Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

A Cryptographic Framework for Ensuring Secure Location Privacy in Mobile Social Networks Using Lightweight Elliptic Curve Encryption Techniques

Muzammil Hussain
Department of Telecommunication, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshsah, Sindh, Pakistan. Email: hussainmuzammil979@gmail.com
Usama Ahmad Mughal
Department of Cyber Security, NASTP Institute of Information Technology, Lahore, Pakistan. Email: usamaahmad@niit.edu.pk
Shazia Feroz*
Department of Electronics Engineering Technology, Benazir Bhutto Shaheed University of Technology and Skill Development, Khairpur Mir's, Sindh, Pakistan.
Corresponding Author Email: shaziaferoz@bbsutsd.edu.pk
Fatima Qureshi
Department of Telecommunication, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshsah, Sindh, Pakistan.
Email: Qureshi080@gmail.com

ABSTRACT

The widespread adoption of smartphones and the exponential growth of Mobile Social Networks (MSNs) have significantly transformed how individuals interact, share information, and connect with their surroundings in real time. Among the core functionalities of these networks, location sharing has emerged as a vital component, enabling services such as friend discovery, check-ins, localized advertisements, and real-time assistance. However, while these features enhance user engagement and service personalization, they also introduce severe threats to user privacy. Disclosing precise geographic coordinates to service providers or peers without adequate security mechanisms exposes users to potential risks, including location tracking, profiling, stalking, and unauthorized surveillance. This research presents a lightweight cryptographic framework aimed at securing user location privacy in MSNs by leveraging the strengths of Elliptic Curve Cryptography (ECC). ECC is chosen for its ability to provide strong encryption with smaller key sizes, making it particularly suitable for resource-constrained mobile environments. The proposed framework

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

ensures secure communication between users and location-based service servers while effectively concealing actual location data from any unauthorized third parties, including potential adversaries and even the service providers themselves. The framework employs a location obfuscation mechanism combined with ECC-based key exchange and encryption protocols to ensure end-to-end confidentiality and user anonymity. Additionally, it incorporates techniques to minimize computational overhead and bandwidth consumption, thereby maintaining optimal performance in mobile settings. The security and efficiency of the proposed scheme are rigorously evaluated through analytical modeling and simulation, and the results are benchmarked against several state-of-the-art privacy-preserving location-sharing protocols. The evaluation demonstrates that the proposed solution not only enhances location privacy and data confidentiality but also significantly reduces computational and communication overhead compared to traditional cryptographic approaches. This research contributes to the growing field of privacy-aware mobile social networking by offering a scalable, secure, and efficient location privacy solution that can be practically deployed in real-world scenarios.

Keywords: Mobile Social Networks (MSNs), Location Privacy, Elliptic Curve Cryptography (ECC), Secure Communication, Lightweight Cryptographic Protocols, Privacy-Preserving Framework.

Introduction

Mobile Social Networking Platforms, which are a key tool in our daily communication due to the development of smartphones and cellular technology, have been experiencing exponential growth. Through the use of location aware capabilities on mobile devices, MSNs the user's physical and social worlds are bridged. Users, the privacy of location is also a big concern for them because they must be able to provide their precise location information to friends or service providers when using this service. Any information about users, such as their user name, precise location and query content, shall be collected by the central service provider. The user's sensitive information will be at risk if private information is disclosed by a potentially untrustworthy service provider or compromised by an adversary. Location Based Services LBs is also more popularity with increasing demand of smart phone or laptop

Online ISSN 3007-3197
Print ISSN 3007-3189

and tablets. Through play store we can download the app related to Location based service such as interest finder, check-in service and navigation etc. They can be divided into two categories, in particular. Privacy of location and query, which is usually maintained using policy solutions, primitive cryptographic approaches, rudimentary perturbations or other methods such as dispersive spatial concealment techniques or some other method. Location based services LBs is also more popularity with increasing demand of smart phone or laptop and tablets. Through play store we can download the app related to Location based service such as interest finder, check-in service and navigation etc. Then, user can easily resolve the queries relate to LBS [1]. The increasing usage of mobile social networks has led to heightened concerns regarding location privacy. Users frequently share their real-time locations, exposing themselves to various privacy risks such as unauthorized tracking, stalking, and potential physical harm. Despite the availability of privacy settings, users often struggle to effectively manage and understand the implications of sharing their location data within these networks. This raises the need for comprehensive solutions that address the complexities of location privacy in mobile social networks, ensuring that users can enjoy the benefits of social connectivity without compromising their personal privacy and security. Therefore, this research proposed an approach that use ECC encryption technique to provide location privacy in LBS for MSN users [2].-We shall consider the various mechanisms and comparison of different techniques used in location privacy preservation services following an analysis.in the future research, the open challenges are helpful for researcher in the field of LBS [3].

Researchers proposed two methods related to location privacy first is a lightweight order- preserving encryption-(OPE) based Scheme this method allows for a flexible privacy location, which can be maintained at an unrelated level of security. This provided method preserves the privacy of user location with respect to friends, service provider, fully trusted party (FTP) and adversaries. Second one can provide the preservation location privacy under unrelated contexts is user-defined location-sharing Scheme (ULSS). Researcher proposed a course- grained proximity detection method. Through different experiment to verify the efficiency and effectiveness of our proposed method [7]. The encryption system is divided into a preparatory and online

Online ISSN 3007-3197
Print ISSN 3007-3189

phase, transferring most of the decryption burdens from the requester to the matching server in order to reduce the user's cryptography and decryption costs. The experiment results showed that the system ensures user privacy, while at the same time eliminating communication overheads [8]. We are discussing threats to location privacy in this report and examining some recent proposals for mechanisms focused on the protection of a person's location when he or she is crowdsourcing [12]. In addition to the Intelligence Crowd Sense Network, Confusion Mechanism and Block Chain, it is possible to divide its network structure into three parts. The results show the effectiveness of the incentive mechanism in this paper to stimulate user engagement, which we have been testing on a campus environment [15]. Particularly, this method is based on request content and location distance. By using the extensive stimulations is validated of our effectiveness scheme it provide the better efficiency and location privacy preservation [18]. The effectiveness of the extracted features in estimating social connections is confirmed by extensive experiments in the real world data set and our method is significantly superior to the baseline models [20]. ECC Elliptic Curve Cryptography and RSA algorithm. Based on these findings, Compared to the RSA algorithm, ECC is more effective in terms of memory requirements, energy consumption, key size, signature generation time, execution time and decryption speed. When it comes to verifying signatures and encrypting data with a constrained environment. The algorithms are reviewed in detail from various aspects of ECC and RSA in the present research, and in all parameters, ECC could be an excellent RSA [32].

