An Efficient and Secure Profile Matching Scheme for Encounter based Mobile Social Network

Fizza Abbas[†], Ubaidullah Rajput [††], Umair Ali Khan[†††] and Farwa Abbas[††††],
fizza_alvi@quest.edu.pk ubaidullah@quest.edu.pk umair.khan@quest.edu.pk farwa.abbas09@yahoo.com
[†, ††, †††]Department of Computer Systems Engineering, Quaid-e-Awam UEST, Nawabshah Pakistan
[††††]Department of Electronics Engineering, Quaid-e-Awam UEST, Nawabshah Pakistan

Abstract
Mobile Social Network (MSN) is an emerging area in recent years where many users are enjoying the facilities of social network on their mobile devices. Encounter-based MSN is a type of MSN where users share a short encounter, exchange some encounter information, and communicate later with the help of the shared encounter information. Encounter-based MSN inherent most of the security and privacy issues associated with MSN. Profile matching is an important and vastly used application of MSN as well as encounter-based MSN. In profile matching, users need to share and match their private information (such as interests). A high similarity may lead to a friendship. The revelation of this private information to an attacker can pose significant threats to the user's privacy. In encounter-based MSN, a significant issue is the secure and accurate exchange of encounter information that can be later used for verification of the encounter. This paper proposes a secure and privacy preserving profile matching mechanism for encounter-based MSN. We have proposed a secure encounter phase and a profile matching phase. During encounter phase, users share their identity along with their signed public key and encrypted interests. The public key is signed by a registration server. During the profile matching phase, users' encrypted interests are matched, and the encrypted results are sent to respective users. The exchange of this information is in encrypted form and only legitimate user can decrypt it. To show the feasibility of the proposed scheme, the computational cost is calculated. In the end, it is observed that the proposed scheme is taking reasonable time to calculate the interests securely. Moreover, the comparison shows that proposed scheme also provides prevention from Sybil attacks, impersonation while keeping the privacy of the users intact.

Keywords:
MSN, Encounter-based MSN, Privacy, Profile matching.

1. Introduction

Mobile social networks (MSN) have become popular among mobile users. MSN is a heterogeneous network in which mobile clients make social relations by matching their attributes or interests provided by user himself or mobility pattern of users. Facebook, Twitter, QQ, Twoo, and many more use context information technologies to let users exchange data and profile information to make relationships [1].

MSN has many paradigms according to the need of mobile users. These include, Proximity based mobile social network (PMSN), Location based mobile social network, and Encounter based mobile social network [1]. PMSN is a popular application nowadays [2]. In Proximity-based mobile social networking (PMSN), users communicate with each other in physical proximity such as subway stations, cinema, university and many more. These networks enable users to use MSN based application while within proximity of each other. Location-based social networks are social networks that utilizes the features of GPS to search location and broadcast respective location and other information [2]. The users of location based mobile social network are in a specific region and share the information with each other [15]. Users find POIs (point of interests) as well as make social ties based on some location. The users normally use a server (sometimes called as location-based server or LBS) that facilitates users by providing POIs based on the users' location. In encounter based mobile social networks, users share a short encounter [3]. During this short interaction, users share some encounter information that can be later used to identify the earlier encounter. When the users are nearby each other, users' mobile equipment stores the encounter information such as common time and location. This encounter history is used to identify each other later at a server. The users find each other based on the encounter information and then struck social ties with each other. Encounter-based MSN are not only serving as a main component of missed-connection services (such as provided by craigslist) but also useful for secure communication [3]. MSN has many applications for example profile matching, wearable services, health services, location-based services and many more. Profile matchmaking is one of the applications of MSN that enables users to find and socialize with other people who have similar interests or backgrounds [2,4]. For example, two users meet with each other in a restaurant. Both can be potential friend to one another because they share a common interest, that is, the food of a restaurant. During profile matching people share their personal information but also have concern towards their privacy [5]. This is because an attacker in the vicinity may learn the private information of users.

