Design and Implementation of Secure Location Service Using Software Engineering Approach in the Age of Industry 4.0

Sumaiah Tabassum[1], Adarsh Kumar[2], Kamalpreet Kaur[3], Priyansh Arora[4], Deepraj Chowdhury[5], Sanjay Misra[6], and Sukhpal Singh Gill[1](✉)

[1] School of Electronic Engineering and Computer Science, Queen Mary University of London, Mile End, London E14NS, UK
sumaiah@se19.qmul.ac.uk, s.s.gill@qmul.ac.uk

[2] Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India
adarsh.kumar@ddn.upes.ac.in

[3] Seneca International Academy, Seneca, Toronto, Canada

[4] Microsoft, Hyderabad, India
priyansh.arora@microsoft.com

[5] Department of Electronics and Communication Engineering, International Institute of Information Technology, Naya Raipur, Chattisgarh, India
deepraj19101@iiitnr.edu.in

[6] Department of Computer Science and Communication, Østfold University College, Halden, Norway
sanjay.misra@hiof.no

Abstract. Data privacy and security are major concerns in any location-based system. In majority of location-based systems, data security is ensured via data replacement policies. Data replacement or hiding policy requires additional measures for providing required security standards for Industry 4.0. Whereas, cryptography primitives and protocols are integral part of any network and can be re-used for ensuring user's locations in Industry 4.0 based applications. In this work, an application has been designed and developed that used RSA encryption/decryption algorithm for ensuring location data's confidentiality. The proposed system is distributed in nature and gives access to location's information after users get authenticated and authorized. In the proposed system, a threshold-based subset mechanism is adopted for keys and their storage. Server is designed to securely store the location information for clients and provide this information to those set of clients or users who are able to verify sum of subset of keys. This work has elaborated the location-based data confidentiality designs in a distributed client/server environment and presented the in-depth system working with different flow diagrams. The command line and graphical User Interface (GUI)-based implementation shows that the proposed system is capable of working with standard system requirements (i5 processor, 4 GB RAM and 64-bits operating system). In addition to location information, system is able to provide much important information (including IP address, timestamp, time to access, hop count) that enhances the overall system capabilities.

L. Garg et al. (Eds.): ISMS 2021, LNNS 521, pp. 397–418, 2023.
https://doi.org/10.1007/978-3-031-13150-9_32

Keywords: Encryption · Decryption · Latitude · Longitude · Location service · Security · RSA algorithm · Industry 4.0

1 Introduction

Location-based services are found to be rapidly evolving in various real-time applications [1]. The location-based services are integrated with application after small to large scale testing by different research groups [2]. Location-based services integrated with communication devices provides various capabilities including location tracking over Google Maps, queries execution subsystem, individual's sensitive information fetching and sharing, privacy concerns etc. [3]. These capabilities are useful if the system uses no-replacement mechanisms for providing/sharing location-based information. In replacement mechanisms, real-user data replaced with fake one and it is processed through location-dependent queries. In location-based queries, source querying location identities cannot be efficiently executed if replacement policy is followed. Thus, other data security and privacy policies need to be discussed and presented.

1.1 Motivation and Our Contributions

In existing location-based system [1–4], there are many shortcomings like (i) the replacement-based data hiding system is easy to break. This can lead to easy attack over user data. As users keep on changing the locations and data is updated regularly, the chances of tracking user's movement is much easier, (ii) similar processes of data hiding are applied to complete data. In this process, a disgruntled person can easily compromise the whole data if data security and privacy are not ensured properly. The disgruntled user can collude the stored data with unknown or fake data such that the complete data become meaningless. (iii) it is easy to find the source of location provider. Thus, any user which practices such processes in the complete execution can identify such activities easily [4]. Specifically to location-based systems or services, the various challenges in existing systems are briefly explained as follows.

- The majority of existing location-based system uses data hiding (with data replacement) policy for security. Such practices can lead to many attacks easily. Thus, they are not useful in real-time applications.
- The existing location-based system is easily prone to attacks because it is easy to manipulate data using high computational devices. Thus, formal system and software practices are required that enhances the location-based services capabilities and shows better results for real-time applications.
- Increasing the system complexity to achieve data security using cryptographic primitives need to be analysed for better performances. Thus, trade-offs between security, performance complexities and security levels are important to discuss, study and experiment.

In this work, software engineering-based methodologies are discussed to design and develop location-based system. In this system, 5 P's and their importance are discussed

for location-based system [1]. The location-based system and services are required to derive and develop many real-time applications [2]. This work has discussed the location-based system project charter with detailed project plan. This plan is useful to achieve real-time application within specific, measurable, achievable, realistic and timely development process. Here, cost estimation is also performed to show the importance of discussed project charter and project plan. Thereafter, software project requirements are discussed to develop location-based secure data management system using cryptography primitives. Next, the feasibility analysis is performed that discusses economic and technical system feasibilities. In continuation, a software architecture is proposed that helps in developing location-based services for various applications. In this work, the discussed architecture explores the communication process that can help in inter-process communication for integrating location-based services. In the proposed distributed location-based system, sum of subset algorithm is used for integrating location services. These location services are useful in providing data access to authentication user only. The sum of subset approach is enhanced with encryption/decryption process using RSA algorithm [5]. To manage the distributed system, a server/client environment is suggested that helps in measuring the system performances and increases the chances of location-based system adaptability in applications. This work presents the system design as well. In the system design, system flow is explained using use-case, activity and sequence diagrams. Finally, implementation details are discussed that uses encryption/decryption processes for handling distributed architecture. The implementation section shows the system outcomes as well.