The review explains why ECC has become a major trend in the current scenario of encryption. Some attacks by the ECDSA, such as Pollards Rho and Pohlig Hellman., but they're very slow as far as the RSA attack is concerned. In order to improve the security of ECDSA, it is possible to carry out further work in this direction by applying more sophisticated ECC computations [33]. As regards complexity and robustness, the results of the proposed system's implementation are promising. The results confirm that for signature generation and verification, the planned scheme is efficient and reliable [34]. Against classical computers and quantum computers, the operation of the NTRU lattice cryptosystem is efficient and

Online ISSN 3007-3197
Print ISSN 3007-3189

secure. A security and performance analysis of our scheme shows that the model is more safe and effective than current models, which will be replaced by new models for the protection of data from quantum computers [35]. In this research privacy preserving scheme has been proposed. Proposed scheme aimed at ensuring secure communication between users and location-based servers while concealing their locations, achieved through the utilization of ECC (Elliptic Curve Cryptography). Moreover, evaluate the effectiveness of this scheme by comparing it with recent approaches.

Preliminaries

This section explain the system model, design model, attack scenario and assumption related to cryptographic tool that is used in this paper.

System Model

The system model architecture use Mobile Social Network (MSN) component consists of Mobile users, LBS, CA, MSN. In our system model Mobile user can request for the service of LBS to the nearby MSN which is called user to MSN communication and MSN installed unit to allow user can exchanged message safely among the MSN. The MSN is considering to support the mobile user in the communication system, this trust is increasing the mobile user. The CA and Location based server are application server which receive the request from different mobile user Location through the wireless internet broadcast.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

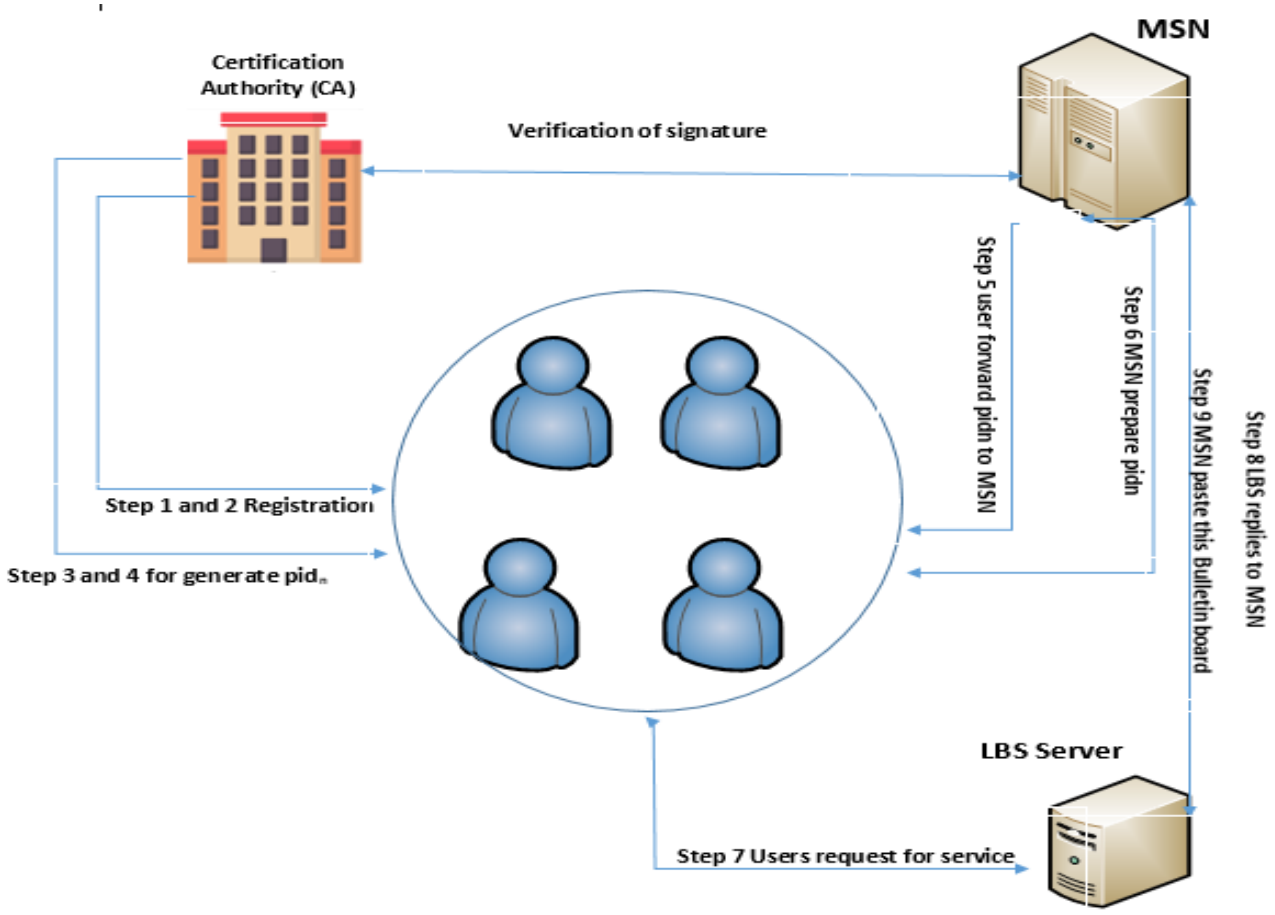


Fig no 1: System Model of our Scheme

In this Scheme CA and LBS server and MSN server are used for define the scenario of the proposed Scheme.

Phase No 1 Registration of the User

- User sends request to CA for Registration through real identity.
- User send e-mail to CA and request for Master PID.
- CA is store that information in to its database and send PKI and SKI key pair to user.
- User generate pair of keys and send all public keys to CA for generating pidn.
- CA is verify and store in to its data base generate pidn send to all pids to user.
- User sends to all pids to registration to MSN for generating MSNuserid.
- MSN generating the MSNuserid and send to user.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Phase No 2 Providing Service to the Users

- Users request the services through MSN to the LSB server.
- LBS store this data in to its data base and send services to MSN.
- MSN received this service and store in to its data base and upload on the bulletin board.
- Users can see the bulletin board and decrypted the message safely.
- LBS will no able to known any information from MSN Bulletin Board because data is posted them with MSNuserid.
- CA is also cannot known services because CA cannot known the identification Pid to MSNuserid.
- MSN only known pid not the actual user information.