Manuscript received December 5, 2024
Manuscript revised December 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.12.22

In Encounter based social networking people share same location at same time [3, 7]. Therefore, there is high probability that these people might share similar interests. For example, in a hospital people are suffering from same disease or in a musical concert two persons might share interests other than music also. In such environment, users run some profile matching protocol that compares their profiles for potential match [7]. However, attacks are possible such as Sybil attack [8]. A malicious user may run the profile matching protocol again and again with varying interest set (that eventually matches to victim). Proximity may reveal users to each other. Therefore, it is better to anonymously share encounter information initially and perform profile matching later (on a central server). Therefore, encounter-based MSN provide an ideal platform for such applicaton.

This paper proposes a protocol for privacy preserving profile matching in an encounter-based social network. We carefully design a mechanism that enable users to securely share the encounter information and later, this encounter information is used to identify each other on a server that help users compute the similarity of their interests. The remainder of the paper is as follows. Section 2 details the related work. Section 3 presents the proposed scheme followed by section 4 that discusses and analyze the proposed scheme. Section 5 concludes the paper along with the future work.

2. Related Work

In literature many researchers are working on privacy preservation approaches for secure profile matching in MSN. This section highlights these approaches and provides the limitations of exiting work. Profile matching mostly uses two cryptographic technique. One is commutative based encryption and other one is pallier cryptosystem. Agrawal et al.'s protocol [4] uses a commutative encryption function for private intersection problems. Authors suggest the power function, $f_e(x) = x_e \ mod \ p$, as an example of a commutative function. The security of their protocol is based on the Decisional Diffie-Hellman hypothesis (DDH). There are some limitations of Agrawal et al. protocol. Their protocol lacks certified set elements and therefore, an attacker can select inputs according to their choice. Moreover, in their approach, only one user gets the information of resultant matching and can cheat the other user. Xie et al.'s Protocol [5] utilizes the trusted third party to certify the interests of user. They use expensive method that is asymmetric key-based cryptography. The proposed protocol provides the facility of friend finding. Wang et al. further enhance Xie protocol and add a feature of best match [6]. They use the concept of matching a user's attributes with various candidates and find the one with most matches i.e. the best match. They follow the concepts of Xie at al. and therefore, have similar issues with Xie. Mostly they talk about using Bluetooth which limits the protocol to only people who are physically near the user. If a user wants to match attributes with people globally, this protocol does not give this provision. Also, the user uses a fix number of attributes which are signed by an attribute verifier. This limits the possibility for a user to change his attributes set. M. Justin et al. propose an approach called SMILE (Secure MIssed connections through Logged Encounters) that uses mobile devices and an intermediate entity. M. Justin et al. approach focuses on interchanging mechanism of users' data such as location and time, by using key exchange with each other during the broadcast [3]. Each contestant utilizes key hashes to create a meeting point using intermediate server without revealing the encounter location to the intermediate server. There are some limitations of SMILE. There is no authentication mechanism. SMILE is likely to effected by Sybil and Man in the Middle (MitM) attack. Moreover, there is a chance of user collusion. A. Mohain et al. explore the functional and security requirements for encounter-based MSN [7]. They examine SMILE and compare it with a set of idealized security and functional requirements. They propose a system which they claim is better than SMILE. However, they use a certified but plain photograph and still claim that their protocol is privacy preserved. They consider centralized repository as drawback in SMILE but use it in one of their two designs. Eagle et al. proposed Social Serendipity approach that relies on server containing user profile [8]. Again, it has single point of failure. Cox et al. presented Smoke Screen by replacing trusted server with service provider to secure real identities [9]. However, they introduce a broker that knows matching results. Hongjuan Li et al. provide peer-to-peer confidential communications with the location privacy and encounter privacy being strictly preserved [10]. The drawback with this work is that the increase in the number of users decreases flexibility. Recently, Bhattacharjee et al. proposed the approach for post disaster scenario [11]. Nonetheless, their approach has less functionality. Moreover, in [12] authors highlight many aspects of application of MSN in their research work.

