Evolutionary Intelligence
https://doi.org/10.1007/s12065-020-00375-y

SPECIAL ISSUE

A novel authentication and authorization scheme in P2P networking using location-based privacy

B. N. Jagdale[1] · **J. W. Bakal**[2]

Received: 15 October 2019 / Revised: 24 January 2020 / Accepted: 21 February 2020

Abstract
In recent years, peer-to-peer (P2P) network has reached popularity in file sharing as it is a distributed and decentralized network architecture. As there is no centralized authority, there arise various attacks, which lead to insecurity in the network. Thus, the security issues of the P2P networks are to be considered with more care. This paper proposes an authentication and authorization approach, named fuzzy enabled advanced encryption standard (AES)-based multi-level authentication and authorization to offer security against various kinds of attacks that occur in the P2P networks. Here, the authentication is carried out with the security factors, namely location profile, one-time password, spatial information, session password, a hashing function, and so on. Initially, the user and the server are registered in the authentication process, and then, hashing functions and AES are used to perform multi-level authorization and authentication processes. Thus, the proposed scheme improves the security of the P2P network. Using the proposed system, the hit ratio obtained is 0.9, and the success rate is 0.7666.

Keywords Location-based privacy · Authentication · Authorization · P2P network · Fuzzy

Abbreviations

P2P	Peer-to-peer
AES	Advanced encryption standard
TTP	Trusted third party
LBS	Location-based services
AA	Attribute authority
ACs	Attribute certificates
ATRA	Adaptive trusted request and authorization
OSNs	Online social networks
OOB	Out-of-band
DES	Data encryption standard
NIST	National Institute of Standards and Technology
3AKEP	Triple-authenticated key exchange protocol for peer-to-peer networks
Privacy DLP	Privacy data leakage prevention

1 Introduction

Unlike centralized facilities, P2P systems perform very attractively, as their decentralized and distributed nature makes them scalable, efficient bandwidth, and high fault-tolerant, they do not need any special administrative arrangements. Approximately about 60% of the Internet's traffic [1] depends on P2P applications. These P2P content distribution applications are very popular throughout the world, among millions of users. The P2P application allows all its users to participate, search, and receive digital content in a distributed manner. Considerable attention in the research community [2], is received by the content distribution in P2P. The P2P technology for content distribution systems acts very useful to both content providers and the end users. From the point of view of media companies, the technology in P2P helps them to produce valuable content, which is available to a large number of users at very low cost and improved performance. These are the effective features of the media companies towards P2P systems adaption, like BitTorrent [3]. One of the most popular P2P distribution systems used on the internet is the BitTorrent, as it is responsible for a large amount of traffic on the internet. In the same way, Internap [4], a managed P2P content distribution application is used, which allows the content owners and the media companies at

✉ B. N. Jagdale
bnjagdale6@gmail.com

J. W. Bakal
bakaljw@gmail.com

[1] Faculty at SCET, MIT World Peace University, Pune, India

[2] Principal, S S Jondhale College of Engineering, Thane, India

Published online: 02 March 2020

a very low delivery cost to publish, distribute and track their games, videos and softwares. Additionally, the audio, video, and software files can be easily accessed and downloaded by the users within a short period [5]. As P2P provides a variety of services [6], its architectures have achieved more popularity in the last years. Due to the presence of inherent weak point in the P2P network, several security threats are rising when applied to various areas, although it is a popular network service on the Internet in recent years. Thus, P2P has security issues which are similar to existing Internet environment [7], as it is an overlay network on the internet.

In the case of universal networks, healthy relationships between the users must be improved to support the business applications. Thus, it requires pervasive security services, which depend on strong authentication and authorization mechanisms [8]. To solve the problems associated with the security issues, various online transaction authentication mechanisms operated by a TTP are used. Once the buyer does the purchase and the payment, the details of the transaction are given to the TTP for the process of authentication and backup. When the process of transaction and authentication is completed, to validate the purchase, an email is sent to the buyer. Thus, as a trusted third party, the TTP can verify the transaction and can process any customer disputes. In the seller-centric model [9], the seller is treated as the central party, the buyer acts as the inferior role, whereas, the TTP performs the supporting role, contains the following risks. (a) Risk of seller fraud: the seller acts as the prime party and forwards the transactions to the third party platform, which is in control of the contents. There occurs a risk if the transaction detail forwarded by the seller is fraudulent. (b) Performance bottlenecks and risk of interrupted operation: while using online TTP, each transaction is sent to the TTP, which creates a heavy burden to the third party platforms and thus, leads to overload, creating performance bottleneck [9].

The available services are in increasing mode on the internet and communication devices along with technological growth. With the development of Internet and smartphones, a new class of services has developed with the presence of location sensors called LBS that combines both the cyber and physical worlds, which seems to be interesting for users. One or more location-dependent services are allotted to every user by the LBS system, which is connected to the LBS provider that sends the information to the server. An example application, which is used to find the nearby places, such as restaurants and gas stations, or to find the locations of nearby friends using location-based friend finders, such as Foursquare. Even though these services are very attractive, they require accessing physical information about the real-world user's life [10]. Users' privacy may be affected if the system is not provided with adequate security mechanisms. The user's behavior, habits, social activities, sickness, and other information can be known by an intruder, by just knowing the users' location [11]. Thus, the users' security and privacy acts as one of the most important issues in LBS. Hence, the privacy of location data should be deeply investigated as most of the researchers indicate the use of hiding the users' location even from the service providers [12]. The privacy of the data can be protected by the encryption algorithms [13]. As the processing power of computers and development of storage devices are improved greatly, the users are easily identified by tracking their locations and movements that they go through, and thus, most LBS are not satisfied with this issue as detecting such trajectory data is possible [14]. For example, users are subjected to location advertisements or prejudice by service providers or to physical harm and extortion [11]. Hence, several researchers have described various methods such as spatial and temporal cloaking [9, 15], fake locations [16], the addition of noise [17], k-anonymity [9], and several other similar methods to deal with this threat [18].

The main aim of this paper is to develop and design an approach based on authentication and authorization in a P2P network using encryption-based multi-level authentication. Authentication is done in terms of security factors, like one-time password, session password, location profile, spatial information, a hashing function, and so on. Initially, the user and the server are registered for the process of authentication in the proposed approach. Then, using AES, and hashing functions, the multi-level authorization, and authentication is performed, undergoing various levels of verification to provide security against different kinds of attacks in P2P networks. Fuzzy-based authentication is used for the security of communication in the proposed system. Hence, the proposed fuzzy-enabled AES-based multi-level authorization and authentication scheme is developed to provide a novel mathematical model to improve the security in the P2P network.

1.1 The major contribution of the paper:

A location-based authentication and authorization scheme in P2P networking: The Location-based authorization and authentication is proposed to assure secure communication in the P2P networks, for which the location of the user is identified using the location detector present in the server side.

The organization of the paper: Sect. 1 explains the introduction to the need for security in the P2P networks. Section 2 discusses the literature review. Section 3 deals with the proposed system of Location-based privacy in P2P networks. Results and discussion are explained in Sects. 4 and 5 deals with the conclusion of the paper.

2 Related work

In this section, the literature survey of various methods used for the security in P2P networks and the challenges of the existing methods are discussed.