Phase No 3 Billing Phase

In this phase LBS provide the billing to user through use channel of MSN bulletin board.

The research aims at developing a system that will ensure reliable communication of user and location based server with hidden locations, as well as an authentication scheme which can be used without compromising any security risk calculate the minimum computation and communication cost.

Attack Model

To classify attackers on the basis of their behavior and capabilities. Their classification includes. Because of their detailed knowledge of the network, these insider attackers should be regarded as a very serious threat. Due to their knowledge of network configuration, eavesdroppers can carry out a variety of sophisticated attacks. The outsider is not a member of the network, and they are seen as much more harmful than an insider. The primary goal of the malicious attackers is to disrupt and degrade network performance without any personal benefits. These attacks are difficult to detect, which may have a serious impact on the network. Now, different scenarios of insider and outsider attacker are discussed below:

Privacy and Security Issues in MSN

As the saying goes, people don't just communicate with their friends and near ones;

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

they also talk to strangers. All over the Internet, there are a lot of strangers. Consequences of Users will be very negatively influenced by the contact of strangers, making them vulnerable to privacy and security concerns. Not all, but a lot of strangers aren't trustworthy. There is no possibility of safeguarding the information shared with these strangers. Such strangers can even obtain user information, if they are not aware of users and sometimes in tricky ways. The severity and importance of information sharing shall be decisive in determining the extent to which there is danger. Privacy will also be an issue in addition to safety issues due to the dissemination and leakage of information [4].

Hacker are the most dangerous person in the cyber world. It's risky to be an unknown enemy, as opposed to familiar enemies. The misuse and sale of user information by these hackers is very dangerous. It means, for example, that the information of a user can be opened in relation to security and privacy concerns both on MSN as well. In MSNs, we give a brief overview of some important privacy and security issues:

Issue of Direct Anonymity: Attackers are attempting to hack a user's shared Social Network ID in order to see his identity and any information or details about him. This issue has been seen in both the user-server domain as well as User-user Domain. You can find this problem with one of these domains. Attackers can make it easy to break other related user data by taking a single information from the user [4].

Issue of k-Anonymity or Indirect Anonymity: Here, the attackers are trying to find or map a user's identity by brute forcing every N number of data about that user and uniquely mapping it. Similarly, this problem exists for both user and server-user sites. To solve this problem, an algorithm that uses a minimal set with information on it must be developed. A user who can't directly map to the users, instead maps to a K or smaller number of users. This could lead attackers into a state of confusion when they discover the identity of their original user [4].

Other Different Attacks: There's a lot of other attacks, like tricking, eavesdropping, wormhole attack and relay. That are related to the user's shared network ID. These attacks mainly occur in the user-user domain because the HTTPS protocol, which is much safer than these types of attacks, protects the user-server domains. These types

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

of attacks should therefore be avoided for user domain [4].

Malicious Attack: The identity of users, their profile information and the possible creation of fake user data can be exploited by these attackers. They're weakening network resources and sometimes damaging data that was provided by the first users. As a result, these attackers create threats such as counterfeiting and tampering which are the main problems to be solved in MSN. As yet, MSN continues to have an open problem of how best to detect these malicious attackers [4].

Sybil Attack: In that case, the attacker manipulates a user's identity so as to reduce overall confidence and system performance in MSN. Three types of Sybil attacks are known as SA 1, SA 2 and SA 3. Only attacks that have been identified with SA 3 are found in the mobile domain. In areas such as the social domain and sensing domains, more attacks are discovered. They're doing nothing in terms of mobility. Therefore, one of the open MSN problems that needs to be resolved is how to deal with a SA3 attack [4].

Attack Scenario

Scenario No 1

CA want to know about the services of the Users.

Proof: CA cannot know the services of users because CA cannot know about the pseudonyms identity that is provided by the MSN so, CA is called semi trusted party in this Scheme

Scenario No 2

MSN want to access about the real identity of the Users

Proof: MSN cannot know about the real identity of users because User can communicate with MSN through pseudonyms identity so, MSN is also called semi trusted party in this Scheme.

Scenario No 3

LBS want to access about the real identity and Location of the Users.

Proof: LBS cannot know about the real identity and location of users because User can request for the service through pseudonyms identity so, LBS can only access bulletin board.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Scenario No 4

If Outsider want to access real identity of the Users.

Proof: The outsider cannot decrypt the pseudonyms identity of user because CA sign this identity through ECC technique, ECC is assumed a fully secure it cannot decrypt because ECC is based on the discrete logarithm problem generating G $g^x \equiv h$ and h= (mod x) it's so difficult to decrypt [39].

In threat model different Scenario have need discussed and shows the behavior of our proposed Scheme against attacker. These Scenario shows how proposed Scheme provides privacy while exchanging information over the network.

Working of Proposed Scheme

In this Scheme CA and LBS server and MSN server are used for define the scenario of the proposed Scheme.