After getting familiar with the existing work regarding MSN, we propose a scheme for profile matching in Encounter based MSN application and then analyze the results. Our scheme considers the security and privacy of users' interests. Another feature of our scheme is the use of a profile matching facilitator server that cannot learn users' interests. Therefore, users can freely post their interests on the server.

3. Proposed Scheme

Our proposed scheme allows two users to communicate each other if both have shared an encounter in the past. An encounter in this context means that both users were in near proximity of each other for some duration of time. Moreover, we use Paillier cryptosystem [13,14] for profile matching. This mechanism provides significant facilities to guarantee the security of the designed protocols.

3.1 Methodology

In the existing work mentioned in the related work section, it is evident that current techniques have some limitations. After understanding these limitations, proposed scheme is designed. The Fig. 1 shows the methodology of proposed scheme.

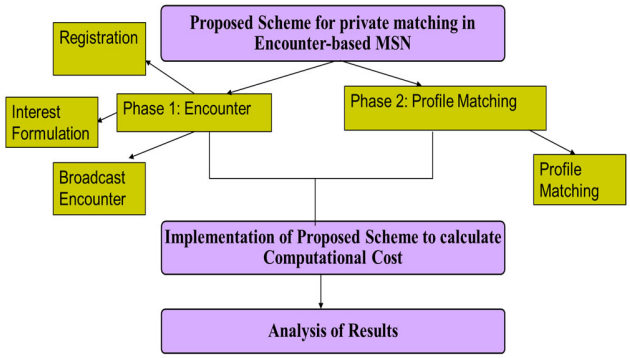

Fig.1 Proposed Methodology

3.2 Proposed Architecture

Fig. 2 shows the generic system architecture of proposed system.

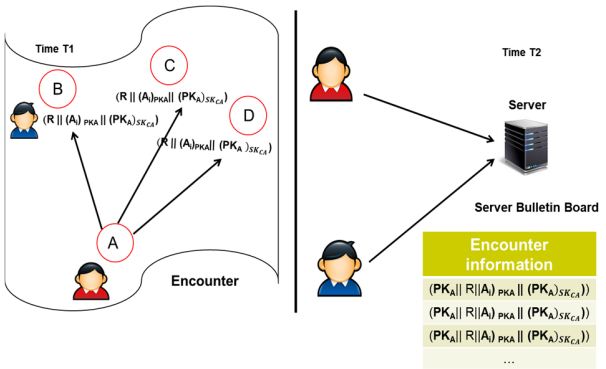

Fig. 2 Generic System Architecture

In our proposed scheme, users A, B, C and D share the encounter information at some time T1. Later, at some time T2, they communicate with each other through a server using the encounter information. A user's mobile device contimoulsy proble near by devices for the execution of the protocol. Whenever two users are in near proximity of each other, there mobile devices exchange the encounter information and save it as well.

3.3 Notations

Table 1 shows the notations and their explanation. The table will help to understand the symbols and cryptographic parameters. The protocol is design by using these notations.

Table 1. Notations

Notations	Explanation
A, B, C, D	Users
A_i	ith interests of user A
PK_A	Paillier public key of user A
PK_B	Paillier public key of user B
SK_{CA}	Signature of CA
R	2 bytes Random number
$(A_i)_{PK}$	*i* individual interests separately encrypted in paillier public key of a user
CA	Certification Authority

3.4 Working of Proposed Scheme

Our scheme is divided into two phases namely the encounter phase and the profile matching phase. There is a certification authority (CA) that verifies the credentials of all the participants. The proposed scheme uses Paillier cryptosystem for encryption and decryption. The paillier cryptosystem is an additive homomorphic system that allows the addition of ciphertexts.

