KEPES
http://scholopress.com/kepes-journal

2023 Volume 21 Issue 3 pp. 750-762

Secure Exchange of IMSI Number between Sender and Receiver

***Deepika Gautam**[1], **Vipin Saxena**[2]

[1]Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, 226025, India
[2]Professor, Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, 226025, India

Abstract

The use of cloud services has revolutionized computer technology which required strong security for transmission of information. When delivery person (receiver) is approaching to the customer (sender), who has order desired products for delivery then it may happen that the hacker may hack the information in terms of customer's location called as Home Location Registration (HLR) for performing the crime scene. Although, delivery person is controlled by Visitor Location Register (VLR) but hackers may hack the HLR. The present work provides a fuzzy based technique for secure exchange of HLR and VLR between customer and delivery person through International Mobile Subscriber Identity (IMSI) numbers without involvement of hacker so that the authorized services may be provided by the delivery person to the customer. A comparison with previous work available in the literature is also reported and computed results are depicted in the form of tables and graphs.

Keywords: Customer, Delivery person, Hacker, HLR, VLR, Fuzzy logic, Encryption and Decryption

1. Introduction

Mobile devices are coming up with portable and easy to carry designs such as tablets, mobile phones, laptops, IP based cameras, I-pads, navigation device, smart watch devices, etc. All these devices provide with wireless communication capabilities such as Wi-Fi, network connections, Bluetooth and mainly having touchscreen interface which is easy for users to interact. The use of mobile devices has expanded the use of huge of functions such as entertainment, productivity, communication and e-commerce. According to the latest survey of 2023, the use of mobile devices reached upto 91.1%. These devices are equipped with an advance sensors, broad functionalities and services. But these gadgets also provide security threads like phishing emails, malware and data breaches. Mobile devices should provide security feature such as encryption, password protection and secure network to protect data against perilous attacks. The IMSI number is a 15 digits number provided by network operator while taking the Subscriber Identity Module (SIM). Using of IMSI provide multiple benefit in services, including text messages, calls and more. The IMSI identifier is saved on SIM in a 64-bit spaces. This device possesses a MAC address, along with a specific key employed during communication with mobile devices. On the other hand, when making a call, it serves as an additional means of identifying the subscriber because it is derived from IMSI and sent during assignment to the subscriber's modem using Authentication and Key Agreement (AKA) and Programmed Input and Output (PIO) protocols. IMSI consists of three components as shown Fig. 1. The Mobile Country Code (MCC) serves as an identifier for

*Corresponding author

DOI https://doi.org/10.6084/m9.figshare.24182547#128

both the service provider and location, utilizing the Mobile Network Code (MNC) combined with a single cell's identification provided by the base station, before finally being complemented by the unique Mobile Subscriber Identification Number (MSIN) for each individual user.

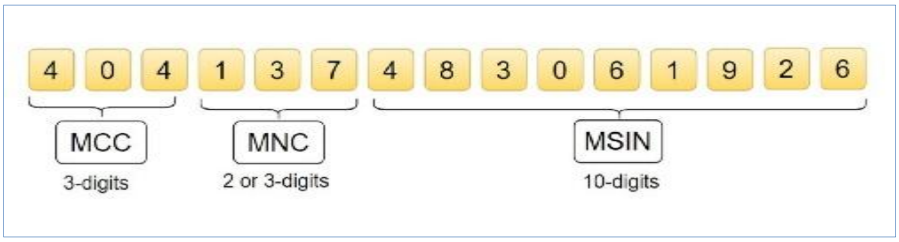

Fig. 1 Format of IMSI number

Information security is grown up these days in technology industry is a critical problem in this digital era and rising a need to provide high security and a shield for crucial information of internet, computers and other electronic devices which are highly used across the network. The feature of encryption, password protection, firewalls and anti-virus software help to assure in security in this computer era. Many researchers and scientists have also contributed amazing algorithms for enhancing the computer security. Most important component of computer security, other than protections, is human behavior, by keeping latest version of software and operating systems, making strong passwords, being alert of shady emails and websites and avoid disclosing private information. To provide protection against hackers, secure information, security of computer and data should be fundamental issue. To maintain wellbeing and security of computer systems and data, a combination of personal safety and technology is necessary.