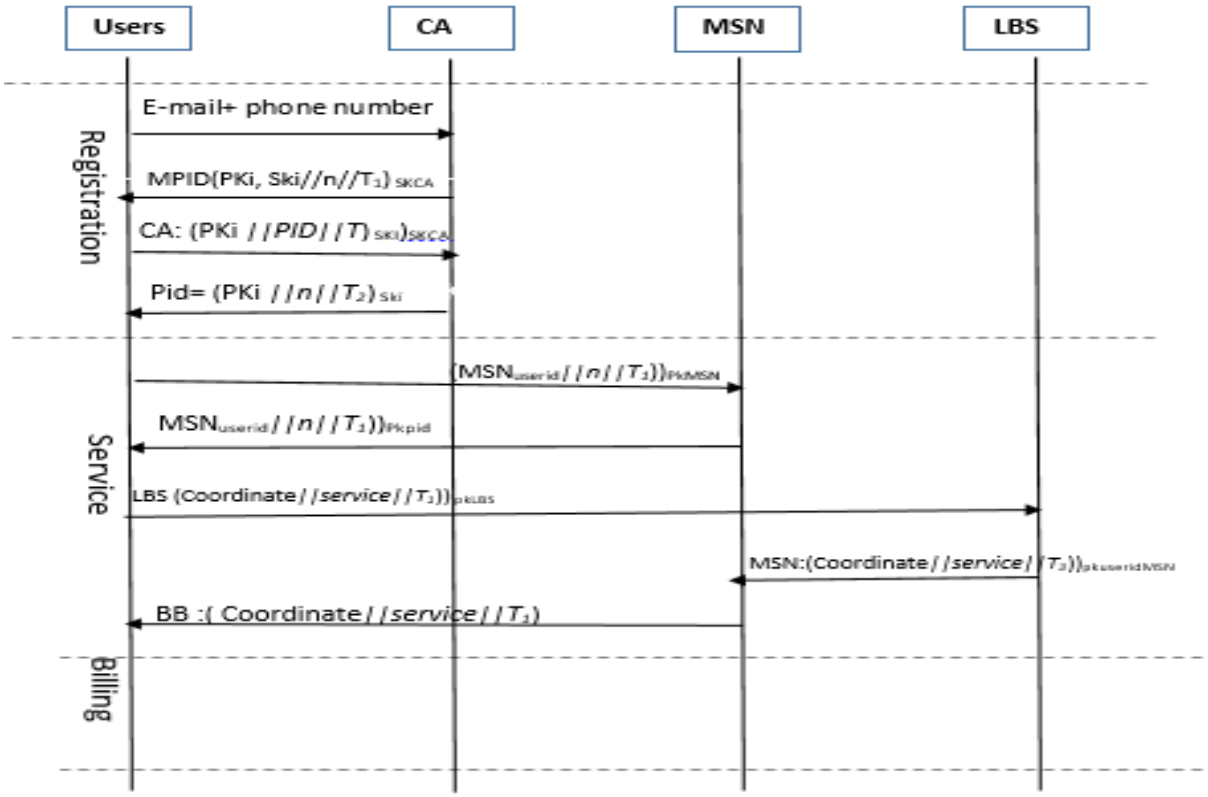
- **Step 1 Registration**
- **User ⟶ CA (Email)**
- **Step 2 CA response to user**
- **CA ⟶ user :(MPID= $(PK_i, SK_i//n//T_{exp}))sk_{CA}$**
- **Step 3 User generates n pki/ski key pair and send n pki to CA.**
- **User ⟶ CA: $(pki //n//T_{exp})_{SKi})_{PKCA}$**
- **Step 4 CA prepare n pids for user**
- **CA ⟶ user pids= (pid1, pid2, pid3----------pidn) PK_{pID}**
- **Pid= $(pk_i //n//T_{exp})Sk_{CA}$**
- **Step 5 user Forward pidn to MSN**
- **User ⟶ MSN $(MSN_{userid}= (pk_i, //n//T_{exp}))pk_{MSN}$**
- **Step 6 MSN prepare MSN $userid_{MSN}$**
- **MSN ⟶ MSN $(MSN_{userid} = (pk_{userid}, sk_{userid} //n//T_i))\ sk_{msn}$**
- **Step 7 User Request for service**
- **User ⟶ LBS: $(Coordinate//service//T_{exp}))pk_{LBS}$**
- **Step 8 LBS replies to MSN**
- **LBS ⟶ MSN :($Coordinate//service//T_{exp}))_{pkuseridMSN}$**

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

- **Step 9 MSN upload the service on bulletin board**
- **MSN ⟶ BB :(Coordinate//*service*//T_{exp})**
- **Step 10 User decrypt the information with Secrete key**
- **Step 11 LBS Provide billing.**

Flow of Our Scheme



Notations

A comparison of the methodology is shown in Table 4.1. To help you figure out the symbol and cryptography primitives to build a network model with this notation, it is included in our system model which explains them.

Notation

Notation	Description	Size
UserMn	Sender user	-
PKi, SKi	ECC public/private key pairs of	32 Bytes (Each)

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

SigCA	CA signature	64 Bytes
T1, T2	Expiration time set by CA	4 Bytes
PKCA	CA public key	32 Bytes
MSNUser id	Pid assigned by MSN	64 Bytes
PKc	Certificate Authority public key	32 Bytes
ski-CA	Certificate Authority signature	64 Bytes
Texp	Expiration time set by user	4 Bytes
H	Hash function	20 Bytes
N	Nonce	32 Bytes
Pid	Personal identifier	32 Bytes

Result and Discussion

In our proposed the time to provide LBS services to users is better to the other Scheme. As the number of users increase proposed Scheme Show better result.

In proposed Scheme we add feature for example email for registration and pseudo identity concept.

The workflow of our proposed Scheme makes it computational efficient. Moreover, the use of ECC Cryptosystem provide security overhead that makes proposed Scheme efficient.

The implementation of Encryption, Decryption, Key and signature generation and verification time and total time taken result are shown below.