3.4.1 Encounter Phase

The broadcast encounter phase further categorized into a registration phase, formulation of interest phase and encounter broadcast phase.

- **Registration Phase**

In this phase, a user generates a paillier public/private key pair and sends his/her unique real identity for example mobile number or social security number (SCN) along with

her public key and a time stamp (T) to a certification

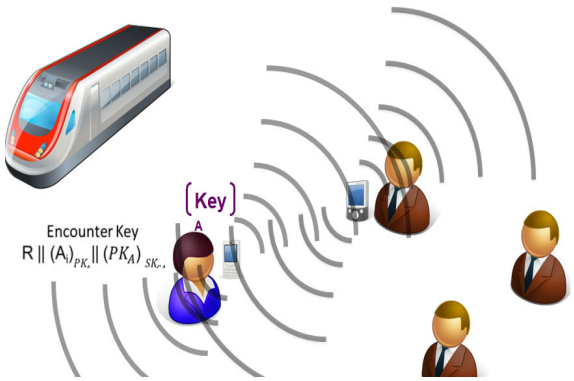

Fig. 3 Encounter information exchange

authority (CA). In next step, CA signed user A's public key and send this back to A. CA keeps the correspondence of real identity and public key for future conflicts.

1. A → CA : URI (Unique real identity)|| PK_A||T (Time stamp)
2. CA → A: $(PK_A)_{SK_{CA}}$

- Formulation of interest sets

A and B make their respective sets according to a super set, such that the Super set is like the following. S ={Athletic, Baseball, cricket, Demography, Movies…. }. That is, A and B sets the corresponding element of their set to a "1", where they show an interest and a "0", where they don't have an interest in that field of S. For example, A = {1, 0, 1, 0, 0, …} and B = {0,1, 1, 0, 0, …}.

In case an addition of the corresponding elements of the sets is performed then a value of "2" shows a match, otherwise a no match.

A+B = {1, 1, 2, 0, 0, …}

where 2 shows there is a matching in respective interest.

After the formulation of the interest set, each user encrypts each element of the set with its paillier public key like the following.

$\{(A_1)_{PK_A}, (A_2)_{PK_A}, \ldots..,(A_n)_{PK_A}\}$ is the encrypted set of *n* interests of user A.

- **Broadcast on Encounter**

After registration, user A generates a 2 bytes random number R and broadcasts his/her encounter information to all peers. This encounter information includes R and signed public key and encrypted interest set. Fig. 3 shows encounter information broadcast.

3. A generates 2 Byte R.
4. A → all peers : R || $(PK_A)_{SK_{CA}}$ || $((A_i)_{PK_A}$ *where i = 1 to n*
5. B receives broadcast

2. Profile matching phase

The profile matching phase is performed on a server namely profile matching facilitation server (PMFS).

Later, user B performs the following steps to communicate with user A. User A and B communicate through a profile matching facilitator server (PMFS). A sends his/her encrypted interests along with his/her public key, signed public key and the nonce R to PMFS. Nonce are the random number use to prevent from replay attack. User B also sends the same information to the PMFS. Both the users identify their previous encounter with the help of signed public key and R.

6. A → PMFS : R || $\{(A_1)_{PK_A}, (A_2)_{PK_A}, \ldots..,(A_n)_{PK_A}\}$ ||PK_A || (PK_A) $)_{SK_{CA}}$
7. B→ PMFS : R || $\{(B_1)_{PK_B}, (B_2)_{PK_B}, \ldots..,(B_n)_{PK_B}\}$ ||PK_B || (PK_B) $)_{SK_{CA}}$

Once both parties posted the information to the server, server will exchange the information to the parties. A and B will encrypt their interests with each other's paillier public key, compute the addition homomorphically and will send the encrypted results to the PMFS.

8. User A will compute $(A_i)_{PK_B}$ +$(B_i)_{PK_B}$= $(X_i)_{PK_B}$
9. User B will compute $(A_i)_{PK_A}$ +$(B_i)_{PK_A}$= $(Y_i)_{PK_A}$

Server will send $(X_i)_{PK_B}$ to B and $(Y_i)_{PK_A}$ to A, blindly.