This work is organised as follows. Thereafter, Sect. 2 discusses related work, Sect. 3 focuses over system methodology. Here, software engineering practices are explored for detailed study and system development. These software engineering practices explains the project plan that can act as an example for overall system development that would be useful for any system integrating location-based services. Section 4 shows the economic and technical feasibility analysis. Section 5 explains the proposed architecture incorporating communication processes, proposed algorithm for location-based information gathering, encryption/decryption processes using RSA algorithm and distributed client/server environment. Section 6 explains the system design and flow. Section 7 presented the system integration and testing processes executed to test the system functionality. Section 8 shows the system execution. Finally, conclusion is drawn in Sect. 9.

2 Related Work

This section discusses the existing works of location-based services. Nosouhi et al. [17] identified the problem of dishonest user's fake location and provide location proof-based concept in the proposed approach. The proposed approach has concentrated over increasing the security and privacy concerns that includes prover-prover collusions with special concentration to reduce location privacy threats. Authors used Blockchain technology and proposed distributed and decentralized scheme for location proof generation and verification. Here, every prover need to broadcast its location to neighboring devices which in-turn uses peer-to-peer network for better short-range communication interface-based

location sharing system. In experimentation, it has been observed that performance of the proposed approach is reliable with Prover-Prover and Prover-Witness based approach. In comparative analysis, it has been observed that the proposed approach outperforms the currently deployed proof-based scheme. The implementation is performed using Android-based platform and results show that performance is an important parameter to say that the proposed approach is comparatively better. Thus, the proposed blockchain-based architecture is capable of establishing dynamic trust and integrating score-based approach for enhancing location-based precise identification scheme. In conclusion, the proposed architecture and implementation-based solution is an effective approach to enlarge it at a large scale for realistic observations.

Tang et al. [18] concentrated over improving the healthcare services using system enabled with fog and cloud computing services. Here, location-based services play an important role in medicine, patient identification and location other healthcare services. Location-based services are useful in various healthcare's subsystems including emergence healthcare services, healthcare (medical or personal) notifications, healthcare supply chain and other subsystems. Location-based services are critical system of healthcare services. If such healthcare system can be fully implemented and followed properly with its full advantages then real advantages can be realized. For example, patient's data, its secure storage and retrieval, and sharing are important parts of any health working system. Here, location-based service can collect the required data timely and process for desired statistics and outcomes.

Tian et al. [19] discusses the characteristics of location-based services. In these characteristics, importance is given to location privacy features that may cause potential threats to different applications. Thus, security and privacy aspects are important to discuss and evaluate for application-based scenarios. Authors proposes a location privacy preserving system using cloud-of things that hides user's trajectory privacy. Here, user's moving behaviours is analysed using Markov chain that interconnects the activities. In this way, it would be much easier to identify the set of activities and provide the useful data. A cloud-based fast real data hiding and display different statistics-based system is useful in many terms including ensuring security concerns, fast data processing, statistics generation and easy to understand visualization. In experimental results, it has been found that performance can be measured in terms of moving steps, cloaking threshold score and anonymity value measures. Thus, the system is effective and efficient to tackle fast location-hiding options to various applications. This recent work gives an indication of importance of location-based system to latest applications in different sectors.

Alam et al. [20] explored the importance of IoT-based location detection services for interaction and communication in 5G technologies. The centralized approach with neighbouring devices network construction and connectivity architecture is designed and experimented to share knowledge-based data with several nodes. The integration of cloud and MANET structure creates an efficient and secure approach for data communication in Cloud, MANET and IoT integrated framework. IoT-based location detection and dynamic connection establishment and data transfer features make the proposed architecture unique and efficient to be integrated in different realistic applications.

Ratajczak et al. [21] proposed integration of location-based system with building and construction industry. The aim of this integration is to improve the overall industry

performances as this industry lacks in meeting the deadlines and costs overruns. Thus, location-based system with specified key indicators are useful in meeting customer requirements. Further, system is extended with augmented reality-based system to have a walkthrough that is need to develop an application-based scenario. The complete scenario is simulated in a laboratory-based experimentation. Results show that the proposed system/solution is very effective. A feedback-based approach confirm this as well. In conclusion, the proposed system is recommended based upon semi-realistic scenario construction and outcome observations. The proposed system does not addresses the data security and privacy. The location-based data is having its own importance. This importance reduces if data is made available at no cost. Thus, there is a need to extend the proposed application-based system with security concerns.

Reddy et al. [22] discussed the importance of location-based services in Internet of Things (IoT) with short range wireless technologies including Bluetooth, Wi-Fi, ZigBee, and Global System for Mobile Communications (GSM). Integration of short range wireless technology and location-based GSM system helps in identifying various locations which in-turn is found to be helpful in control and operation of devices along with user interfaces. In this work, it has been observed that context-aware application relies over principles of context-awareness, modelling and reasoning. Various other features that includes context application facts include architecture style, abstraction, fault tolerance capabilities, uniquely identifiable services, privacy, security, data analysis etc. In the proposed system, security, privacy and open research challenges are integrated with location-based services which in-turn improves the overall system capabilities. Thus, an application-based scenario is available to study the importance of location-based services and possibilities of its integration with other systems.

