# PRIVACY PRESERVATION IN SPATIAL CROWDSOURCING

Ms.N.Gayathriy, Assistant professor, Coimbatore Institute of Technology

Jasmine.J, Bindhu S, Haripriya S, Karthikeyan P L

Coimbatore Institute of Technology, Coimbatore, Tamilnadu

**Abstract--- Spatial crowdsourcing (SC) is a platform that engages a set of workers and requesters to complete specific tasks within a particular period of time. With the help of spatial crowdsourcing, the requesters can outsource their tasks to a set of workers, who will complete the tasks by travelling to the specified locations or from their current location itself. The SC server is responsible for task allocation of the workers. Both the worker and the requester are demanded to reveal their sensitive details to the SC server. The SC server fails to provide security on privacy of the workers and the requesters. The personal information may be tracked further by the SC server and the details maybe misused. To overcome the issue, a framework is proposed which involves the usage of symmetric and asymmetric cryptographic techniques to secure the sensitive details so that the SC server will never know the details of the workers and the requesters.**

**Keywords:**

Spatial crowdsourcing, Double encryption, Sc-server, Cryptographic techniques.

## I.INTRODUCTION

Spatial crowdsourcing has emerged in the past few years with the advancement of mobile computing, software functionality and security features. Many location based tasks are harder to complete as the requesters have to travel to the location every time to request for a task to be completed. But, with the help of spatial crowd sourcing platform, the requesters can request for the completion of their tasks from their location itself. The requesters can outsource their tasks to a set of workers. The SC-sever is responsible for task allocation of the worker. The SC-server can assign the workers based on the performance criteria, or based on the distance between the requesters and workers. Both the requesters and workers are demanded to reveal their true credentials to the SC-server. The SC-server might misuse the details of the workers and requesters. For example, with the leakage of information, an adversary may invoke a broad spectrum of attacks such as physical stalking, identity theft, and breach of sensitive information [1]. This will cause a major threat to the privacy of the users.

The issue about the privacy of workers and requesters have been extensively studied in the following literature survey. An approach was made by proposing a third party server (Privacy Service Provider server) [2]. The PSP server can assign tasks to workers who are at a minimum distance from the requester. Even though the location details are secured, there is no assurance for securing the personal details of workers and requesters. Some existing works adopt novel cryptographic techniques called Private Information Retrieval (PIR)[3] to protect workers' privacy. To provide location-based anonymous services, previous works develop a novel algorithm based on the spatial and temporal protection. Literatures [4],[5],[6] does a further improvement in security of their proposed model, they developed an emerging mechanism of peer-to-peer anonymization. To approach the inefficiency of homomorphic encryption, SKD-trees were used to index encrypted worker details. [7]

The work in [8] proposed a solution for anonymous credentials. The protocol has a registration phase in which a user chooses a secret and the server "blindly" signs it using a two-party protocol. During a time period t, a user can then log in to the server using his acquired signature and the server cannot distinguish which user logged in, nor link a user's login to any past logins. However, if a user attempts to login twice with the same credentials during the same time period, the user will be detected and denied access

Aforementioned schemes about privacy of personal details are not applicable to the SC due to the complex application scenarios in SC.

## II. BACKGROUND

Cryptographic algorithms are most frequently used in various domains for privacy preservation. One such method to perform calculations on encrypted information is Homomorphic Encryption(HE). The

function of cryptography is to protect the sensitive information from being disclosed when performing computations on encrypted data. The two broad classifications of cryptograph are symmetric key and asymmetric key cryptography. Based on how they are applied on the plaintext, cryptographic algorithms are categorized into two types: Block ciphers , Stream ciphers.

**Block Ciphers**

Block ciphers work on a fixed-length segment of plaintext data, a 64- or 128-bit block as input, and outputs as a fixed length ciphertext. The message is broken into blocks, and each block is encrypted through a substitution process. Where there is insufficient data to fill a block, the blank space will be padded prior to encryption.
Block ciphers are mostly used in symmetric key encryption. DES, Triple DES, and AES are based on the block ciphers.