10. PMFS → A: $(Y_i)_{PK_A}$
11. PMFS → B: $(X_i)_{PK_B}$

Both parties decrypt the results and find the matches securely by counting corresponding 2s.

4. Result and Discussion

This section contains the detailed discussion on simulation and results. The results show the performance and feasibility of proposed scheme.

4.1 Experimental Setup

The proposed scheme has encryption, decryption and addition operation based on Paillier cryptosystem. During

the implementation, the computational cost of these operations is calculated, and finally overall cost is considered. The test bench is comprised of a computer with i7 processor and 8 GB of RAM. The implementation uses JAVA due to its rich support for cryptographic primitives. To get average execution time, the simulation was executed 100 times.

4.2 Result and Discussion

During implementation, the total number of interests are 500 and time is calculated in milliseconds.

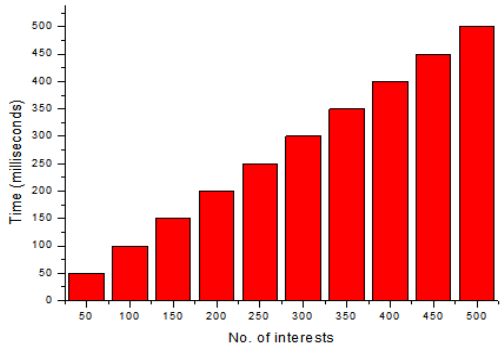

Fig. 4 Total Time for i Paillier Encryption

Fig. 4 shows the total time taken by i paillier encryptions. The result shows the linear increment. The time for encrypting 50 interests is only 0.05 seconds and for 500 interests are 0.5 seconds.

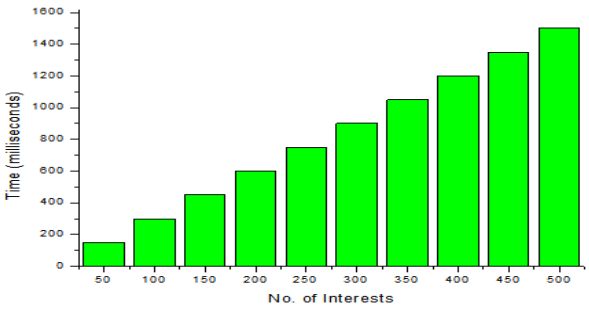

Fig. 5 Total Time for i Paillier Decryption

The Paillier decryption is also calculated during experiment. The decryption takes more time than encryption because of the Paillier cryptosystem property. The Fig. 5 shows that for 50 interests, the decryption cost is 3 times more than encryption. The time for 50 interests is around 0.16 seconds and for 500 interests is around 1.6 seconds.

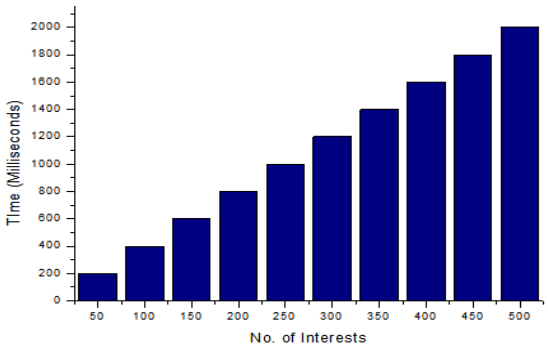

Fig. 6 Overall Computational Cost

The total cost for execution of 50 interests is around 0.2 seconds only and for 500 interests is 2 seconds. This performance shows that our proposed scheme is feasible for encounter-based MSN user. Because, proposed scheme does not require real time processing and user can compute it anytime. Fig. 6 shows overall computational cost.

4.3 Security Analysis

The existing work has some issues for example Sybil attacks, impersonation attack and privacy preservation. Our proposed scheme is providing reasonable security from these issues.