Cryptography plays a vital role for shielding the information over the communication and it has different kinds of the Mathematical algorithms for protecting the information and communication networks. It also protects from unapproved access and altering of information and can be used to verify users, verify the information integrity and provide communication network security. In cryptography, data is encrypted and decrypted with the help of keys so that only the authentic receiver may read the data. It has generally two categories which are asymmetric and symmetric cryptography using the keys in the form of numerals and characters.

In symmetric key cryptography, the information is encrypted and decrypted using same type of key and thus symmetric key cryptography is of less powerful cryptography which might generate security issues in future whereas asymmetric key whose another name is public key cryptography, employs two different keys i.e., public or private key. The private key is used to decode the information; while the public key is used to encrypt the information. So, the private key should be kept a secret while the public key can be shared across network. This method is more secure and better than the symmetric key cryptography because incase the information and public key is revealed, still private key required to decrypt the information.

During the information exchange, bidirections communication takes place in which the transmitter and receiver send and receive the data in a two-way communication. There are several applications like video calling, messaging and gaming uses two-way communication feature which provide real-time communication between different individuals or devices. This feature allows interaction and data sharing in bidirections using different routes with wired and wireless channels. The protocol is hold up by Transmission Communication Protocol/Internet Protocol (TCP/IP). In order to make connection channel, both the transmitter and the receiver should have suitable hardware, software, and good-speed network access.

In the present work, a system model is introduced using Unified Modeling Language (UML) which give information about a graphical notation of the software systems, static and dynamic behavior. It has different types diagrams represent a particular aspect of the software system, such as class, sequence, use case and activity. It provides wide range of moldable modeling language of software systems from easy desktop applications to complex level of application. There are many object-oriented programming languages which can implement the designed model for better understanding. In the work an algorithm is introduced for protecting IMSI numbers between the customer and delivery person. By monitoring on the traffic between mobile users and the network, one can get IMSI numbers from the network which further use to track the location of a user using any kinds of hand-held device. A fuzzy based technique is used for generating the secret keys for IMSI number protection that overcomes limitations and security issues through ElGamal and fuzzy ElGamal algorithms. Both the algorithms use to generate a new cryptographic key pair. The lack of availability of the Original Equipment Manufacturer (OEM) information about IMSI numbers are the need for secrecy protection. A mechanism is proposed to generate IMSI key pairs from scratch based on ElGamal and fuzzy ElGamal and evaluated the computational time with reported image histogram. This approach uses a .txt file format and Python programming language is used with Visual Studio as a scripting language to enhance the functionality of the both algorithms.