Rahman et al. [19] employed a pairing-based cryptographic model for privacy-preserving secure data exchange protocol, which successfully controlled different attacks, namely man-in-the-middle attack, masquerade attack, message manipulation attack, and the more sophisticated target oriented attack, but was a time-consuming method. Yang et al. [20] designed an authentication system with AA server, which provided increased security and discriminated user access, but the quality of service was not considered in this method. Chae and Cho [21] used the Enhanced secure device authentication algorithm. This method used very less time, but with reduced efficiency. Touceda et al. [22] employed a method of authorization in structured P2P networks based on ACs, which provided improved efficiency, but suffered from overhead problems. Li et al. [23] implemented a method called ATRA model, which provided various advantages, such as improved success rate, less time, efficient resource sharing, and less average cost, but a prototype system was absent in this method. Chae et al. [7] designed a privacy data leakage prevention method, used to prevent the leakage of privacy data of P2P sharing file, but failed to provide leakage protection in all the outgoing files. Ghaffari et al. [18] designed a method of distributed anonymizing protocol based on a peer-to-peer architecture that had low time and computation cost, but over-speeding detection cannot be done using this method. Yeh et al. [24] used three batch authentication protocols, which provided security against impersonator attacks and passive adversaries, but the computational cost was very high. Pecori and Veltri [6] used Triple-Authenticated Key Exchange Protocol method which does not need trusted third parties, pre-shared secrets or Public Key Infrastructure, but there was a possibility for malicious attacks. Cheng et al. [25] developed an efficient symmetric key based authentication scheme for P2P live streaming system with network coding, to provide in-network detection against pollution attacks and entropy attacks concurrently. Initially, they developed a homomorphic message authentication code (MAC), named as PMAC, which has low computation overhead and small key size. After that, the PMAC and the delayed key disclosure approach were used to make sure that the peers could not only detect the corrupted blocks, but also upload blocks in accordance with random linear network coding.

2.1 Challenges

By analyzing the existing methods, we have noticed that the following challenges present in the existing algorithms:

- There is no special procedure [26] for most of the current security protocols of P2P-based OSNs. In this system, each of the users is authenticated by OOB method, which may impose the increased speed of social networks [24].
- Most of the existing protocols only support one-to-one authentication [24]. These protocols do not assume the control measures of underlying devices, including computing power and memory limitations [24].
- A well-known identity protection mechanism, k-anonymity is used to determine the trade-off among time, privacy, and quality of service [18].
- A large number of trust and access control models are given to achieve secure communication through the wired networks, but these methods provide less efficiency due to the complexities involved by the amount of trust data and the requirement of more time than expected [23].

The proposed method is designed to solve these challenges of the existing methods. To provide the secured communication between users, this paper implements the location-based authorization and authentication scheme in P2P networks, which overcome the issues in the OOB method. The encryption-based multi-level authentication utilized in this work provides security against different kinds of attacks in P2P networks. In Location-based authorization and authentication, the location of the user is identified using the location detector present in the server side. Also, the authentication process is done with the factors of security, such as a session password, one-time password, spatial information, location profile, a hashing function, and so on. Hence, the proposed method offers secure communication among users in P2P networks.

3 Proposed method

The absence of centralized authority in the P2P network leads to insecurity due to the presence of various attacks, and so the security issues must be noted carefully. The design of OSNs in the next generation uses P2P technology in which the users communicate with each other through the internet service. Various methods are used to provide communication, but the security of information between users is a challenge. Thus, to provide secure communication between users, the proposed method implements the location-based authorization and authentication scheme in P2P networks. In this technique, initially, the user is registered in the server using the username and password. The server determines the location of the user using the location detector and additionally, produces a key that is forwarded to the user and thus, the registration process terminates. The registration process is followed by the authentication process, in which two sets of intermediate messages are generated between the user and the server to provide two levels of verification. Once the two-levels of verification are completed, the process of authentication terminates and is followed by authorization. Then, the process of authorization occurs, in which the first user develops a message that is transferred to the second user. The second user accepts the message from the first user and develops another message that includes the details of both the users. Hence, the message is sent to the server, which compares the received message from the users with the messages calculated in the server corresponding to each user. If both the messages are same, then, two-level verification is completed and hence, both the users start communicating with each other. The block diagram of the proposed method is given in Fig. 1.

User registration is carried out by sending the information of the user to the server side. Initially, the user information, such as username and password of the user is given to the server. The server stores the username and the password as stored username and password. At the server side, the information obtained from the user is processed to find the location of the user and generates a key in the server side. The server sends the generated location and the generated key to the user, which is saved in the form of stored location and stored key. The stored location and the stored key are used in the authentication and authorization section of the proposed method of location-based privacy.

The user authentication process is performed by comparing the intermediate messages produced in the user side and the server side. If both the intermediate messages produce the same message, then the verification level is completed. For the first level of verification, an intermediate message is created in the user side using the username, password, stored location, and the stored key. The created intermediate message is sent to the server. The server creates another intermediate message using the stored username, stored password, generated key and the generated location. Thus, the intermediate messages at both the user side and the server side are compared with each other. If both the messages are equal, the first level of verification is completed.

For the second level of verification, the fuzzy function is applied to the intermediate message produced for the first level verification at the server to obtain the transform profile. The transform profile, in addition to the generated key and the session password, creates another intermediate message in the server side. Similarly, the fuzzy function is applied to the intermediate message of the user side for the first level verification to obtain the transform profile. Similar to the previous step, the transform profile, together with the stored key and received password, another intermediate message is generated in the user side for second level verification.

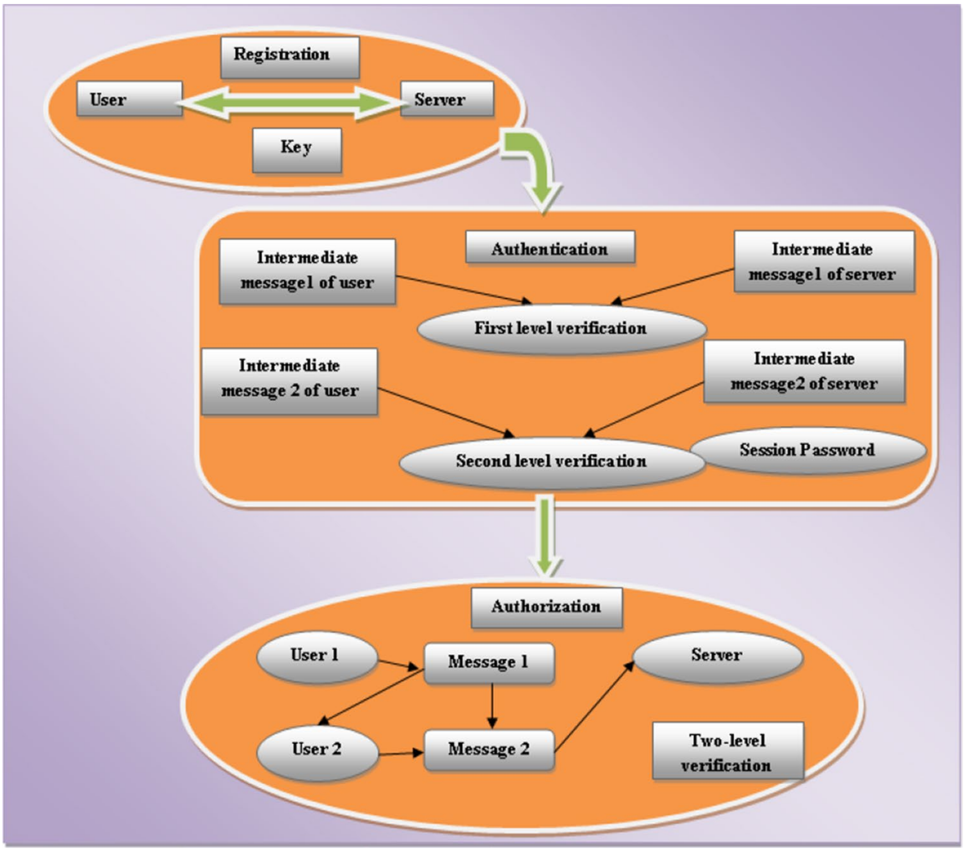


Fig. 1 Block diagram of the proposed authentication and authorization scheme

Thus, both the intermediate messages at the user side and the server side are compared. If both the messages are the same, the second level verification is completed. Once the authentication process is completed, the authorization process is preceded.

The process of authorization is done between two users and the server. Initially, the user 1 creates an intermediate message using the user name, hashing function of the stored key, hashing function of stored location, and a request. The generated intermediate message is given to the user 2. User 2 receives the message from user 1 and in addition to its own information, such as user name, hashing function of the stored key, and the hashing function of stored location, it creates another intermediate message in the user side. The intermediate message created by user 2 is sent to the server side, where two levels of verification are carried out. The first level of verification is performed for user 1, and the second level of verification is carried out for user 2.