Schmidtke et al. [23] discussed the importance of deploying location-based services for COVID-19-pandemic situation. In this survey, the location-aware application primarily focused over Big data construction, geospatial data analysis, visualization, data related to spreading of disease and state of other emergency services. Data privacy related to people's real location are major concern in any location-aware systems. Thus, those solutions are discussed that motivates users to share their private and comprehensive data for analysis and other benefits. The web-based variations of data collection, analysis and processing to other systems for spatial analysis and service providing are two privacy preserving COVID-19 usage. The conducted survey has gone through the pros and cons of this system. In a major finding, it has been observed that the key steps in developing privacy preserving COVID-19 contact tracking application and taking maximum usage of it are challenging but in-demand application especially during COVID-19 times. In literature, many such solutions are derived. Table 1 shows the comparative state-of-the-art work analysis for recently developed location-based system. This comparative analysis also shows the pros and cons of the techniques taken for comparative analysis.

Critical Analysis: In literature, various lightweight and traditional cryptographic primitives are discussed for different applications. These cryptographic primitives can be used for resourceful and resource constraint environments. The performance of these primitives varies from system to system under different configurations. Location-based services can be implemented over both resourceful and resource-constraint environments [24]. The major challenge in integrating location-based system with existing

Table 1. Comparative state-of-the work analysis for recently developed and/or discussed location-based systems.

Author	Year	A	B	C	D	Pros	Cons
Nosouhi et al. [17]	2020	Y	Y	Y	I	Used blockchain technology for verification Proposed trust and incentive-based	All security dimensions are not considered for implementation User-interactive location-based service is required for better statistics
Tang et al. [18]	2019	Y	N	Y	T	Generalized cloud and fog computing-based proposal is made for healthcare system The location-based services can give more precision and importance to	Lack of software practices does not ensure that the developed system is capable to integrate unknown situations which may fails the critical system understanding
Tian et al. [19]	2019	Y	N	Y	I	In this work, cloud-based architecture is proposed that handle the user's movement and capabilities to ensure data sharing functionalities This work has proposed a replacement strategy for hiding the true user's location and maintain data security and privacy concerns	Lack of software practices does not ensure that the developed system is capable to integrate unknown situations which may fails the critical system understanding Security aspects from multi-dimensional viewpoint should be considered and validated to say that the proposed system is efficient in realistic applications

(*continued*)

Table 1. (*continued*)

Author	Year	A	B	C	D	Pros	Cons
Alam et al. [20]	2020	N	N	Y	I	Cloud, MANET and IoT-based framework is unique in providing quality services to data exchange and management The proposed framework provides various features using integrated technologies that are beneficial for flexible and advanced data management	Lack of software practices does not ensure that the developed system is capable to integrate unknown situations which may fails the critical system understanding Major focus is drawn towards network construction and data management rather other data related issues including data security
Ratajczak et al. [21]	2019	N	N	Y	I & S	This work proposed location-based system with augmented reality concept for construction and building The location-based system is useful in handling construction industry efficiently as observed from laboratory-based small scale implementation	Security issues need to be addressed especially data security aspects. The location-based data is important for experimentation and if data is revealed with no cost then importance of this data reduces Smart and sustainable infrastructure solution could be proposed for construction industry

(*continued*)

Table 1. (*continued*)

Author	Year	A	B	C	D	Pros	Cons
Reddy et al. [22]	2019	Y	N	Y	I	Focused over context-aware applications, architecture and services Location-based system is one part of the complete system. Thus, it helps in understanding the possibilities of location-based system integration with other	Security and privacy concerns are partially discussed. There is need to discuss multi-dimensional security aspects to protect the system from large set of attacks GSM-based location services have large set of existing applications. However, IoT-integrated applications require distributed location-based application. Thus, new solutions are required to incorporate the additional requirements
Schmidtke et al. [23]	2020	Y	N	Y	N	This work has surveyed location-based system in recent work A classification of location-based services with different short-range technologies can be explored	Detailed survey over security aspects in location-based system is required

A: security and privacy concerns, B: prover-prover collusions, C: location-based service (generation and verification), D: implementation (I)/simulation (S)/theoretical model (T), Y: yes, N: no

real-time applications include: (i) data privacy is a major concern in location-based data collection and sharing. Thus, it should be explored with different security dimensions, (ii) location-based system need system specific solutions for integration and enhancing existing application capabilities, (iii) system specific location-based attributes are important to study and relate before designing and implement it in real-time applications, (iv) location-aware data storage is necessary to study because large user's network

can generate large amount of data which require analysis accordingly, and (v) location-based services are providing advantage in many futuristic applications. Thus, the scope of location-aware data, its location and importance to other need careful considerations.

3 Methodology

In the overall system, software engineering methodologies and practices are followed to learn and analyse the progress. This section discusses methodology and more details are presented as follows:

3.1 The 5 P'S

The success of a project depends on management whether we manage it properly or not. Through the original methodology, we have prepared our own methodology [5].

- *Process:* Agile development life cycle is the base of our project. This method is opted because functional requirements of this project are explicitly stated rather than dynamic ones. Besides, more time is allowed to work on programming to assure the quality of the product.
- *Project:* Completion of project took 7 months. One of the prominent goals is to create desktop application in which one's location can be automatically retrieved that coordinate through secured channel accessed by authorized personnel.
- *Product:* It includes a mobile or web based application or web service and a manual to explain the development of this product step-wise.
- *People:* It includes the target audience such as learning institutions or common people. Adarsh Kumar, Kamalpreet Kaur and Priyansh Arora (Co-authors) are stakeholders of this project.
- *Problem:* There are many security concerns due to leakage of location information through various applications.