2. Research Background

Security in the mobile world is a real challenging area of the research and researchers have been developed various kinds of the security protocols incorporated in the security algorithms. It will have great potential to be applied on most of personal multimedia devices. For this purpose, mobile security in research papers involves to examine existing studies and publications on data breaches, malware and other security threats. By utilizing signature-based and machine learning approaches, Cinar and Kara (2023) evaluated the present status of mobile security and highlighted the impact in the light of the various security aspects. The Open System Interconnection (OSI) model consisting of seven-layers had been used as the reference model for communication from one device to another device by the various researchers (1981) which is an organized structure to illustrate how network's functions work from the top to down manner. Meeuwisse (2017) wrote a book which stressed over the importance of cybersecurity and the risks that had arisen as a result and it consists of explanation of various terminologies used to describe cybersecurity. Further, Rao et. al., (2023) proposed a Bahdra framework for telecommunications networks, which is used for modeling the threats that are particular to a certain domain. The framework is divided the attack life cycle into three phases and each is containing eight tactical groups and 47 tactics that are consistent with ATTACK. Jiang et al., (2018) used the proxy signatures; a novel delegation-based approach which was developed for cellular roaming systems in order to minimize message flows of conventional anonymous security mechanisms. Lema et. al., (2021) used reinforcement learning to enhance the wireless networks' hidden capacity to learn transmission parameters based on interactions between transponders, recipient, core network and interceptor devices used as cooperative communication devices. The resilient strategy was put out by Ettiane et al. (2021) to defend the 5th Generation (5G) of Machine Type Communication (MTC) system's technical and architectural design from signal DoS assaults that aim to interfere with Radio Resource Control (RRC) protocols. By suggesting an approach that was based on the logarithmic characteristics and power functions, Kumar et. al., (2021) proposed a security mechanism during data exchange using Online Analytical Processing (OLAP). By utilizing a composite Paillier cryptosystem and Homomorphic encryption approach, Kumar and Saxena (2013) addressed significant security challenges related to cloud computing during computation, storing, and data espionage. The primary contributions of Afzal and Murugesan (2022) were to detect anomalies and network security on Signaling System (SS7) network protocol layer which was used to resolve unwanted traffic patterns and identified using the Snort Intrusion Detection System (IDS) and the Wire Shark packet capture tool. In order to account for technology advancement, the trend of the proliferation of digital communications services is identified by Asrani and Kar (2022). It also looked at the factors influencing spatial Information and Communication Technology (ICT) usage in India as well as how social systems influence the technology acceptability at different levels of exposure. In order to guarantee database consistency, Kim's (2020) goal was to keep the HLR database's memory blocks on disc. When data of HLR is lost, then one can use a recovery approach using logging and creating the check points. Danquah and Kester (2019) also examined several articles over the security and created penetration tests and efficient security assessment for the Unstructured Supplementary Service Data (USSD) applications. By reviewing the Burrows-Abadi-Needham (BAN) logic and performing security verification using the AVISPA tool, Tan (2018) developed an authentication scheme for mobility networks that uses elliptic curve cryptosystems to ensure the security. Gope et al., (2021) created an untraceable, anonymous identification scheme that promises to overcome all security problems and provide a way to communicate securely for handheld communication devices. Utilizing blockchain technology and pseudonyms, Haddad (2023) suggested a security mechanism for the 5G network. Waqas et al., (2023) suggested a modelling approach between attackers and users using an advance threat strategy based on the Double Q-learning algorithm. The suggested approach was compared to current Q-learning, Sarsa, and greedy algorithms. The distributed security algorithms may be used for the security of the mobile device which are available in the Milenkovic (1992).

The mobile network authentication method relies heavily on IMSI, however it is also susceptible to security risks. IMSI catchers, are tools that may intercept and record IMSI numbers, possibly enabling attackers to pose as genuine subscribers and get access to network services. From the literature, it is observed that there are continuous attempts to provide more secure mobile network authentication procedures, such as the improved authentication and encryption methods used in 5G networks. Fraunholz et al. (2022) analyzed the IMSI probing assault and its effectiveness while also presented a unique attack variation that challenges the performance level and permits the geolocation identification at the cell level of granularity.

Cryptographic techniques are widely used to enhance mobile security and protect sensitive information stored on mobile devices, transmitted over networks, and used in mobile applications. Some of the most common cryptographic techniques used in mobile security include: Encryption, Hashing, Digital Signatures, Secure Key Exchange, Biometric authentication. For a mobile crowd sensing approach, Arulprakash and Jebakumar (2022) worked on a security model employing a blockchain concept. Mobile crowd gathers a vast amount of data efficiently from several nodes. As a result, there were several security concerns and data breaches. Muheidat et al., (2022) were concerned about the security risks of 5G/6G because to the smart goods that have enhanced lifestyles, such as entertainment, smart traffic lights, automated driving, and other smart items. In terms of security and energy efficiency, quantum technologies will assist 6G systems. Extensible Authentication Protocol (EAP), a standardized method of Authentication Key Agreement (AKA), was employed by Edris et al., (2022) to push end users' experiences into the fifth generation. A proof verifier protocol for security was provided and EAP AKA and 5G-AKA protocols were afterwards compared by the authors to examine security and efficiency outcomes. In order to discover a suitable approach for convex efficiency and the offloading ratio, to address the use of processing power and transmission resources., Chen et al., (2022) studied Mobile Edge Computing (MEC) for developing Cyber Physical Systems (CPS) using Deep Reinforcement Learning (DRL).