For the first level of verification, two intermediate messages are created for user 1, one by concatenating the hashing function of calculated location with the hashing function of generated key and the other by concatenating the hashing function of received location with the hashing function of received key. Thus, both the intermediate messages are compared with each other. If both the intermediate messages are the same, the first level of verification is completed. For the second level of verification, again two intermediate messages are created for user 2, one by concatenating the hashing function of calculated location with the hashing function of the generated key, and the other by concatenating the hashing function of received location with the hashing function of the received key. Thus, on comparing, if both the intermediate messages of user 2 are the same, the second level of verification is completed.

The final step in the authorization process involves the creation of a shared authorization key for message transfer between the users. The server initially develops an intermediate message by EX-OR-ing the shared authorization key for message transfer with the transform profile of user 1. Then, this intermediate message is given to user 1, who concatenates it with the calculated transform profile of user 1 to produce the shared authorization key for message transfer to user 1. Similarly, the server creates an intermediate message by EX-OR-ing the shared authorization key for message transfer with the transform profile of user 2. This intermediate message is given to user 2, and is concatenated with the calculated transform profile of user 2 to produce the shared authorization key for message transfer to user 2. When both the shared authorization keys for message transfer in user 1 and user 2 are same, both the users start to communicate with each other. Hence, the process of authorization is completed.

3.1 User registration

The user name and the password of the user are given to the server, who saves the name and the password of the user and determines the location of the user. The determined location of the user is given in Eq. (1) as,

$$L_i^c = LD\left(I_i\right) \tag{1}$$

where L_i^c is the computed location of the ith user and $LD(.)$ is the location detector function.

The location of the ith user is used to generate a key that is used for the authentication and the authorization and is sent back to the user. The generated key is given in Eq. (2) as,

$$K_{u_i} = h\left(I_i^s \| P_i^s\right) \oplus h\left(L_i^c\right) \tag{2}$$

where I_i^s is the stored ID of the ith user, P_i^s is the stored password of the ith user, and $h(.)$ is the hashing function.

3.2 User authentication

The username is concatenated with the password and then, encrypted depending on the stored key K_{ui}^s, which is EX-ORed with the stored location of the user to produce an intermediate message S_1 by the user, as given in Eq. (3),

$$S_1 = E^{K_{u_i}^s}\left(I_i \| P_i\right) \oplus L_i^s \tag{3}$$

where $E^{k_{ui}^s}(.)$ is the AES encryption by $K_{u_i}^s$, I_i is the username of the ith user and P_i is the password of the ith user. The reasons for using AES in this work are that it is more secure than its predecessors, such as DES and 3DES and utilizes longer key lengths. Also, it enables faster encryption than DES and 3DES, and perfect for software applications, hardware, and firmware, which require high throughput and low latency. According to the NIST statement, AES is "capable of protecting sensitive government information well into the next century". Also, it is easy to implement in hardware and software and offers good protection against various attacks.

The intermediate message S_1 is sent to the server side. In the server side, the stored username is concatenated with the stored password and encrypted based on the generated key K_{ui}, which is EX-ORed with the generated location of the user and is given in Eq. (4) as,

$$S_1^c = E^{K_{u_i}}\left(I_1^s \| P_1^s\right) \oplus L_i^c \tag{4}$$

where $E^{K_{u_i}}(.)$ is the AES encryption by K_{ui}. The intermediate messages generated at both the user side and the server side are compared. If $S_1 = S_1^c$, the first level verification is completed. The transform profile D_s is obtained by applying a fuzzy function on the intermediate key generated in the server side. Fuzzy Logic [27–29] is a mathematical approach to compute the approximate value based on the multi-valued logic. In this research, Fuzzy Logic has been used for generating the intermediate messages. It is a good tool for dealing with uncertainty. Also, it has been used in several reliable security systems for enhancing security.

The fuzzy membership function is calculated using the triangular membership function and is given in Eq. (5) as,

$$D_s = F\left(S_1^c\right) \tag{5}$$

The input data is transferred into fuzzified data using the triangular membership function, given in Eq. (6) that consists of three vertices, x, y, and z of $F\left(S_1^c\right)$ in a fuzzy set B, where x is the lower boundary, y is the centre with membership degree of ‘1′ and z is the upper boundary with membership degree of ‘zero’.

$$F\left(S_1^c\right) = \begin{cases} 0 & if\ S_1^c \le x \\ \frac{S_1^c - x}{y - x} & if\ x \le S_1^c \le y \\ \frac{z - S_1^c}{z - y} & if\ y \le S_1^c \le z \\ 0 & if\ S_1^c \ge z \end{cases} \tag{6}$$

The server generates an intermediate message S_2 by EX-OR-ing the session password with the hashing function of generated key $h\left(K_{ui}\right)$ and finally, multiplied with the transform profile and is given in Eq. (7) as,

$$S_2 = \left(h\left(K_{u_i}\right) \oplus SP\right) \otimes D_s \tag{7}$$

where SP is the session password.

The intermediate message S_2 and the session password are sent to the user to obtain the calculated intermediate message S_2^c. The relation of S_2^c given in Eq. (8) is obtained by EX-OR-ing the received session password with hashing function of saved key and finally, multiplied with the calculated transform profile D_s^c.

$$S_2^c = \left(h\left(K_{u_i}^s\right) \oplus SP^R\right) \otimes D_s^c \tag{8}$$

The calculated transform profile D_s^c is obtained using Eq. (9) as,

$$D_s^c = F\left(S_1\right) \tag{9}$$

The intermediate message S_2 of the server is compared with the calculated intermediate message S_2^c at the user side. As,$S_2 = S_2^c$, the second level verification is completed. Thus, the user is authenticated with the server.

3.3 Authorization

The authorization process involves two users u_i and u_j and a server. Initially, the user u_i generates the intermediate message M_1, as given in Eq. (10), which is given to the user u_j.

$$M_1 = \left\{I_i, h\left(K_{u_i}^s\right), h\left(L_i^s\right), REQ\right\} \tag{10}$$

where I_i is the ID of the ith user, $h\left(K_{u_i}^s\right)$ is the hash function of the stored key of ith user, L_i^s is the stored location of the ith user and REQ is the request message.

The user u_j sends the intermediate message M_1 along with the intermediate message M_2 to the server as in Eq. (11).

$$M_2 = \left\{I_i, h\left(K_{u_i}^s\right), h\left(L_i^s\right), I_j, h\left(K_{u_j}^s\right), h\left(L_j^s\right) REQ\right\} \tag{11}$$

where I_j is the ID of the jth user, $h\left(K_{u_i}^s\right)$ is the hash function of the stored key of jth user, and L_j^s is the stored location of the jth user.

The server calculates an intermediate message R_i^c corresponding to the ith user by concatenating the hashing functions of the calculated location of the user L_i^c and the hashing function of the generated key K_{u_i} and is given in Eq. (12) as,

$$R_i^c = h\left(L_i^c\right) \| h\left(K_{u_i}\right) \tag{12}$$

An intermediate message R_i^R is generated using the information obtained from the user M_2 and is given in Eq. (13) as,

$$R_i^R = h\left(L_i^R\right) \| h\left(K_{u_i}^R\right) \tag{13}$$

Then, these two intermediate messages are compared with each other. If $R_i^c = R_i^R$, the first level of authorization is completed.

The server again calculates an intermediate message R_j^c corresponding to the jth user by concatenating the hashing functions of the calculated location of the user L_j^c and the hashing function of the generated key K_{u_j}, and is given in Eq. (14) as,

$$R_j^c = h\left(L_j^c\right) \| h\left(K_{u_j}\right) \tag{14}$$

In the server, R_j^R is an intermediate message generated using the information obtained from the user M_2 and is given in Eq. (15) as,

$$R_j^R = h\left(L_i^R\right) \| h\left(K_{u_j}^R\right) \tag{15}$$

These two intermediate messages are compared with each other, and if $R_j^c = R_j^R$, the second level of authorization is completed.