3.2 Project Charter

Project charter contains the following components [6]:

- **Expectations of the Customer:**
  To develop a web-based application for providing security about the user's location (user gives prior permission to share information of location)
- **Project Scope:**
  To use RSA algorithm for encryption of user's location and issue an access to certified user.
- **Analysis Technique for Interaction:**
  To implement this project after analysis of data.
- **List of Stakeholders:**
  The main stakeholders are Adarsh Kumar, Kamalpreet Kaur and Priyansh Arora (Co-authors).

- **Deliverables of Project:**
  Functional requirements are the project outcomes.
- **Evaluation Procedure of Project:**
  To run various tests to evaluate the working of project in to check whether this project is performing encryption and decryption of user location contains longitude and latitude value.
- **Projected Timeline:**
  This project has been completed in 8 months, which has been estimated using Program Evaluation and Review Technique (PERT) method.
- **User Training:**
  There is no need of user training, because it is real-time system.
- **System Maintenance:**
  This project is developed in such a way, which can be self-maintained easily. If there is a need to maintain manually, then it could be easily done without making an impact of stored data.

3.3 Project Plan

S.M.A.R.T Analysis: "SPecific, Measurable, Achievable, Realistic and Timely"
To develop a technique which is able to perform the encryption and decryption without any interference, can be completed in 7 months (99% possibility) [7]. We can create a working prototype of the proposed idea within 3 months to demonstrate its working. Table 2 show the work breakdown structure of project and length of various activities is estimated using PERT chart.

Cost Estimation/Budget
No costs for devices or system installation because whole equipment is typically owned. The development of the system will use free software that includes Qt which is also free of expenses. Most of the time would be consumed by programming and testing. Research will be on track just after the development of the software, which spends less time than expected. Programming will consume lot of time due to development based on agile model. Moreover, it is more appropriate for smaller projects with less challenge.

3.4 Requirements Specification

Function Requirements:

- Web-based application as a functional prototype, which can secure the location using encryption and decryption and also forward this information using secure network.

Non-functional Requirements:

- *Reliability:* Location of the user must be existing.

Table 2. Project tasks and their dependencies

Task ID	Task name	Duration	Start	End	Predecessor
T1	Requirement gathering	64 h	1/02/2020	09/02/2020	NA
T2	e-portfolio training	78 h	11/02/2020	22/02/2020	NA
T3	Project definition	16 days	22/02/2020	13/03/2020	NA
T4	Draft preliminary software specifications	5 days	13/02/2020	18/02/2020	NA
T5	Add feedback on specifications of software	1 day	18/02/2020	18/02/2020	NA
T6	Create timeline for delivery	1 day	19/02/2020	19/02/2020	T5
T7	Review of existing similar projects	90 h	20/02/2020	04/03/2020	MA
T8	Create working prototype	1 day	05/03/2020	05/03/2020	T7
T9	Implementation	21 days	06/03/2020	2/04/2020	T8
T10	Developer testing	21 days	06/03/2020	02/04/2020	T8
T11	Deliverables	700 h	24/03/2020	31/07/2020	NA
T12	Draft documentation	20 days	5/07/2020	9/08/2020	NA
T13	Final documentation	4 days	11/08/2020	22/08/2020	NA
T14	Prepare manual	2 days	26/08/2020	27/08/2020	NA
T15	Demonstration	1 day	07/09/202020	07/09/2020	NA

- *Performance:* The response time of developed application will me minimum as possible.
- *Safety:* No tracing can be made during the deployment stage as the samples are anonymously presented.
- *Scalability:* Should be able to maintain itself inasmuch there is no use of any data.

Software Requirements:

- To implement this application, there is a need of 64-bit Ubuntu/Windows OS.
- Geocoder

Geocoder is process of translating an address into a coordinates (longitude & latitude).

- Python language for coding
- Pyuic for changing GUI to python code
- MySQL
- Python Qt Designer

Python Qt designer designs a Graphical User Interface (GUI) for web-based applications for deployment. It is very easy to develop an application by downloading and installing it. Qt Creator Integrated Development Environment (IDE) tool [8] is available for the development of application. Moreover, the tasks such as building a project can be automated and other tasks such as actions refactoring, checking code syntax, offering semantic highlighting and writing code.

Hardware Requirements:

- 500 GB Storage
- 64-bit Architecture
- 8 GB Main Memory (RAM)
- Processor 2.16 GHz.

4 Feasibility Analysis

A feasibility study is applied for determining the possibility of a plan that includes certainty of a project whether it is legally and technically possible as well as economically acceptable or not. It informs us about the how worth the investment on the project [9]. A project may not be achievable because of plethora of reasons, such as necessitate numerous resources, which puts negative impact on these resources [11]. Consequently, the performance of other tasks get alleviated alongside might charge greater than an institute will receive back through taking on a project that isn't lucrative.

4.1 Economic Feasibility

This kind of feasibility contains a cost/benefit examination of this desktop application, supporting relations select the possibility, cost and other points associated with a task prior to the distribution of budgetary assets [10]. It upgrades the validity of project assisting users to choose the constructive financial benefits for the development of the project [12]. We have utilized open source software such as "PYUIC", "PYQT", "PYTHON" and "UBUNTU" to develop our application, which makes it economical.