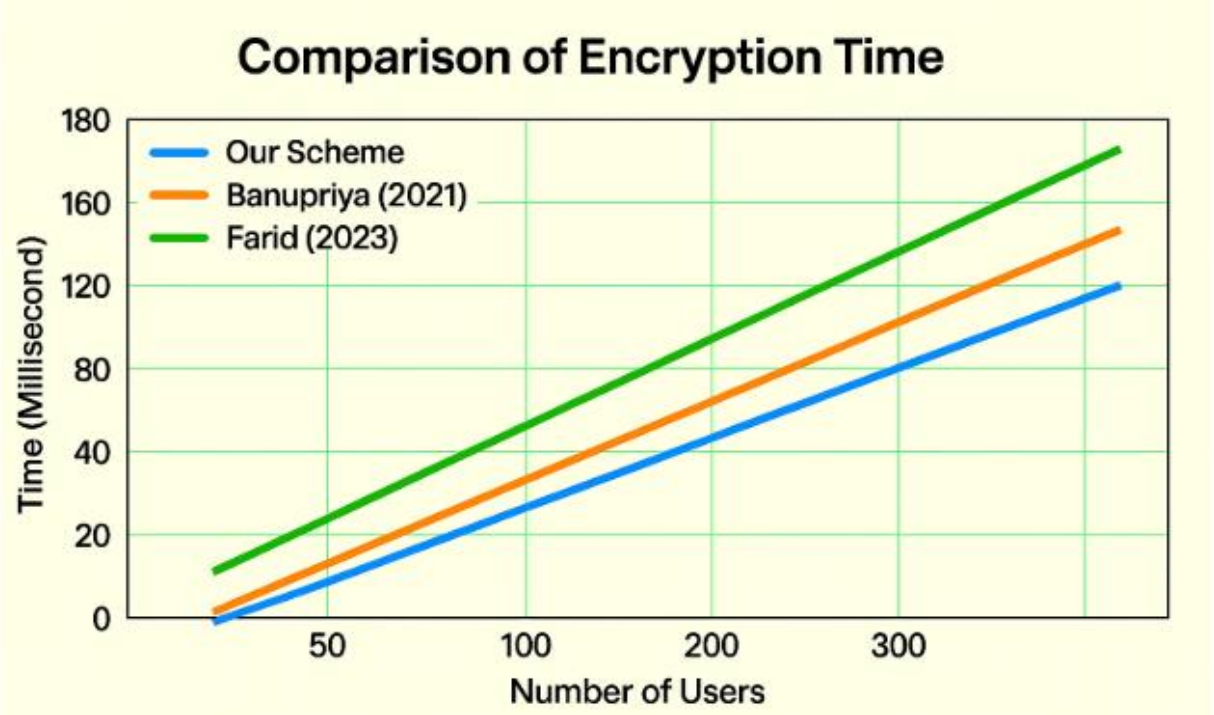
Encryption Time for Services

During the implementation, MSN's total number of users is 300 and time to encrypt requests for services is calculated at millisecond figure 5.1. ECC encryption is used in this scheme, which shows the effective computational costs. It took only 24.4 milli seconds to encrypt a 50.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about



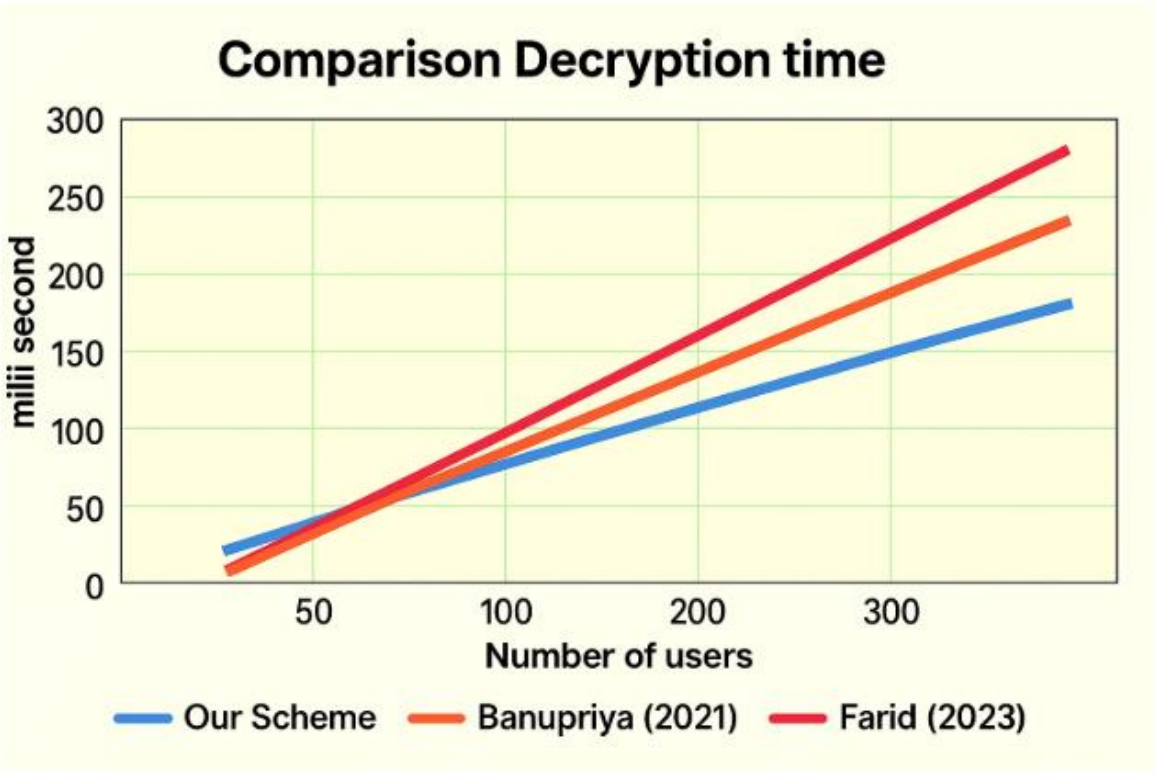
Decryption Time for the Service

During the experiment, the decryption time for services shall also be calculated. It takes more time to decrypt than it does to encrypt. The LBS is decrypting a request for services that the proposed system uses ECC encryption in order to demonstrate efficient computational costs. According to the figures 5.3 and 5.4, for 50 user requests, the LBS server costs only 33ms to decrypt.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about