In order to provide security and secrecy for sensitive information for a strong wireless network, Asimi et al., (2018) created effective cryptographic primitives and security protocols. For telecare medical information systems, Tan (2019) presented a novel identity-based cryptographic delegation technique. In Java code, the Jintcharadze and Elza (2020) suggested a combination of symmetric and asymmetric keys and demonstrated the advantages of the combined cryptography techniques. As per Ali et al. (2020), the data routed over the channel is crucial variable that has to be safeguarded and proposed a method for securely transmitting the data through various cryptographical algorithms, also computed the complexity of computation and evaluated the performance measures. Thakur and Kumar's (2011) have focused on the efficiency of algorithms by considering the various contexts and compared the behavior and effectiveness of the Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish with various data loads. Latif et al., (2020) studied the results of time evaluations of AES, DES, 3DES, Ron's Code (RC2), and Rivest Shamir and Adleman (RSA) using various text file sizes and key sizes. The end findings demonstrated that the LabVIEW simulator approach was superior than the Advanced Encryption Toolkit. Thirupalu and Reddy (2020) examined several asymmetric algorithms and hashing methods to provide the secure capacity of the protected data. On the basis of encryption time with the change of several file properties such different data kinds, content size, data volume, and key sizes, Masram et al., (2014) offered the study and comparison of some symmetric key cryptographic ciphers.

From the above work, it is observed that none of the research paper was related to the matching of the HLR and VLR for identification of the crime scene at the location of the customer and a fuzzy based technique is used to secure exchange of HLR and VLR between customer and delivery person through IMSI number which reduces the chances to involve the hackers over the communication channel. The methodology on the basis of above aspect is reported into the next section.

3. Methodology

The Global System has two crucial parts. They are Home Location Register (HLR) as well as Visitor Location Register (VLR). Note that these systems facilitate all mobile communication services. The Home Location Register (HLR) can be described as a database. Within it is stored the data of users who use a specific mobile network provider. The location of this information is fixed. HLR provides details about a user's profile. This includes services used by the user. It also includes the user's mobile number. Lastly it entails their location. All calls made by the user happen with HLR's aid. Likewise, all messages sent by the user happen with HLR's aid.

From Fig. 2 Department of Telecommunication (DoT) supports and promotes telecommunication development in India. It forms policies for the growth of telecommunications industry in India, oversee license and permits for companies that operate in telecommunications industry. It also controls frequency allocation, etc. The GSM element is one of the essential services of a GSM network. It supervised and process the calls of the clients. All the subscribers data is hold by HLR which is a permanent database and the original copy is hold by DoT and also holds the information of subscribers according to a particular area code or country. It has two Public Switched Telephone Network (PSTN) deals with call disconnection, number translation, and routing, and (Mobile Switching Center) MSC is for calls processing such as tracking and billing.

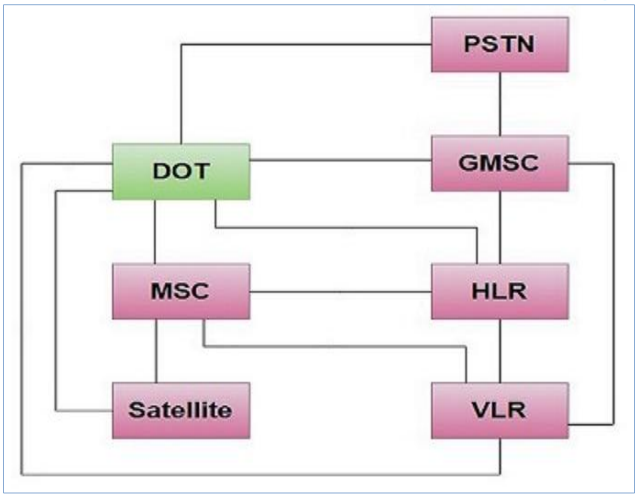

Fig. 2 Interaction of the Various Classes

MSC's are also responsible for providing connection between VLR and HLR, and handles all billing issues like authentication, handover, etc. The communication between HLR and VLR held via satellite to users living in mobile areas or remote areas in two-way communications and data; terminals come in a variety of sizes, from handheld to laptop-size devices. Table 1 showing the components of GSM has own attribute and functions.