4.2 Technical Feasibility

This kind of feasibility focuses on technical resources available to the institute. It provides the assistance in case of taking decisions if the particular resources meet maximum value. Technical attainability similarly comprises equipment assessment, programming, and other advanced basics of the anticipated structure. For verifying the technical feasibility, a working prototype of this application is developed [13]. The working of prototype shows that feasibility of this project technically.

5 Proposed Framework

This desktop-based application contains 4 different modules. *Command Prompt* is used to create client and server processes in this first module and then establish a connection between them. In the second module, client sends a message to server, which contains necessary input to create details of the location. In the third module, positional refinements are generated to finalize the process of encryption. In the fourth module, system provides access to the authorized users to encrypt and decrypt the message. For attaining parallelism in Python code, the threading module is used. Initially, thread class represents a process which is running in an isolated thread. The development will be decided by two ways: by rescinding run() method in the subclass or by passing a callable object to the constructor, it surpass the run() and __init__() methods for this class. Then, it calls start() method of thread to initiate the communication just after creating the thread. Moreover, it controls the thread by calling an alternate run() method. After the start of the development, thread's state considers as "alive" and further, it does not treated as "alive" once run() method stops its execution. The execution of run() method can be stopped naturally or by creating an unhandled exceptional case. If the string is "alive" then tests is alive() technique. Moreover, thread's join() method can be called by other threads. It will prevent to consider thread's join() method will finish execution.

5.1 Architecture

Figure 1 shows the process of generation of positional details and starts the communication and then apply encryption to the input utilizing the interface of a particular interface. The implementation of desktop application contains following modules:

1. Generating client and server process.
2. Use sum of subset algorithm to generate positional information.
3. Apply the encryption mechanism on details of the position.
4. Forwarding the encrypted and decrypted text to the user.

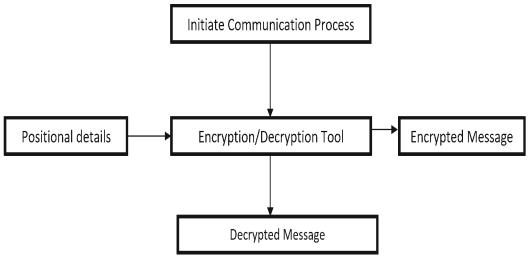

Fig. 1. System architecture of application

5.2 Start Communication Process

Command Prompt is used to create client and server processes in this first module and then establish a connection between them. Socket module provides an access to Berkeley Software Distribution (BSD) socket interface, which can be run on various platforms such as Windows, Mac or UNIX. Figure 2 shows a socket which is an anticipated representation for the one particular terminal of a network communication channel.

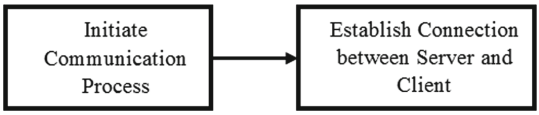

Fig. 2. Initiation of communication process

Initially, server starts the communication and then interacts with client process to verify the subset sum.

5.3 Using Sum of Subset Algorithm to Obtain Location Details

The process of using sum of subset algorithm [14] to obtain location details is shown in Fig. 3. This second module manages the transfer of message from client to server and contains the key information to make the positional refinements. In this scenario, two numbers M and n are used to define issue of Subset Sum (SS) i.e. SS (n, M). The Scenario of SS (n, M) is created by choosing a reliably irregular vector a $\in$ Z n M, a reliably arbitrary vector s $\in$ {0, 1} n, and producing with T = a · s mod M. The main motive of this process is to identify s using the value of T, a and n. The stability of infringement SS (n, M) is depends on the proportion between n and log M, i.e. normally indicated to as the depth of the happening of the whole subset. The Scenario, when n/log M is under 1/n or bigger than n/log2 n, the issue can be solved in polynomial time [15]. Moreover, there is no necessity of calculations which needs under 2ω(n) time when the depth is stable or uniform as little as O (1/log n). It is additionally realized that the subset aggregate issue can just get more earnestly as its thickness draws nearer to one [16]. We have developed a cryptosystem in this project and its security is relative to the stability

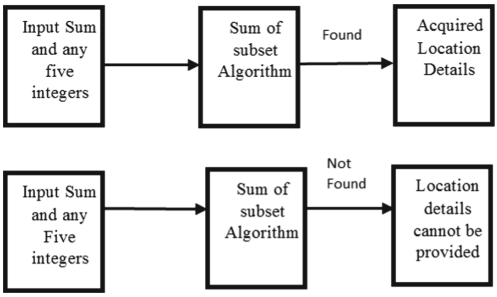

Fig. 3. Using sum of subset algorithm to obtain location details from server

of the SS (n, qn) issue, where q is a positive entire number of greatness Õ(n). Figure 3 shows the utilization of RSA algorithm for encryption of important information about the location of the user.

5.4 Encryption and Decryption of Positional Details Using RSA Algorithm

In this third module, positional details will be created to perform the process of an encryption is presented in Fig. 4. The encryption of details of the position will be performed only if client is able to offer the proper sum. The value of proper sum is required for the process of decrypt the details of position to the user. If client is not able to provide the proper sum then positional details will not be shared with client and marked client as an unauthorized user. Further, client shares its public key with the server as a sum of subset using RSA algorithm and appeals to share data. Next, public key will be used by server for encryption and shares the encrypted data with the client, who decrypts this data after receiving it. The shared data is asymmetric in nature and this data can be decrypted by the browser if third party contains the browser's public key. If required subset will be identified then position details will be encrypted with hexadecimal order of the ASCII values and share with the respective user.