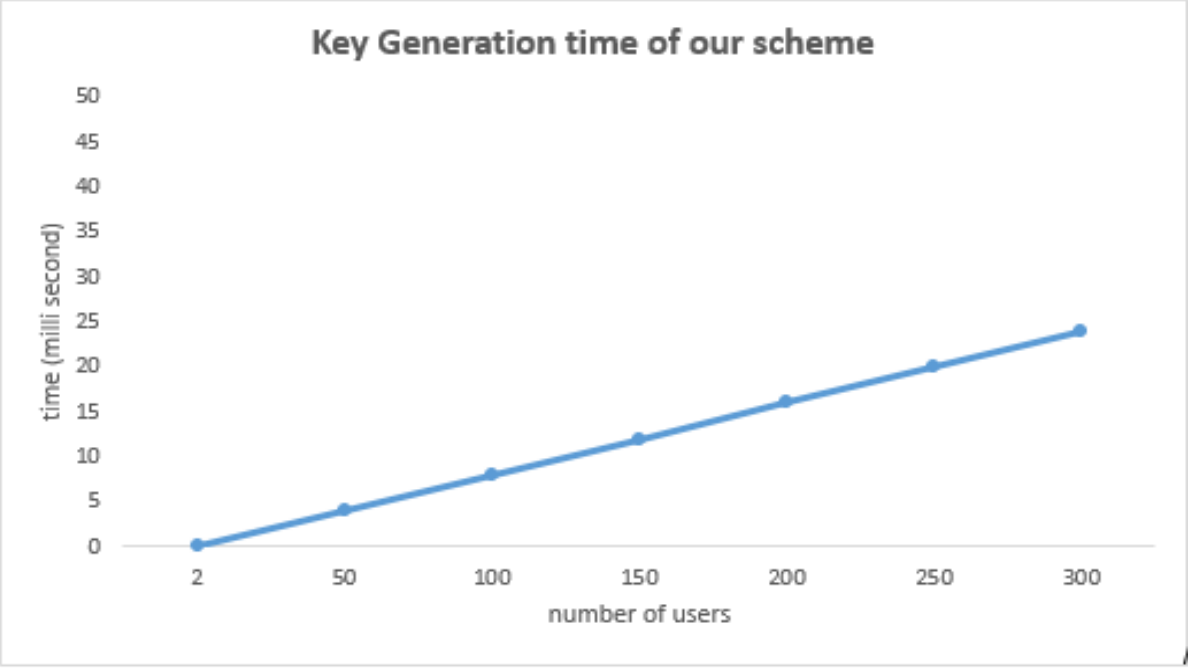
Key Generation Time

During the experiment, the key generation times for services shall also be calculated. It takes less time than encryption and decryption to generate a key. Figure 5.5 and figure 5.6 shows that for a 50 user request, the LBS server will cost just4ms to

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about



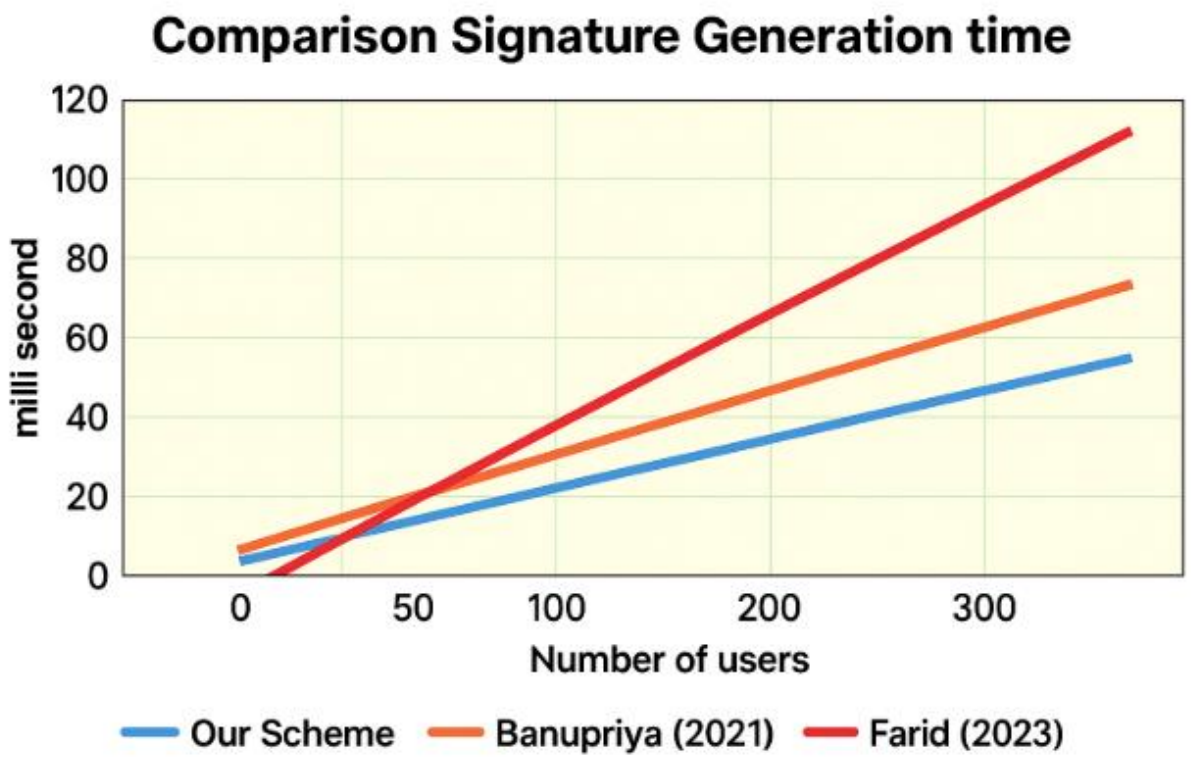
Signature Generation Time for the Service

During the experiment, time for signature generation of services shall also be calculated. It takes less time to generate a signature, as opposed to encryption. The efficient computational cost is shown by the CA's signature generation of the request for the service that the proposed system uses the ECC signature. Figure 5.7 and 5.8 show that for 50 user requests, the cost to CA of signature generation was just 17.5ms.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about



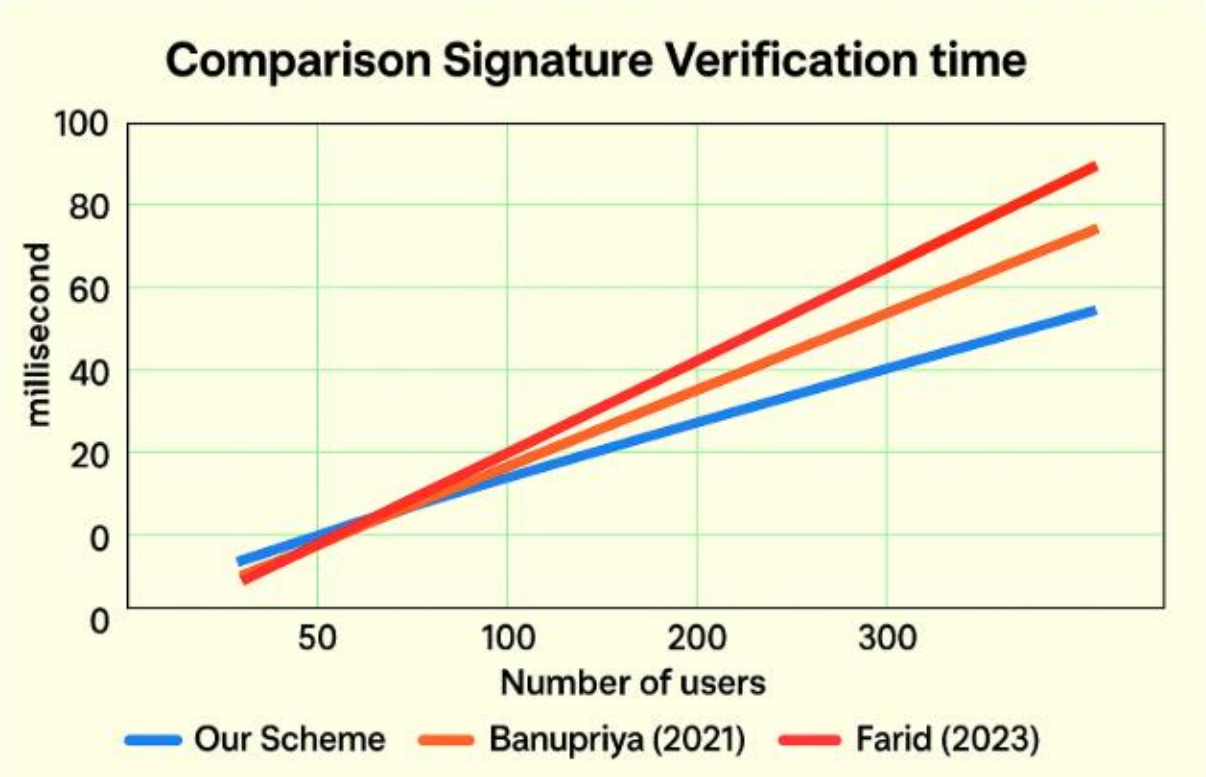
Signature Verification Time for the Service