**Stream Ciphers**

Stream cipher is applied to single bits of data. A cryptographic key is used to generate a pseudo-random stream of digits that are combined with the plaintext digits to create the cipher text. One-time padding are used to generate a completely random stream of digits for use in the encryption stage.

Keystream is a sequence of (pseudo) random digits used in enciphering plaintext and needs to be of the same length as the plaintext message. The keystream is typically XOR with the plaintext using a bitwise operation on individual bits.

Stream ciphers provide faster encryption and decryption than block ciphers, and is used in both symmetric and asymmetric key cryptosystems.

Cryptographic algorithms are used to guarantee the integrity of exchanges. These are known as cryptographic hash functions.
For every message, a hash value of a fixed length with a certain number of properties is created by these functions. These are “one-way” functions: it is virtually impossible to recreate the input data from the hash alone. Even for slight modification in the message, good hash function will produce a hash very different from that of the original message, and the new hash cannot be predicted based on the modification. Finally, a good hash function should also be resistant to collusions.

## III LEARNING METHODS

### A. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) is symmetric encryption algorithm. It is comparatively faster than DES. As key size of DES is small, DES has to be replaced. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

ENCRYPTION PROCESS

AES encryption has four sub-processes.

- Byte Substitution
- Shift rows
- Mix Columns
- Add Round Key

DECRYPTION PROCESS

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order .

### B. RIVEST-SHAMIR-ADLEMAN

**RSA (Rivest–Shamir–Adleman)** is an asymmetric cryptographic algorithm. Two different keys are used for asymmetric algorithms.This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private.

The features of RSA algorithm are

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

### C. ELLIPTIC CURVE DIFFIE-HELLMAN KEY EXCHANGE

ECDH (Elliptic Curve Diffie–Hellman Key Exchange) is anonymous key agreement scheme, which allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel. ECDH is similar to that of classical DHKE (Diffie–Hellman Key Exchange) algorithm, but it uses ECC point multiplication instead of modular exponentiations.

### D. SHA-256

Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed for securing data. It works by transforming the data using a hash function: an algorithm that consists of bitwise and modular additions, and compression functions. The hash function then produces a fixed-size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. Other algorithms are 2SHA-1, SHA-2, and SHA-3. The above are designed with increasingly stronger encryption in response to hacker attacks

## III. PROPOSED ARCHITECTURE

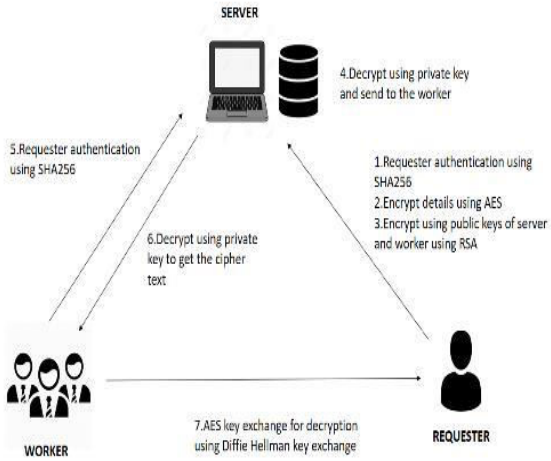


Figure1:SC Architecture

In the proposed model, both the workers and requesters are requested to register their details for authentication purposes. This is done securely using the SHA-256 algorithm. The SHA -256 algorithm ensures one-way encryption so that the password cannot be decrypted and is stored securely in the SC-server. This ensures authenticity. The requester can login safely and request for the task to be completed by providing the personal details and information about the task to be completed. A unique ID is generated for each requester and worker using PRNG (Pseudo Random Number Generator). Except the requester id, other sensitive details are encrypted using the AES algorithm. This ensures confidentiality.