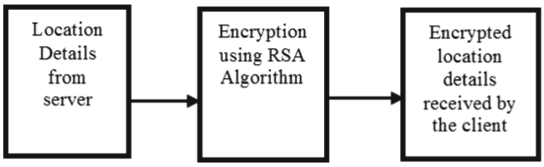

Fig. 4. Encryption and decryption process

5.5 Communication of Encrypted and Decrypted Positional Details to the Client

In this fourth module, server sends an encrypted/decrypted message to the user as presented in Fig. 5. When user shares the information about subset numbers then server starts interaction with user. If the given subset number does not satisfy the sum of subset algorithm then server denies to share positional details. Further, details of location address would be shared with user or server refuses to share encryption details with user. Server will respond with negative response "There is no subset with given sum, so location details (longitude and latitude) will not be shared" if client is not able to obtain a correct subset sum.

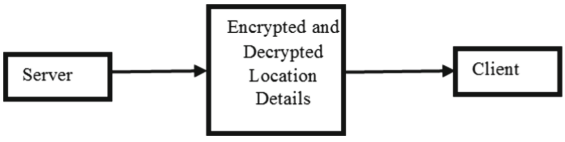

Fig. 5. Communication of location details to the client

Figure 6 shows the execution process to enter subset sum. Client will select 'n' to exit the loop and select 'y' to continue the execution process.

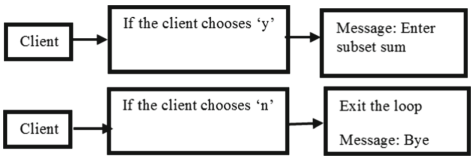

Fig. 6. Execution after acquiring the location details

6 Design Description

This section describes the design of the proposed work using three UML diagrams such as use case diagram, activity diagram and sequence diagram. Figure 7 shows a use case diagram to describe the interaction of user with the system. User initiates the communication processes and giving the input for the creation of positional description along with the information about the message to be encrypted. Further, server process performs the encryption and decryption of message. Figure 8 shows an activity diagram to start the communication process, where encryption/decryption happens and needed input for positional refinements age is specified. Otherwise, there is a need to restart the procedure. Figure 9 shows the sequence diagram to describe an interaction among client process, server process, decryption and encryption. First, client-server starts the communication using ports and give a feedback for the generation of positional details and further, message will be encrypted or decrypted.

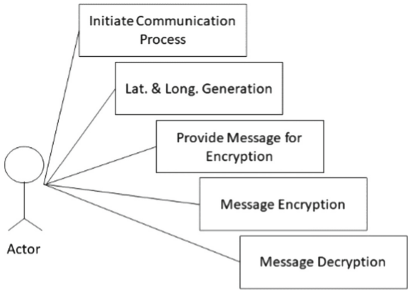

Fig. 7. Use case diagram

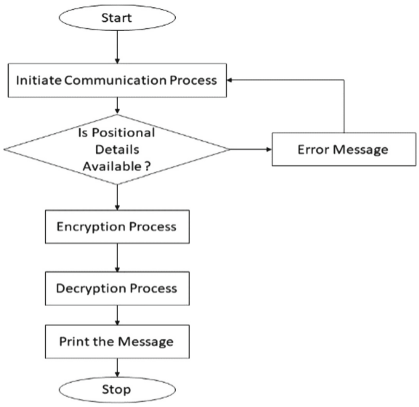

Fig. 8. Activity diagram

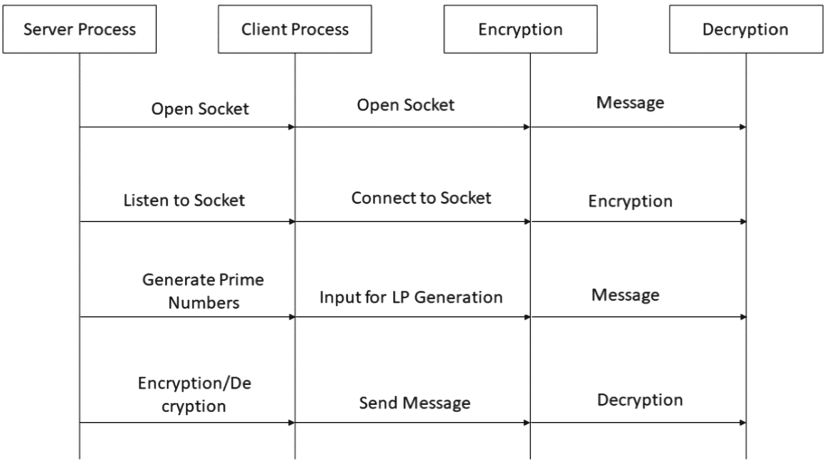

Fig. 9. Sequence diagram

7 Integration and Testing

This section describes the performance evaluation, where various different inputs are evaluated to identify the output after processing of set of operations. To start performance evaluation, encrypted location will be issued firstly. Further, programmer provides the destination address to port the server. The destination address can be edited if it is required in the server's module. Next, socket is ready to listen the request of client. Server shares that address after confirming the valid authentication. "Sum of subset problem" is considered to validate the client's authentication if client returns the required valid subset sum and numbers shadowed by colon (:). After verification of valid client, the location details will be provided by the server. After identification of correct subset sum, the server provides details of position and client process is able to check the decrypted and encrypted locations. Further, client can press *"Y"* to continue and can process *"N"*

to exit the process here. The location details will not be shared with client if the sum of subset is not verified correctly and server sends the reason of not sharing location as "given subset cannot be found with given sum".