In the authorization section, the shared authorization key for message transfer, K^{AK} is determined. The shared authorization key is obtained by EX-OR-ing the encryption of the concatenated location of both ith user and jth user with the hashing function of the calculated key of both ith user and jth user and is given in Eq. (16) as,

$$K^{AK} = E^{KS}\left(L_i^c \| L_j^c\right) \oplus h\left(K_{u_i} \oplus K_{u_j}\right) \tag{16}$$

The value of K^{AK} is used to create an intermediate message Z_1 by EX-OR-ing with the transform profile D_s^i of the ith user and is given in Eq. (17) as,

$$Z_1 = K^{AK} \oplus D_s^i \tag{17}$$

This message is sent to the ith user in order to calculate the shared authorization key for message transfer in ith user and is given in Eq. (18) as,

$$K_c^{AK} = Z_1 \oplus D_{s_i}^c \tag{18}$$

Similarly, the intermediate message Z_2 is obtained by EX-OR-ing K^{AK} with the transform profile D_s^j of the jth user and is given in Eq. (19) as,

$$Z_2 = K^{AK} \oplus D_s^j \tag{19}$$

This intermediate message is sent to the jth user to calculate the shared authorization key for message transfer in jth user and is given in Eq. (20) as,

$$K_c^{AK} = Z_2 \oplus D_{s_j}^c \tag{20}$$

Thus, both the computed values of shared authorization key for message transfer in Eqs. (18) and (20) are compared. If both the values are equal, ith user and jth user start to communicate with each other.

4 Results and discussions

The results and discussion of the proposed Location-based privacy method are discussed in this section. The results of the proposed method in terms of hit ratio and success rate are discussed in this section.

4.1 Experimental setup

The proposed classifier is implemented in JAVA using the PC installed in Windows 10 OS and Intel(R) i3 processor with the 4 GB RAM and 64-bit operating system.

4.2 Comparative methods

The competing methods used for the analysis are 3AKEP [6], Privacy DLP method [7], and Proxy and certificate-based protocol [24] for proving the superiority of the proposed Location-based privacy method.

4.3 Performance metrics

The evaluation metrics, namely hit ratio and success rate, are considered for the analysis of the proposed method and are given using the terms below,

(a) Hit ratio

The term hit ratio is defined as the ratio of correctly identified attackers among the total attackers and is given in Eq. (21) as,

$$\textit{Hit ratio} = \frac{\textit{correctly identified attackers}}{\textit{total attackers}} \tag{21}$$

(b) Success rate

The success rate is defined as the ratio of the sum of correctly identified attackers and the normal users to the total users and is given in Eq. (22) as,

$$\textit{Success rate} = \frac{\textit{correctly identified attackers} + \textit{correctly identified normal users}}{\textit{Total users}} \tag{22}$$

4.4 Comparative analysis

The analysis of the methods based on the hit ratio and the success rate is performed through varying the number of malicious attackers. Figure 2a shows the hit ratio analysis in the presence of Password Guessing Attack among 75 users depending on the number of malicious attackers. When the number of malicious attackers is 20, the hit ratio for the methods, such as 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.2, 0.25, 0.35, and 0.65, respectively. Thus, the proposed method provides a high hit ratio as compared to the existing conventional methods.

Figure 2b depicts the analysis based on the success rate in the presence of Password Guessing Attack among 75