The worker after successfully logging in, generates a pair of keys (w_pub and w_priv) using the RSA key generation algorithm. The pubic key of the worker is then successfully sent to the requester through the SC –server. The requester further encrypts the AES encrypted details along with the id of the requester using the worker's public key. Similarly, the server also generates a pair of keys (serv_pub and serv_priv) using the RSA key generation algorithm and sends it to the requester. A worker id is also generated at the requester side using PRNG. The requester encrypts the details encrypted using w_pub again with serv_pub including the worker's id. This double encryption ensures integrity

After performing double encryption, the encrypted details are sent to the server. The server first decrypts the details using its private key (serv_priv). Only the worker's id will be visible to the server. With this, the server knows which worker to allocate and sends the details to that worker. The worker again decrypts using the private key (w_priv). After decryption, the requester's id will be visible to the worker. Further, the worker will request for the AES decryption key from the corresponding requester with the help of requester's id. The AES decryption key is then shared between the requester and worker with the help of diffie hellman elliptic curve key exchange algorithm. The requester can be verified by using hash functions. Using this model, data can be securely shared between the worker and requester without revealing the information to the SC-server.

## IV. CONCLUSION

In this paper, we have proposed a model which can be used to securely share details between the workers and the requesters without revealing the details to the SC-server. The sensitive details thus cannot be breached. In our future work, the selection of a particular worker based on various criteria such as reviews, distance, skills etc. is to be done. This will make sure that the requester finds the suitable worker so that the task specified can be done easily and quickly.

## References

[1] L. Pournajaf, L. Xiong, V. S. Sunderam, and S. Goryczka. Spatial Task Assignment for Crowd Sensing with Cloaked Locations. In MDM, pages 73–82, 2014

[3] Ghinita G, Kalnis P, Khoshgozaran A, et al. Private queries in location based services: anonymizers are not necessary. In: Proceedings of the ACM SIGMOD international conference on management of data, Vancouver, BC, Canada, 9–12 June 2008, pp.121–132. New York: ACM.

[4] Chow CY, Mokbel MF and Liu X. Spatial cloaking for anonymous location-based services in mobile peer-topeer environments. Geoinformatica 2011; 15(2): 351–380.

[5]. Ghinita G, Kalnis P and Skiadopoulos S. Mobihide: a mobilea peer-to-peer system for anonymous locationbased queries. In: Papadias D, Zhang D and Kollios G (eds) Advances in spatial and temporal databases. Berlin: Springer, 2007, pp.221–238.

[6]. Chow CY, Mokbel MF and Liu X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proceedings of the 14th annual ACM international symposium on advances in geographic information systems, Arlington, VA, 10–11 November 2006, pp.171–178. New York: ACM.

[7] Hang Xe,kai Han,Charting Xu,Jingxim Xu and Fei Gui,"Towards location privacy protection in spatial crowd sourcing",(Privacy preservation for large scale Internet of Things – Research Article) 19 Dec 2018.

[8] Jacques Bar Abdo , Thomas Bour Geau,Jacques Demorjian and Hakina Chaouchi , "Extended Privacy in crowdsouring location-Based services using mobile cloud computing ", http://dx.doi.org/10.115/2016/7867206, 2016.

[9] Monica Da silva, Jose viterbo bernardini, Cristiano Maciel ,"Identifying privacy Functional Requiements for Crowdsourcing Applications in smart cities, IEEE ,2018.

[10] Bozhong liu, Lingchen,Xingquan Zhu , Ying Zhang,Chengqi Zhang,Weidong Qui, "Protecting Location Privacy in Spatial Crowdsourcing using Encrypted data ", https://www.yelp.com/dataset_challenge, https://snap.stanford.edu/data/loc-gowalla.html,2005.

[11] Yanmin Gong,Yuanxiong Guo and Yuguang Fanq ,"A Privacy-Preserving Task Recommendation Framework for Mobile Crowdsourcing ",IEEE ,2014.

[12] Abdurahman Alamer , jianbing Ni,Xiaodong Lin,and Xuemin (Sherman) Shen,"Location Privacy-Aware Task Recommendation for Spatial Crowdsourcing ", IEEE, 2014.

[13] Hien To,Gabriel Ghinita,Cyrus Shahabi,"A Framework for Protecting Worker Location Privacy in Spatial Crowdsourcing" ,IEEE,2014.

[14] Yingjie Wang,Zhipeng Cai,Xiangrong Tong,Yang Gao,Guisheng Yin,"Truthful incentive mechanism with location privacy preserving mobile crowdSourcing systems",13 feb 2018.