8 Implementation Details and Results

The software and hardware requirements for this research are described in Sect. 3. This section discusses the implementation details and working of proposed technique. Figure 10 shows the screen that give the option to choose the processes. We have created two processes here:

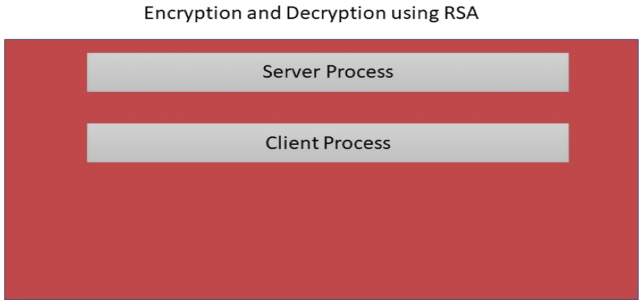

Fig. 10. Server/client process

- Server process is accessed by the person who has to share his/her location details.
- Client process is accessed by the person who wants to know someone's location details.

Figure 11 shows the window that opens when clicked on Server process. Port is opened and socket starts listening at this point.

Fig. 11. Selection of server process

Figure 12 shows the window that opens when clicked on Client process. Here in this window, sum and five numbers in the set should be given.

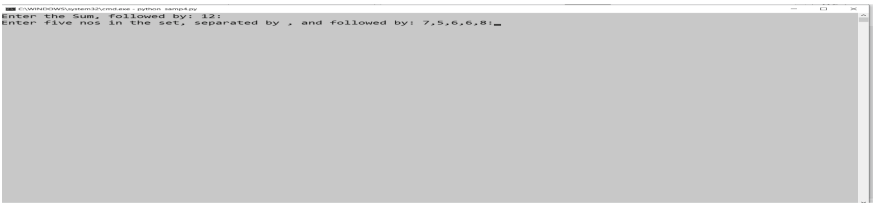

Fig. 12. Selection of client process

Fig. 13. An output of server process

Figure 13 shows the output of server process when the client has entered the sum and subset correctly. It discloses the location details (latitude, longitude) to the client as he/she is authorized.

Figure 14 shows the output on the client process window i.e. the location details are disclosed to him/her by the server.

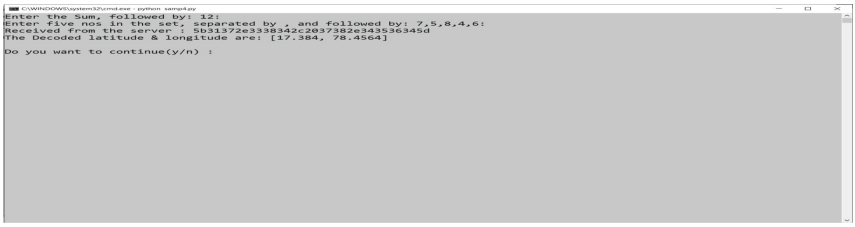

Fig. 14. An output of client process

Figure 15 shows the output where the client gives an unsatisfied sum and subset combination, which implies that the client is unauthorized.

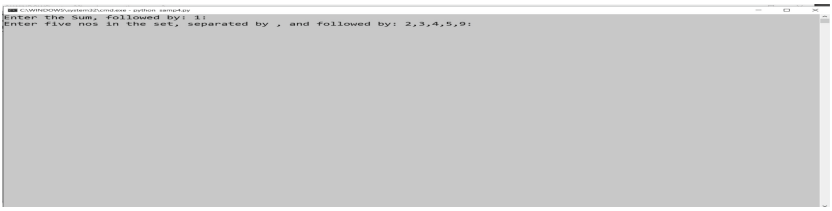

Fig. 15. Client is unauthorized

Figure 16 shows the output where the server recognizes the client to be unauthorized and does not disclose the location.

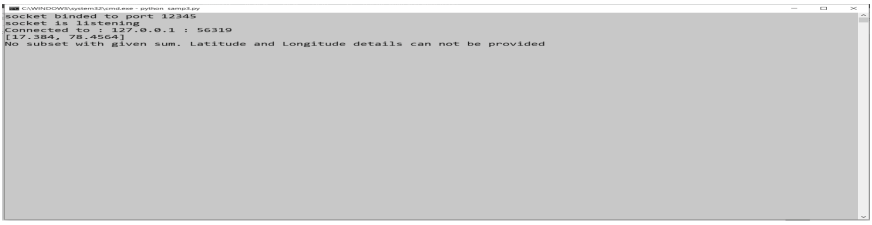

Fig. 16. Server recognizes the client to be unauthorized

9 Conclusions and Future Work

Location-aware system has advantages in various real-time applications. With these advantages, the scope of data collection, its availability for public usage and analysis for statistics are equally important to study and discuss. In traditional approach, data security uses data hiding approach for protection which in-turn uses data replacement with fake data. Such approaches are not much secure and easy to break with high computational device. Thus, there is a strong need to develop cryptographic primitives-based location-aware services that promises data security in all data stages (storage, processing and transmission). In this work, an application is developed for Industry 4.0 to enable encryption and decryption of location using RSA algorithm, which gives access to the location to only authorized users. This work has considered subset as a key and help to locate the correct location. The server keeps the details of the location in a confidential way, will be shared with only valid clients who verifies the sum of subset. The departments such as navy and army can use this application to transfer their message with high security. Further, Police personnel can also use this application for the decryption of messages of anti-social elements. Presently, this is a desktop based application, which can be extended for mobile devices in the future. Currently, this application is tested using single client and server but this application can be tested using multiple clients.