4.3.1 Sybil attacks prevention

The registration phase prevents assigning multiple public keys to a single user. A user cannot run protocol again and again with a different key. If a user detects multiple protocol attempts with a single key, he/she simply ignores.

4.3.2 Impersonation attack prevention

Only the authorized user holds his/her public private registered key pair. No user can impersonate until a user keeps his/her cryptographic credential safe.

4.3.3 Privacy preservation

User's interests are encrypted and therefore, only the successful profile matching allows users to share mutual interests. This also prevents PMFS learning the private interests of users. The PMFS blindly facilitates users to exchange their encrypted results.

4.4 Comparison with existing work

Table 2 shows the comparison of proposed scheme with SMILE [3], Mohein et. al. [7] and Bhattacariya et. al.

[11] with respect to different parameters. The proposed scheme prevents each of the impersonation and sybil attacks. The encrypted computations do not allow other users or PMFS knowing the results and therefore, our proposed scheme preserves the privacy of user profiles. The only identity is a signed public key that does not reveal user's actual identity.

Parameters	[3]	[7]	[11]	Proposed Scheme
Impersonation attack prevention	x	√	x	√
Sybil Attacks Presentation	x	x	x	√
Privacy preservation	√	x	√	√

Table 2 Comparison with existing work

5. Conclusion and Future Work

This research proposes a privacy preservation technique for Mobile Social Network (MSN). The MSN has many paradigms and applications. This research proposes a secure and privacy preserving profile matching scheme for encounter-based MSN that uses Paillier cryptosystem. The proposed scheme has two phases i.e. encounter phase and profile matching phase. Users share the encounter information and later communicate with each other on a server. The encounter information comprises of user's personal identity, encrypted results and public key. The certification authority (CA) signs a user's public key to prevent future conflicts. A user broadcasts the encounter information to all peers in the vicinity for example at subway, university etc. At a later time, users find each other on a profile matching facilitation server with the help of encounter information. They encrypt their interests with each other's' paillier key and exchange the encrypted interests through the server. If a number of interests are matched, then they can be friend.

To analyze the feasibility of proposed scheme, we calculated the execution time that is required to encrypt and decrypt the interests. Our implementation uses JAVA for its rich support for the cryptographic primitives. The experimental analyze shows the feasibility of proposed scheme.

The proposed scheme is evaluated on static system. In future, the proposed scheme feasibility can be checked on mobile devices. Moreover, we aim to extend the number of interests and also aim to further evaluate the security of the proposed scheme with more attack scenarios.

References

[1] Najaflou, Y., Jedari, B., Xia, F., Yang, L. T., & Obaidat, M. S. "Safety Challenges and Solutions in Mobile Social Networks," IEEE Systems Journal, 2013.

[2] R. Zhang, Y. Zhang, J. Sun,and G. Yan," Fine-grained Private Matching for Proximity-Based Mobile Social Networking," IEEE INFOCOM, pp. 1969- 1977, 2012.

[3] J. Manweiler, R. Scudellari, and L. P. Cox, "SMILE: encounter-based trust for mobile social services," 16th ACM conference on Computer and communications security, pp. 246-255, 2009

[4] R. Agrawal, A. Evmievski, and R. Srikant, ``Information sharing across private databases," in Proc. ACM Int. Conf. Manage. Data (SIGMOD), 2003, pp. 86-97.

[5] Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," IEEE 9th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 252-259, 2011.

[6] Y. Wang, J. Hou, Y. Xia, and H. Z. Li, ``Efficient privacy preserving matchmaking for mobile social networking," against malicious users," Concurrency Comput., Practice Exper., vol. 27, no. 12, pp. 2924-2937, 2015.

[7] A. Mohaien, D. F. Kune, E. Y. Vasserman, M. Kim, and Y. Kim, " Secure encounter-based mobile social networks: Requirements, designs, and tradeoffs," IEEE Transaction on Dependable and Secure Computing, vol. 10, no. 6, pp. 380-393, 2013.