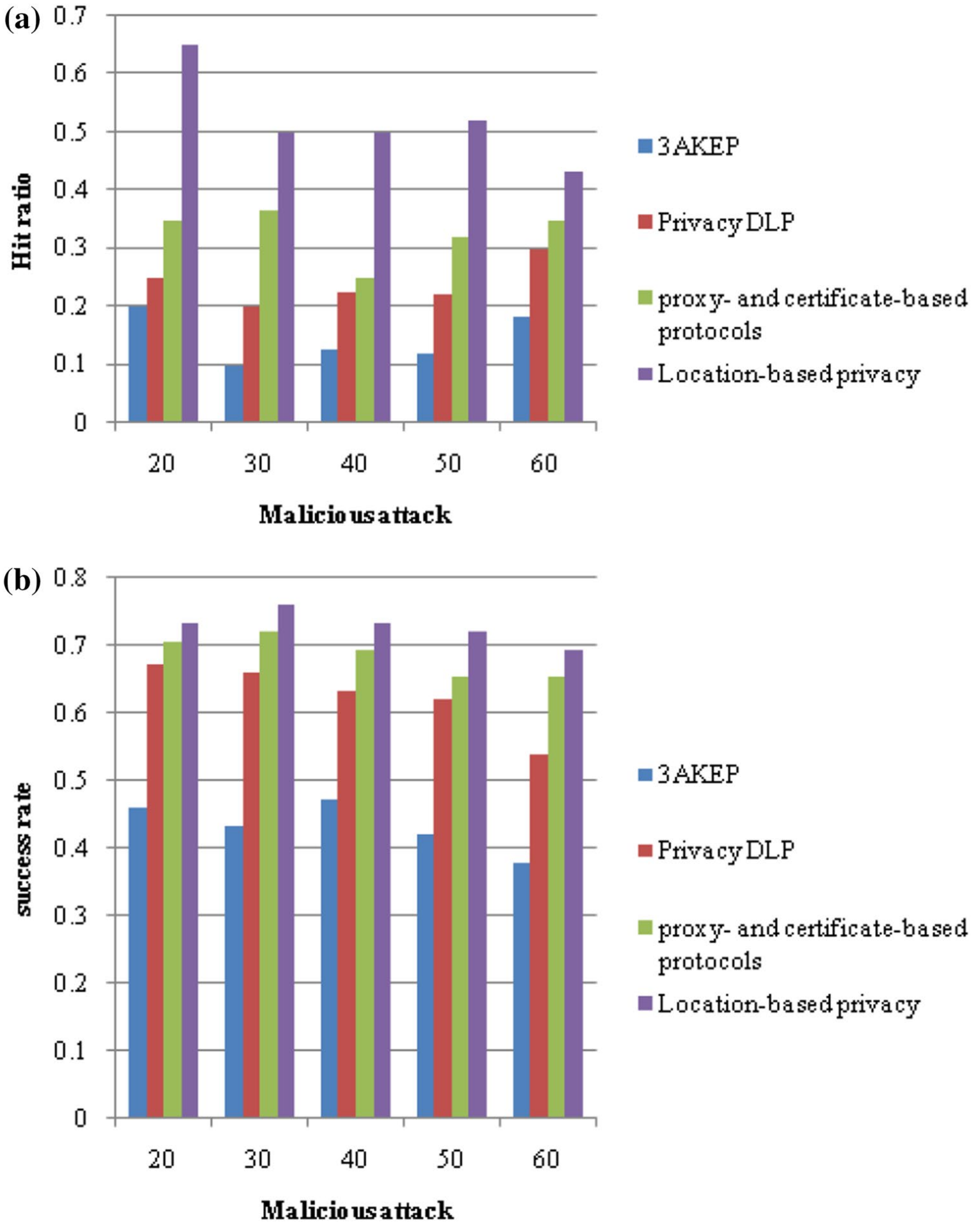


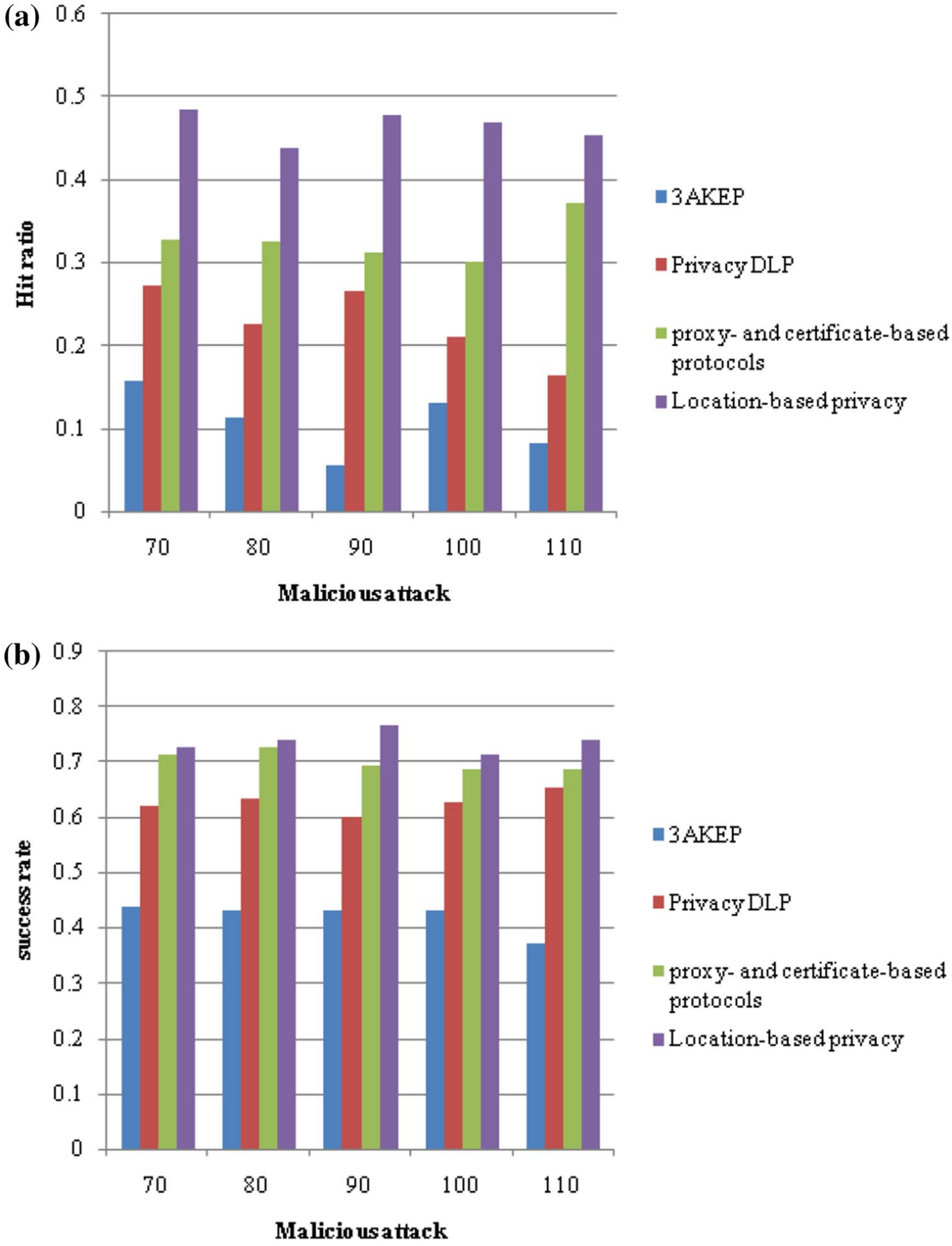
Fig. 2 Analysis in the presence of password guessing attack for 75 users, **a** Hit ratio, **b** success rate

users based on the number of malicious attackers. When the number of malicious attackers is 20, the success rate for the methods, namely 3AKEP, Privacy DLP, Proxy and certificate-based protocol and Location-based privacy is 0.46, 0.6733, 0.7066, and 0.7333, respectively.

Figure 3 shows the analysis based on Hit ratio and Success rate in the presence of Password Guessing Attack for 150 users. Similarly, Fig. 3a shows the hit ratio in the presence of Password Guessing Attack among 150 users depending on the number of malicious attackers. When the number of malicious attackers is 100, the hit ratio for 3AKEP, Privacy DLP, Proxy and certificate-based protocol and Location-based privacy is 0.13, 0.21, 0.3, and 0.47, respectively. In the same way, Fig. 3b depicts the success rate in the presence of Password Guessing Attack among 150 users depending on the number of malicious attackers. When the number of malicious attackers is 100, the success rate for 3AKEP, Privacy DLP, Proxy and certificate-based protocol and the Location-based privacy is 0.4333, 0.6266, 0.6866, and 0.7133, respectively. Thus, the proposed method provides a high success rate as compared to the other conventional methods.

Figure 4 presents the analysis on Hit ratio and Success rate in the presence of a Brute Force Attack for 75 users. Figure 4a shows the hit ratio in the presence of Brute Force Attack among 75 users depending on the number of malicious attackers. When the number of malicious attackers is 50, the hit ratio for the methods, such as 3AKEP method, Privacy DLP method, Proxy and certificate-based protocol

Fig. 3 Analysis in the presence of password guessing attack for 150 users, **a** Hit ratio, **b** success rate



method and the Location-based privacy method is 0.5, 0.56, 0.72, and 0.76, respectively. Thus, the proposed method provides a high hit ratio as compared to the existing conventional methods.

Similarly, Fig. 4b depicts the success rate in the presence of Brute Force Attack among 75 users depending on the number of malicious attackers. When the number of malicious attackers is 50, the success rate for the methods, namely 3AKEP method, Privacy DLP method, Proxy and certificate-based protocol method and the Location-based privacy method is 0.1533, 0.3933, 0.4666, and 0.4933, respectively. Thus, the proposed method provides a high success rate as compared to the other conventional methods.

Figure 5 depicts the analysis based on Hit ratio and Success rate in the presence of a Brute Force Attack for 150 users. Figure 5a shows the hit ratio in the presence of Brute Force Attack among 150 users depending on the number of malicious attackers. When the number of malicious attackers is 100, the hit ratio for 3AKEP, Privacy DLP, Proxy and certificate-based protocol and the Location-based privacy is 0.53, 0.64, 0.76, and 0.83, respectively. Thus, the proposed method provides a high hit ratio as compared to the existing conventional methods.

Similarly, Fig. 5b depicts the success rate in the presence of Brute Force Attack among 150 users depending on the number of malicious attackers. When the number of