References

1. Vasilis, A., Havlena, M., Kiefer, P., Giannopoulos, I., Schindler, K., Raubal, M.: Gaze-Informed location-based services. Int. J. Geogr. Inf. Sci. **31**(9), 1770–1797 (2017)
2. Kachane, S., Feng, Y., Jayalath, D., Wang, C.: A New Location-Based Services Framework for Connected Vehicles Based on the Publish-Subscribe Communication Paradigm (2019)
3. Binh, T.N.: Location-based real-time casino data, U.S. Patent 9,626,826 (18 April 2017)
4. Chen, L., et al.: Robustness, security and privacy in location-based services for future IoT: a survey. IEEE Access **5**, 8956–8977 (2017)
5. Cicirelli, F., Fortino, G., Giordano, A., Guerrieri, A., Spezzano, G., Vinci, A.: On the design of smart homes: a framework for activity recognition in home environment. J. Med. Syst. **40**(9), 200 (2016)
6. Singh, A., Singh Gill, S.: Measuring the maturity of Indian small and medium enterprises for unofficial readiness for capability maturity model integration-based software process improvement. J. Softw.: Evol. Process **32**(9), e2261 (2020)
7. Waraga, O.A., Bettayeb, M., Nasir, Q., Talib, M.A.: Design and implementation of automated IoT security testbed. Comput. Secur. **88**, 101648 (2020)
8. Patwary, A.A.N., Fu, A., Battula, S.K., Naha, R.K., Garg, S., Mahanti, A.A.: FogAuthChain: a secure location-based authentication scheme in fog computing environments using Blockchain. Comput. Commun. **162**, 212–224 (2020)
9. Singh Gill, S., Buyya, R.: Failure management for reliable cloud computing: a taxonomy, model, and future directions. Comput. Sci. Eng. **22**(3), 52–63 (2018)
10. Rao, J., Pattewar, R., Chhallani, R.: A privacy-preserving approach to secure location-based data. In: Bhalla, S., Bhateja, V., Chandavale, A.A., Hiwale, A.S., Satapathy, S.C. (eds.) Intelligent Computing and Information and Communication. AISC, vol. 673, pp. 47–55. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7245-1_6
11. Abidi, S., Essafi, M., Guegan, C.G., Fakhri, M., Witti, H., Ghezala, H.H.B.: A web service security governance approach based on dedicated micro-services. Procedia Comput. Sci. **159**, 372–386 (2019)
12. Lin, C., He, D., Kumar, N., Choo, K.K.R., Vinel, A., Huang, X.: Security and privacy for the internet of drones: challenges and solutions. IEEE Commun. Mag. **56**(1), 64–69 (2018)
13. Asuquo, P., et al.: Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet Things J. **5**(6), 4778–4802 (2018)
14. Ibarra, O.H., Kim, C.E.: Fast approximation algorithms for the knapsack and sum of subset problems. J. ACM (JACM) **22**(4), 463–468 (1975)
15. Lyubashevsky, V., Palacio, A., Segev, G.: Public-key cryptographic primitives provably as secure as subset sum. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 382–400. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_23
16. Impagliazzo, R., Naor, M.: Efficient cryptographic schemes provably as secure as subset sum. J. Cryptol. **9**(4), 199–216 (1996). https://doi.org/10.1007/BF00189260
17. Nosouhi, M.R., Yu, S., Zhou, W., Grobler, M., Keshtiar, H.: Blockchain for secure location verification. J. Parallel Distrib. Comput. **136**, 40–51 (2020)
18. Tang, W., Zhang, K., Zhang, D., Ren, J., Zhang, Y., Shen, X.S.: Fog-enabled smart health: toward cooperative and secure healthcare service provision. IEEE Commun. Mag. **57**(5), 42–48 (2019)
19. Tian, Y., Kaleemullah, M.M., Rodhaan, M.A., Song, B., Al-Dhelaan, A., Ma, T.: A privacy preserving location service for cloud-of-things system. J. Parallel Distrib. Comput. **123**, 215–222 (2019)

20. Alam, T.: Efficient and secure data transmission approach in cloud-MANET-IoT integrated framework (2020)
21. Ratajczak, J., Riedl, M., Matt, D.T.: BIM-based and AR application combined with location-based management system for the improvement of the construction performance. Buildings **9**(5), 118 (2019)
22. Venkateswara Reddy, R., Murali, D., Rajeshwar, J.: Context-aware middleware architecture for IoT-based smart healthcare applications. In: Saini, H.S., Sayal, R., Govardhan, A., Buyya, R. (eds.) Innovations in Computer Science and Engineering. LNNS, vol. 74, pp. 557–567. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-7082-3_64
23. Schmidtke, H.R.: Location-aware systems or location-based services: a survey with applications to CoViD-19 contact tracking. J. Reliab. Intell. Environ. **6**(4), 191–214 (2020). https://doi.org/10.1007/s40860-020-00111-4
24. Gill, S.S., et al.: AI for next generation computing: emerging trends and future directions. Internet Things **18**, 100514 (2022)