[8] N. Eagle and A. Pentland, ``Social serendipity: Mobilizing social software," IEEE Pervasive Comput., vol. 4, no. 2, pp. 28-34, Jan./Mar. 2005.

[9] L. P. Cox, A. Dalton, and V. Marupadi, ``SmokeScreen: Flexible privacy controls for presence-sharing," in Proc. ACM 6th Int. Conf. Mobile Syst., Appl. Services (MobiSys), 2007, pp. 233-245.

[10] H. Li, Y. Chen, X. Cheng, K. Li, and D. Chen, "Secure friend discovery based on encounter history in mobile social networks," Springer Journal of Personal and Ubiquitous Computing, vol. 19, no. 7, pp. 999-1009, 2015.

[11] Bhattacharjee, S., & Bit, S. D. (2019). EnTER: an encounter based throwbox deployment strategy for enhancing network reliability in post-disaster scenarios over DTN. In Proceedings of the 20th International Conference on Distributed Computing and Networking (pp. 413-416). ACM.

[12] A. Nagender, and S. Gambhir. "Recent Advances in Ad-Hoc Social Networking: Key Techniques and Future Research Directions." Wireless Personal Communications (2020): 1-19.

[13] P. Paillier and D. Pointcheval, “Efficient public-key cryptosystems provably secure against active adversaries,” in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 1999, pp. 165–179.

[14] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 223–238.

[15] C. heng-Hao, W. Chuen Wu, C. Wang, Tzung-Shi Chen, and J. Chen. "Friend recommendation for location-based mobile social networks." IEEE seventh international conference on innovative mobile and internet services in ubiquitous computing, pp. 365-370, 2013.

Dr. Fizza Abbas received the bachelor's degree in computer system engineering from the Quaid-e-Awam University of Engineering, Science and Technology (Quest), Pakistan, in 2007, and the master's degree in communication system and networks from Mehran University, Pakistan, in 2011. She successfully completed her PhD in Computer Engineering from Hanyang University, Korea in 2017. Her research interests are security and privacy in social network services, mobile social networks, cloud computing, mobile cloud computing, and vehicle ad hoc networks. She has more than 12 years of teaching experience and currently working as Associate Prof. in Quest Pakistan. She has served as a reviewer in many conferences and journals. She is an author of many International and national papers.

Dr. Ubaidullah Rajput received his bachelor’s degree in Computer System Engineering from Quaid-e-Awam University of Engineering, Science and Technology (Quest), Pakistan in 2005. He received his Master's in Computer System Engineering from NUST Islamabad, Pakistan in 2011. He successfully completed his PhD in Computer Engineering from Hanyang University, Korea. His research interests are security and privacy issues in crypto-currency, security and privacy issues in VANETS, Internet of Things (IoT), mobile social networks and cloud computing. He has more than 15 years of teaching and research experience and currently working as Associate Professor. in Quest Pakistan. He has served as a reviewer in many conferences and journals. He is author of many International and national papers.

Dr. Umair A. Khan received his Master and PhD degrees from Alpen-Adria University, Klagenfurt, Austria in 2010 and 2013, respectively. Since then, he has been working as an associate professor and head of the department of computer systems engineering in Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, Pakistan. He has also worked in Fraunhofer Institute of Integrated Circuits, Erlangen, Germany, and Machine Perception laboratory, Hungarian Academy of Sciences, Budapest, Hungary as a research scientist in 2016-17. His research interests include context-based information retrieval from images and videos using deep learning.

Farwa Abbas received the bachelor's degree in electronic engineering from the Quaid-e-Awam University of Engineering, Science and Technology (Quest), Pakistan, in 2012, and the master's degree in communication system from Quaid-e-Awam University of Engineering, Science and Technology (Quest),, Pakistan, in 2019.