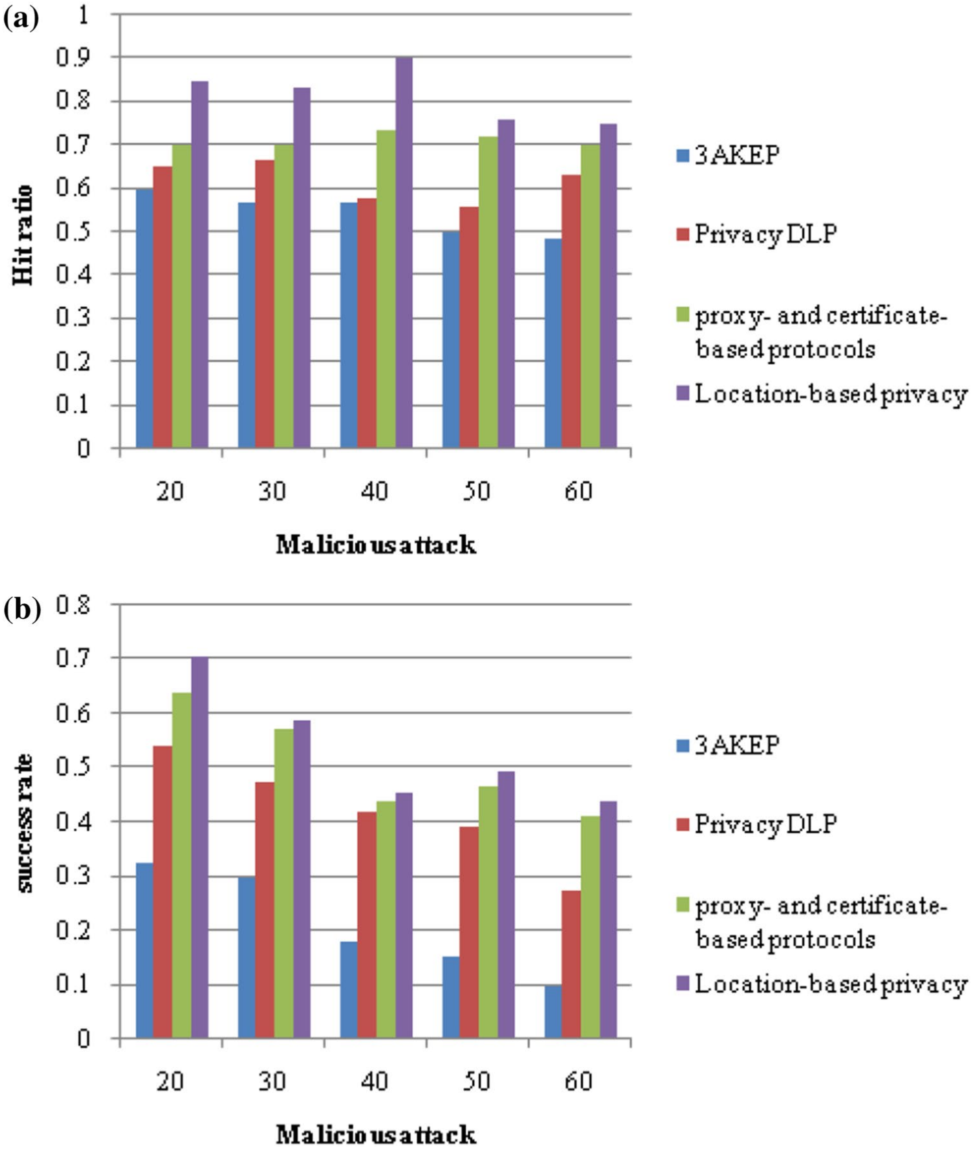


Fig. 4 Analysis in the presence of brute force attack for 75 users, **a** Hit ratio, **b** success rate

malicious attackers is 90, the success rate for the methods, namely 3AKEP, Privacy DLP, Proxy and certificate-based protocol and Location-based privacy is 0.2, 0.38, 0.46, and 0.5266, respectively.

Figure 6 depicts the analysis based on Hit ratio and Success rate in the presence of Dictionary Attack for 75 users. Figure 6a shows the hit ratio in the presence of Dictionary Attack among 75 users depending on the number of malicious attackers. When the number of malicious attackers is 20, the hit ratio for the methods, such as 3AKEP, Privacy DLP, Proxy and certificate-based protocol and Location-based privacy is 0.5, 0.55, 0.7, and 0.85, respectively. Thus, the proposed method provides a high hit ratio as compared to the existing conventional methods.

Similarly, Fig. 6b depicts the success rate in the presence of Dictionary Attack among 75 users depending on the number of malicious attackers. When the number of malicious attackers is 40, the success rate for 3AKEP, Privacy DLP, Proxy and certificate-based protocol and the Location-based privacy is 0.18, 0.38, 0.48, and 0.5466, respectively. Thus, the proposed method provides a high success rate as compared to the other conventional methods.

Figure 7 depicts the analysis based on Hit ratio and Success rate in the presence of Dictionary Attack for 150 users. Figure 7a shows the hit ratio analysis in the presence of Dictionary Attack among 150 users depending on the number of malicious attackers. When the number of malicious attackers is 100, the hit ratio for the methods, 3AKEP, Privacy DLP, Proxy and certificate-based protocol and Location-based privacy is 0.61, 0.61, 0.7, and 0.81, respectively. Thus, the proposed method provides a high hit ratio as compared to the existing conventional methods.

Similarly, Fig. 7b depicts the success rate in the presence of Dictionary Attack among 150 users depending on the

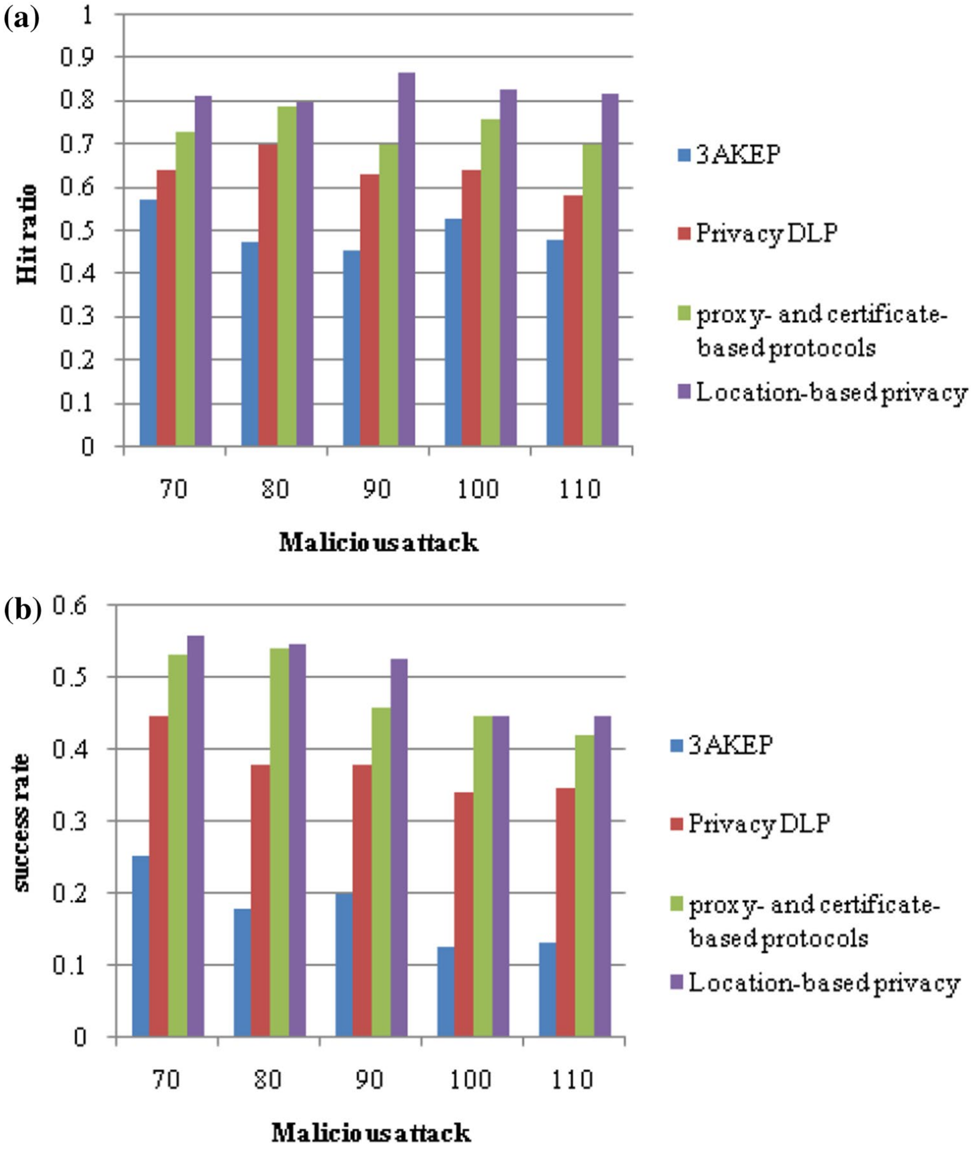


Fig. 5 Analysis in the presence of brute force attack for 150 users, **a** Hit ratio, **b** success rate

number of malicious attackers. When the number of malicious attackers is 100, the success rate for 3AKEP method, Privacy DLP method, Proxy and certificate-based protocol method and the Location-based privacy method is 0.1666, 0.36, 0.3933, and 0.46, respectively. Thus, the proposed method provides a high success rate as compared to other conventional methods.

4.5 Comparative discussion

Table 1 shows the comparative discussion of the proposed method with the existing conventional methods on varying the number of malicious attacks, in the presence of Password Guessing Attack. In the case of 75 users, the hit ratio for 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.2, 0.3, 0.3666, and 0.65, respectively. The success rate of 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.7333, 0.6733, 0.72, and 0.76, respectively. For 150 users, the hit ratio for 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy methods is 0.1571, 0.2714, 0.3727, and 0.4857, respectively. The success rate of 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.44, 0.6533, 0.7266, and 0.7666, respectively.