During this experiment, the duration of signature verification for services shall also be calculated. It takes less time to verify the signature as opposed to encryption. The LBS shall perform the signature verification of the service proposed for use in the ECC Signature validation system, showing its efficient computational cost. For a total of 50 user requests, the figure 5.9 and 5.10 show that for Signature verification by LBS server only 11.5ms are available.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about



Total Time Consumed by our Scheme

The Total time consumed by our Scheme is also calculate during an experiment. The LBS perform the Total time consumed by our Scheme and proposed Scheme utilize ECC total time consumed show the efficient computational cost. The figure 5.11 and figure 5.12 shows that for Total time consumed by our Scheme for just 97.7s for the 50 users.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 8 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

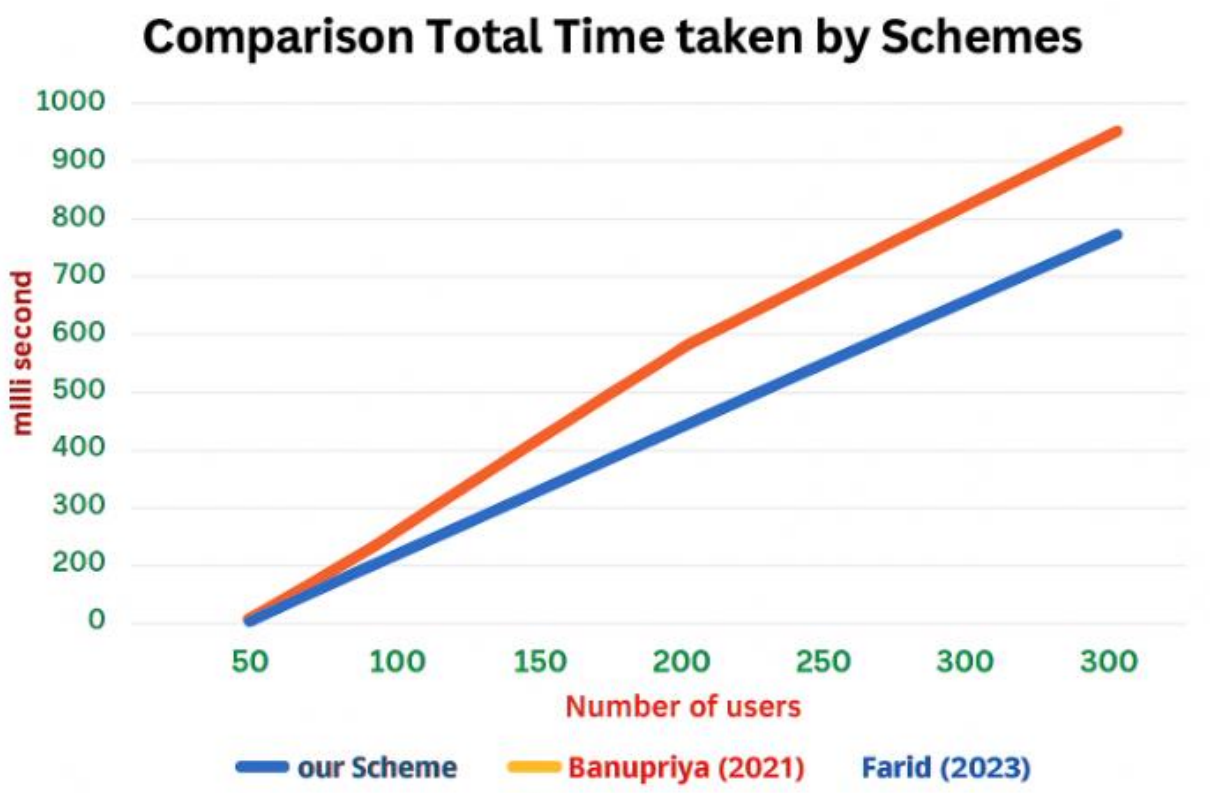


Table 2 Total Time Consumed by our Scheme

Total time consume of our scheme using (ECC)163						
Number of users	Key generation time(msec)	Encryption time(msec)	Decryption time(msec)	Signature generation time(msec)	Signature verification time(msec)	Total time in (msec)
2	0.16	0.976	1.32	0.3	0.46	3.216
50	4	24.4	66	7.5	11.5	97.7
100	8	48.8	113	15	23	135.4
150	12	73.3	198	22.5	34.5	243.2
200	16	97.6	264	30	46	345,4
250	20	122	330	37.5	57.5	456.2
300	24	146.4	396	45	69	552.3

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Conclusion and Future Work

This research focuses on location privacy of MSN users while enjoying location based services for example finding restaurants, hospitals, schools and many more. The research proposed an scheme using ECC cryptographic system to ensure location privacy. In first phase, the algorithm has been designed that includes series of steps using ECC encryption and decryption mechanism. The other phase of this work include implementation, in which Java has been used to calculate the computational and communication cost of proposed approach. The algorithm has been run to calculate the time consumption of users up to 500 while enjoying services. In the end of this research, comparison with other approaches also included to show the effectiveness of proposed scheme.

In the future, this framework could be expanded by incorporating various ECC Key Sizes to minimize signature generation and verification costs for users. Moreover, the scheme can be enhanced so that users can use services without billboards.

References

[1] C. Rechberger and R. Walch, "Privacy-preserving machine learning using cryptography," in *Security and Artificial Intelligence*, Cham: Springer International Publishing, 2022, pp. 109–129.

