key keys protects their privacy. Because if the key is exchanged completely securely, no person or entity will be able to decrypt user data. Finally, we evaluated the proposed method in terms of security and efficiency. We first evaluated the different parts of the method separately in terms of key management, privacy, and resistance to various attacks. Then, to evaluate the efficiency, we discussed the key exchange time and data exchange time and proved the efficiency of the proposed method.

References

[1]. Xiao, X., Chen, C., Sangaiah, A. K., Hu, G., Ye, R., & Jiang, Y. (2018). CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks. Future Generation Computer Systems, 86, 863-872.

[2]. Facebook Privacy Policy (2017) Facebook Privacy Policy (2017). April 2017 Available at http://facebook.com/policy.php. Accessed Apr 2017.

[3]. da Silva, P. M., Dias, J., & Ricardo, M. (2017). Mistrustful P2P: Deterministic privacy-preserving P2P file sharing model to hide user content interests in untrusted peer-to-peer networks. Computer Networks, 120, 87-104.

[4]. Bigwood, G., Rehunathan, D., Bateman, M., Henderson, T. and Bhatti, S., 2008, October. Exploiting self-reported social networks for routing in ubiquitous computing environments. In 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (pp. 484-489). IEEE.

[5]. Raji, F., Jazi, M. D., & Miri, A. (2014). PESCA: a peer-to-peer social network architecture with privacy-enabled social communication and data availability. IET Information Security, 9(1), 73-80.

[6]. Li, R., Shen, C., He, H., Gu, X., Xu, Z., & Xu, C. Z. (2017). A lightweight secure data sharing scheme for mobile cloud computing. IEEE Transactions on Cloud Computing, 6(2), 344-357.

[7]. Wang, Z., Ma, Z., Luo, S., & Gao, H. (2018). Enhanced instant message security and privacy protection scheme for mobile social network systems. IEEE Access, 6, 13706-13715.

[8]. Fugkeaw, S., & Sato, H. (2018, March). Enabling Dynamic and Efficient Data Access Control in Cloud Computing Based on Attribute Certificate Management and CP-ABE. In 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP) (pp. 454-461). IEEE.

[9]. Qiu, M., Gai, K., Thuraisingham, B., Tao, L., & Zhao, H. (2018). Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future Generation Computer Systems, 80, 421-429.

[10]. Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. Ieee Access, 6, 38437-38450.

[11]. Malluhi, Q. M., Shikfa, A., Tran, V. D., & Trinh, V. C. (2019). Decentralized ciphertext-policy attribute-based encryption schemes for lightweight devices. Computer Communications, 145, 113-125.

[12]. Liu, X., Sun, J., Yang, W., Jiang, M., & Yang, F. (2019). Ensuring efficient multimedia message sharing in mobile social network. Multimedia Tools and Applications, 78(22), 31003-31017.

[13]. Yahiatene, Y., Menacer, D. E., Riahla, M. A., Rachedi, A., & Tebibel, T. B. (2019, April). Towards a distributed ABE based approach to protect privacy on online social networks. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-7). IEEE.

[14]. Qiu, Z., Zhang, Z., Tan, S., Wang, J., & Tao, X. (2019). Hierarchical Access Control with Scalable Data Sharing in Cloud Storage. Journal of Internet Technology, 20(3), 663-676.

[15]. Chaudhari, P., & Das, M. L. (2019). Privacy preserving searchable encryption with fine-grained access control. IEEE Transactions on Cloud Computing, 9(2), 753-762.

[16]. Ibtihal, M., & Hassan, N. (2020). Homomorphic encryption as a service for outsourced images in mobile cloud computing environment. In Cryptography: breakthroughs in research and practice (pp. 316-330). IGI Global.

[17]. Chen, X. (2020). Security-preserving social data sharing methods in modern social big knowledge systems. Information Sciences, 515, 404-416.

[18]. Zhang, S., Yao, T., Arthur Sandor, V. K., Weng, T. H., Liang, W., & Su, J. (2021). A novel blockchain-based privacy-preserving framework for online social networks. Connection Science, 33(3), 555-575.

[19]. Garompolo, D., Molinaro, A., & Iera, A. (2022). Bridging separate communities with common interest in distributed social networks through the use of social objects. Future Generation Computer Systems, 129, 440-452.

[20]. Cheng, J., Fu, A. W. C., & Liu, J. (2010, June). K-isomorphism: privacy preserving network publication against structural attacks. In Proceedings of the 2010 ACM SIGMOD International Conference on Management of data (pp. 459-470).

[21]. Bhagat, S., Cormode, G., & Srivastava, D. (2010). Prediction promotes privacy in dynamic social networks. In 3rd Workshop on Online Social Networks (WOSN 2010).

[22]. Sahinoglu, M., Akkaya, A. D., & Ang, D. (2012). Can we assess and monitor privacy and security risk for social networks”. Procedia-Social and Behavioral Sciences, 57, 163-169.

[23]. DaemenJ, R. (2002). TheDesignofRijndael: AEStheAdvanced Encryption Standard.

[24]. Daemen, J., & Rijmen, V. (2001). Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology. 19-22.

[25]. He, Z., Cai, Z., Han, Q., Tong, W., Sun, L., & Li, Y. (2016). An energy efficient privacy-preserving content sharing scheme in mobile social networks. Personal and Ubiquitous Computing, 20(5), 833-846.

[26]. Yang, F., Pu, Y., Hu, C., & Zhou, Y. (2020, September). A blockchain-based privacy-preserving mechanism for attribute matching in social networks. In International Conference on Wireless Algorithms, Systems, and Applications (pp. 627-639). Springer, Cham.

[27]. “javax.crypto,”Oracle.[Online].Available: https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html.