Table 2 shows the comparative discussion of the proposed method with the existing conventional methods on varying the number of malicious attacks, in the presence of Brute Force Attack. For 75 users, the hit ratio for 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.6, 0.6666, 0.7333, and 0.9, respectively. The success rate of 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.3266, 0.54, 0.64, and 0.7066, respectively. In the presence of 150

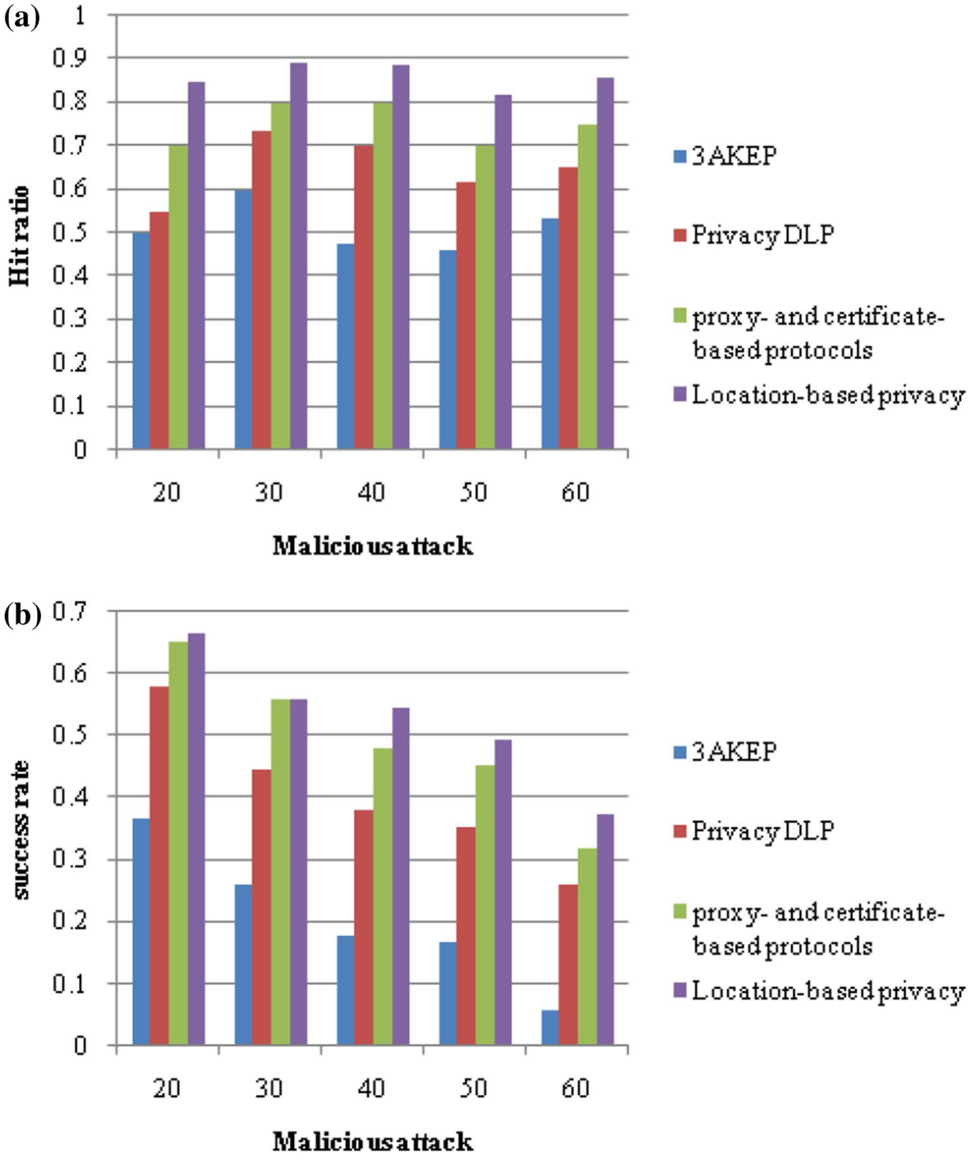


Fig. 6 Analysis in the presence of dictionary attack for 75 users, **a** Hit ratio, **b** success rate

users, the hit ratio for 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.5714, 0.7, 0.7875, and 0.8666, respectively. The success rate of 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.2533, 0.4466, 0.54, and 0.5466, respectively.

Table 3 shows the comparative discussion of the proposed method with the existing conventional methods on varying the number of malicious attacks, in the presence of Dictionary Attack. While 75 users are considered, the hit ratio of 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and the Location-based privacy is 0.5333, 0.7333, 0.8, and 0.89, respectively. The success rate of 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and the Location-based privacy methods is 0.3666, 0.58, 0.6533, and 0.6666, respectively. In the presence of 150 users, the hit ratio for 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and Location-based privacy is 0.5777, 0.6625, 0.7857, and 0.8285, respectively. The success rate of 3AKEP, Privacy DLP, Proxy and certificate-based protocol, and the Location-based privacy is 0.2333, 0.4466, 0.5666, and 0.5733, respectively.

Thus, in all the three cases, the hit ratio and the success rate for the proposed location based privacy method is higher as compared to other methods and provides enhanced security in the network.

5 Conclusion

In this paper, the proposed Location based privacy protocol is used to develop an authentication and authorization approach with the use of encryption-based multi-level

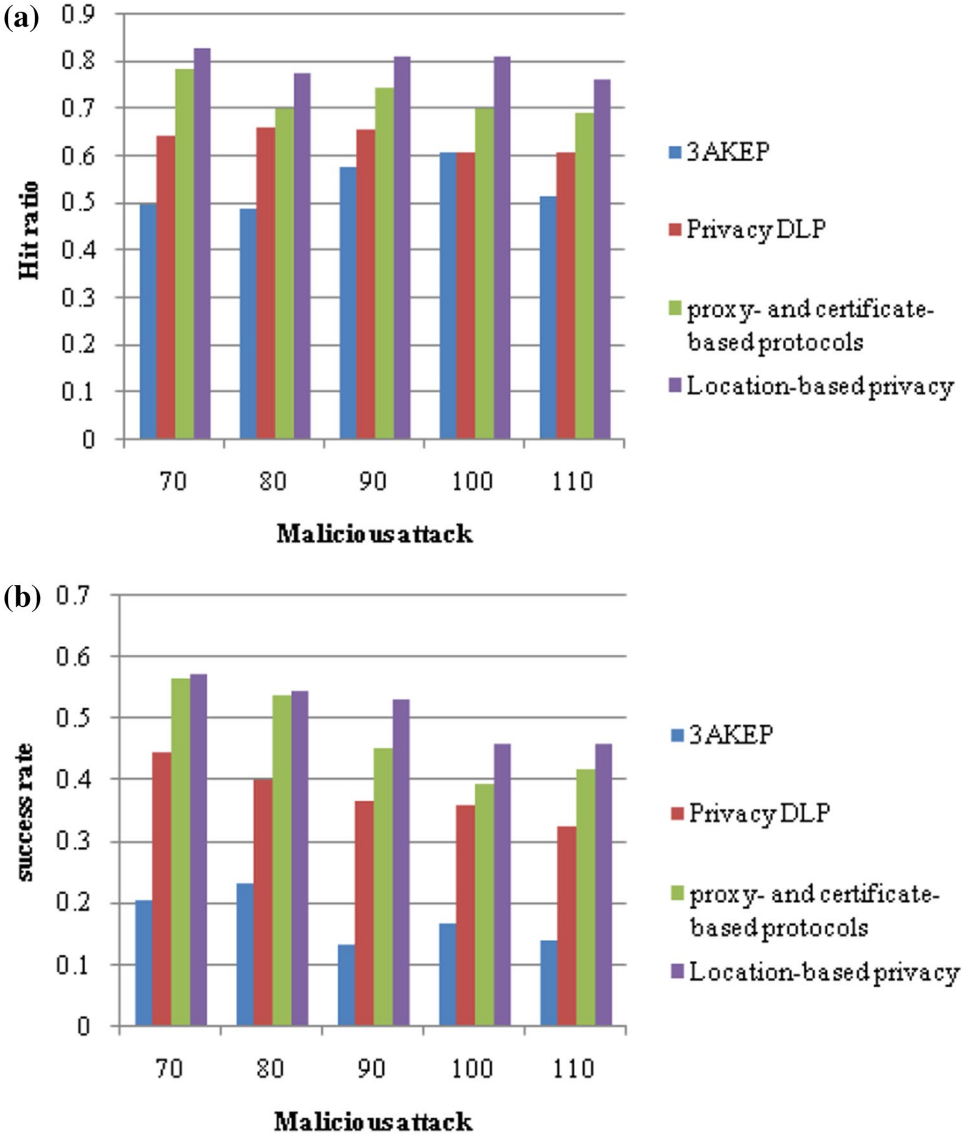


Fig. 7 Analysis in the presence of dictionary attack for 150 users, **a** Hit ratio, **b** success rate