[2] F. Li, S. Wan, B. Niu, H. Li, and Y. He, "Time obfuscation-based privacy-preserving scheme for Location-Based Services," in *2016 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2016, pp. 465–470.

[3] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, 2018.

[4] S. Ji, P. Mittal, and R. Beyah, "Graph data anonymization, DE-anonymization attacks, and DE-anonymizability quantification: A survey," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 2, pp. 1305–1326, Secondquarter 2017.

[5] Hussain, M., Alvi, F.A. and Rajput, U., 2023. Comparative Analysis of Privacy

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Preserving Location Based Services Mechanisms.

[6] M. B. Rajashekar and S. M. Sundaram, "A survey on user's location detail privacy-preserving models," *SN Comput. Sci.*, vol. 1, no. 3, 2020.

[7] Peng, T., Liu, J., Wang, G., Liu, Q., Chen, J. and Zhu, J., 2020. A user-defined location-sharing scheme with efficiency and privacy in mobile social networks. *Scientific Programming*, *2020*, pp.1-13.

[8] Wu, L., Zhao, S., Wei, X. and Meng, L., 2023. Privacy- preserving and efficient user matching based on attribute encryption in mobile social networks. *International Journal of Network Management*, *33*(3), p.e2192.

[9] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," ACM Comput. Surv., vol. 54, no. 1, pp. 1–36, 2022.

[10] Safi, S.M., Movaghar, A. and Ghorbani, M., 2022. Privacy protection scheme for mobile social network. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), pp.4062-4074.

[11] Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z. and Iyengar, A., 2021. Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys (CSUR)*, *54*(1), pp.1-36.

[12] A. Bashanfar, E. Al-Zahrani, M. Alutebei, W. Aljagthami, and S. Alshehri, "A survey on location privacy-preserving mechanisms in mobile crowdsourcing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 7, 2019.

[13] Nuanmeesri, S., 2023. Mobile application for the purpose of marketing, product distribution and location-based logistics for elderly farmers. *Applied Computing and Informatics*, *19*(1/2), pp.2-21.

[14] B. Zhu, S. Zhu, X. Liu, Y. Zhong, and H. Wu, "A novel location privacy preserving scheme for spatial crowdsourcing," in *2016 6th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, 2016, pp. 34–37.

[15] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors (Basel)*, vol.

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

18, no. 11, p. 3894, 2018.

[16] K. Yang, K. Zhang, J. Ren, and X. Shen, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 75–81, 2015.

[17] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Comput. Netw.*, vol. 135, pp. 32–43, 2018.

[18] Ni, L., Tian, F., Ni, Q., Yan, Y. and Zhang, J., 2019. An anonymous entropy-based location privacy protection scheme in mobile social networks. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), pp.1-19.

[19] A. Alamer, J. Ni, X. Lin, and X. Shen, "Location privacy-aware task recommendation for spatial crowdsourcing," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, 2017, pp. 1–6.

[20] J. Li *et al.*, "Drive2friends: Inferring social relationships from individual vehicle mobility data," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5116–5127, 2020.

[21] L. Zheng, H. Yue, Z. Li, X. Pan, M. Wu, and F. Yang, "K-anonymity location privacy algorithm based on clustering," *IEEE Access*, vol. 6, pp. 28328–28338, 2018.

[22] P. Jagwani and S. Kaushik, "Privacy in location based services: Protection strategies, attack models and open challenges," in *Information Science and Applications 2017*, Singapore: Springer Singapore, 2017, pp. 12–21.

[23] Zhang, S., Wang, G., Bhuiyan, M.Z.A. and Liu, Q., 2018. A dual privacy preserving scheme in continuous location-based services. *IEEE Internet of Things Journal*, *5*(5), pp.4191-4200.

[24] Holland Zahner, D.G., 2023. Navigating STEM major and transfer destination choices: community college student experiences through the lens of practice theory. *Community CollegeReview*, p.00915521231182119.

[25] R. Al-ani, B. Zhou, Q. Shi, and A. Sagheer, "A survey on secure safety applications in VANET," in *2018 IEEE 20th International Conference on High*

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2018, pp. 1485–1490.

[26] Y. Qiu, Y. Liu, X. Li, and J. Chen, "A novel location privacy-preserving approach based on blockchain," *Sensors (Basel)*, vol. 20, no. 12, p. 3519, 2020.

[27] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, 2021.

[28] X. Wang, Y. Xing, Y. Wei, Q. Zheng, and G. Xing, "Public opinion information dissemination in mobile social networks – taking Sina Weibo as an example," *Inf. Discov. Deliv.*, vol. 48, no. 4, pp. 213–224, 2020.

[29] M. K. Tefera, X. Yang, and Q. T. Sun, "A survey of system architectures, privacy preservation, and main research challenges on location-based services," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 6, pp. 3199–3218, 2019.

[30] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux, "Hiding in the mobile crowd: LocationPrivacy through collaboration," IEEE Trans. Dependable Secure Comput., vol. 11, no. 3, pp. 266–279, 2014.

[31] B. Liu, L. Chen, X. Zhu, Y. Zhang, C. Zhang, and W. Qiu, Protecting location privacy in spatial crowdsourcing using encrypted data. 2017.

[32] Vahdati, Z., Yasin, S., Ghasempour, A. and Salehi, M., 2019. Comparison of ECC and RSA algorithms in IoT devices. Journal of Theoretical and Applied Information Technology, 97(16).

[33] Toradmalle, D., Singh, R., Shastri, H., Naik, N. and Panchidi, V., 2018, August. Prominence of ECDSA over RSA digital signature algorithm. In 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on (pp. 253-257). IEEE.

[34] Lalem, F., Laouid, A., Kara, M., Al-Khalidi, M. and Eleyan, A., 2023. A Novel Digital Signature Scheme for Advanced Asymmetric Encryption

Online ISSN 3007-3197
Print ISSN 3007-3189

Techniques. Applied Sciences, 13(8), p.5172.

[35] Banupriya, S., Kottursamy, K. and Bashir, A.K., 2021. Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain. Peer-to-Peer Networking and Applications, 14, pp.2813-2825.

[36] Bhatia, M.K., Rajpurohit, R.S. and Gulafshan, B.J., A Study of Cryptographic Algorithms.

[37] https://en.wikipedia.org/wiki/Discrete_logarithm#Algorithms