Table 1 Comparative discussion based on password guessing attack

Password guessing attack				
	For 75 users		For 150 users	
Methods	Hit ratio	Success rate	Hit ratio	Success rate
3AKEP	0.2	0.7333	0.1571	0.44
Privacy DLP	0.3	0.6733	0.2714	0.6533
Proxy and certificate based protocol	0.3666	0.72	0.3727	0.7266
Location based privacy	0.65	0.76	0.4857	0.7666

Table 2 Comparative discussion based on brute force attack

Brute force attack				
	For 75 users		For 150 users	
Methods	Hit ratio	Success rate	Hit ratio	Success rate
3AKEP	0.6	0.3266	0.5714	0.2533
Privacy DLP	0.6666	0.54	0.7	0.4466
Proxy and certificate based protocol	0.7333	0.64	0.7875	0.54
Location based privacy	0.9	0.7066	0.8666	0.5466

authentication. The authentication process is done with the security factors, such as session password, one-time password, spatial information, location profile, a hashing function, and so on. In the first step of the authentication process, the user and the server are registered, and then, AES and hashing functions are used to perform multi-level

Table 3 Comparative discussion based on dictionary attack

Dictionary attack				
	For 75 users		For 150 users	
Methods	Hit ratio	Success rate	Hit ratio	Success rate
3AKEP	0.5333	0.3666	0.5777	0.2333
Privacy DLP	0.7333	0.58	0.6625	0.4466
Proxy and certificate based protocol	0.8	0.6533	0.7857	0.5666
Location based privacy	0.89	0.6666	0.8285	0.5733

authorization and authentication processes. The security of communication is done based on the fuzzy-based authentication in the proposed system. Thus, the proposed system ensures security in the P2P network. The result obtained shows that the proposed Location-based privacy protocol provides better Hit ratio and Success rate values as compared to existing conventional methods. The proposed system obtained the hit ratio of 0.9, and the success rate of 0.7666, proving that the proposed system provides better security in the P2P network. In future, the access control mechanism for P2P networking will be developed.

References

1. García-Dorado JL, Finamore A, Mellia M, Meo M, Munafò M (2012) Characterization of ISP traffic: trends, user habits, and access technology impact. IEEE Trans Netw Serv Manag 9(2):142–155
2. Passarella A (2012) A survey on content-centric technologies for the current Internet: CDN and P2P solutions. Comput Commun 35(1):1–32
3. Bittorrent (2001) [Online]. https://www.bittorrent.com
4. Internap (1996) [Online]. https://www.internap.com
5. Qureshi A, Megías D, Rifà-Pous H (2015) Framework for preserving security and privacy in peer-to-peer content distribution systems. Expert Syst Appl 42(3):1391–1408
6. Pecori R, Veltri L (2016) 3AKEP: Triple-authenticated key exchange protocol for peer-to-peer VoIP applications. Comput Commun 85:28–40
7. Chae CJ, Shin YJ, Choi K, Kim KB, Choi KN (2016) A privacy data leakage prevention method in P2P networks. Peer-to-Peer Netw Appl 9(3):508–519
8. Forné J et al (2010) Pervasive authentication and authorization infrastructures for mobile users. Comput Secur 29(4):501–514
9. Gruteser M, Grunwald D (2003) Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on mobile systems, applications and services—MobiSys'03, pp 31–42
10. Almuhimedi H et al. (2015) Your location has been shared 5398 times! a field study on mobile app privacy nudging. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems—CHI'15, pp 787–796
11. Gutwirth S (2002) Privacy and the information age. Rowman & Littlefield Publishers, Lanham
12. Hengartner U (2007) Hiding location information from location-based services. In: Proceedings of the international conference on mobile data management, pp 268–272
13. Mukhedkar M, Powar P, Gaikwad P (2015) Secure non real time image encryption algorithm development using cryptography & steganography. In: Proceedings of annual IEEE India conference (INDICON), pp 1–6
14. Lin M, Hsu WJ (2014) Mining GPS data for mobility patterns: a survey. Pervasive Mob Comput 12:1–16
15. Ying B, Makrakis D (2015) Protecting location privacy in vehicular networks against location-based attacks. Int J Parallel Emerg Distrib Syst 30(2):101–117
16. You TH, Peng WC, Lee WC (2007) Protecting moving trajectories with dummies. In: Proceedings of the IEEE international conference on mobile data management, pp 278–282
17. Hoh B, Gruteser M (2006) Protecting location privacy through path confusion. In: Proceedings of the first international conference on security and privacy for emerging areas in communications networks, pp 194–205
18. Ghaffari M, Ghadiri N, Manshaei MH, Lahijani MS (2017) P4QS: a peer-to-peer privacy preserving query service for location-based mobile applications. IEEE Trans Veh Technol 66(10):9458–9469
19. Rahman SMM, Masud MM, Hossain MA, Alelaiwi A, Hassan MM, Alamri A (2016) Privacy preserving secure data exchange in mobile P2P cloud healthcare environment. Peer-to-Peer Netw Appl 9(5):894–909
20. Yang HK, Cha HJ, Kim YH (2016) mVoIP for P2P service based authentication system using AA authentication server. Peer-to-Peer Netw Appl 9(3):529–538
21. Chae C, Cho H (2018) Enhanced secure device authentication algorithm in P2P-based smart farm system. Peer-to-Peer Netw Appl 11(3):1230–1239
22. Touceda DS, Cámara JMS, Zeadally S, Soriano M (2015) Attribute-based authorization for structured peer-to-peer (P2P) networks. Comput Stand Interfaces 42:71–83
23. Li Z-Y, Liu L, Chen R-L, Bi J-L (2016) An adaptive secure communication framework for mobile peer-to-peer environments using Bayesian games. Peer-to-Peer Netw Appl 9(6):1005–1019
24. Yeh LY, Huang YL, Joseph AD, Shieh SW, Tsaur WJ (2012) A batch-authenticated and key agreement framework for P2P-based online social networks. IEEE Trans Veh Technol 61(4):1907–1924
25. Cheng C, Jiang T, Zhang Q (2013) TESLA-based homomorphic MAC for authentication in P2P system for live streaming with network coding. IEEE J Sel Areas Commun 31(9):291–298
26. Buchegger S, Schiöberg D, Vu L, Datta A (2009) PeerSoN : P2P social networking—early experiences and insights. In: Proceedings of the second ACM EuroSys workshop on social network systems, pp. 46–52
27. Sharma A, Johari PK (2017) Eliminating collaborative black-hole attack by using fuzzy logic in mobile ad-hoc network. Int J Comput Sci Eng 5(5):34–41
28. Chander S, Vijaya P, Dhyani P (2016) MKF-firefly: hybridization of firefly and multiple kernel-based fuzzy c-means algorithm. Int J Adv Res Comput Commun Eng 5(7):213–216
29. Veeraiah N, Krishna BT (2018) Intrusion detection based on piecewise fuzzy C-means clustering and fuzzy Naïve Bayes rule. Multim Res 1(1):27–32