Table 1 Classes and Functions of Components of GSM

Name of Class	Attribute	Functions
Satellite	Satellite_Id, Satellite_Address, No_ Active_User	Satellite class controls the transmission of signal and its amplification
HLR	HLR_Id, HLR_Subscriber_Name, Subscriber_Address, Subscriber_Mob_No, Port_No	HLR controls the profile of the customer, location, activity status
MSC	MSC_Id, MSC_No, MSC_Location	MSC class will authenticate to the authorized users and accordingly call routing, location update, network interface activities shall be happened
GMSC	GMSC_Id, GMSC_No.,GMSC_District, GMSC_Location	GMSC class will perform the call routing outside the mobile network
PSTN	PSTN_Id, PSTN_Address, PSTN_Name	PSTN class provide the services through public telecommunications infrastructure
VLR	VLR_Id, VLR_Subscriber_Name, Subscriber_Address, Subscriber_Mob_Number, Port_No	HLR controls the profile of the delivery person, location, activity status
DoT	DoT_Name, DoT_Id, DoT _Location	DoT class Coordinates the telephonic services.

Sequence diagrams are useful for documenting the interaction of several processes in a system, with or without following the dependencies among several activities. The data flow process is shown using a series of rectangles. Each rectangle represents one input or output node, and is connected to the others by solid lines. Some nodes are labeled showing the purpose. From Fig. 3 sequence diagram illustrates how various keys are exchanged when the user's location is being determined.

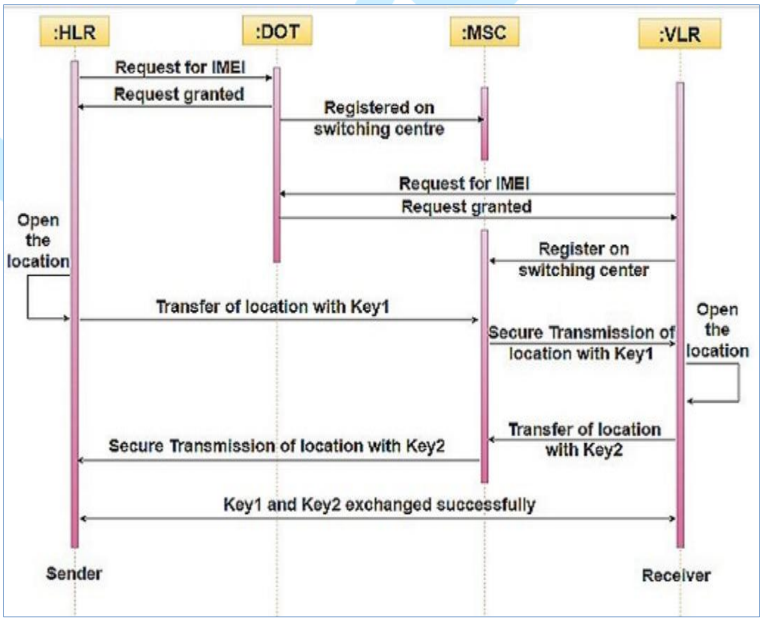
:HLR
:DOT
:MSC
:VLR
Request for IMEI
Request granted
Registered on switching centre
Request for IMEI
Request granted
Open the location
Register on switching center
Transfer of location with Key1
Secure Transmission of location with Key1
Open the location
Transfer of location with Key2
Secure Transmission of location with Key2
Key1 and Key2 exchanged successfully
Sender
Receiver

Fig. 3 Mutual Authentication for Sharing of the IMSI Number

It can either start from HLR or VLR. First, user is required to register over any mobile network which is directly hold by DoT who maintains user records and include all relevant data with location and other details obtained from mobile network providers. The diagram begins at HLR, where IMEI is a mandatory 15-digit number that indicates the device's location. Once the location is operational, Key1 is transferred to MSC, which is in charge of routing calls, SMS, and other services. Key1 is sent from MSC to VLR. Similar to that, the entire process might begin at VLR. By asking to open location then sending Key2 to MSC and then HLR. This way both the keys: Key1 and Key2 are exchanged between the HLR and VLR. Key1 and Key2 are asymmetric keys i.e., one is public key and other is private key. This map a table of information of user related to location of user and other information too. The above diagram begins at HLR, where IMEI is a mandatory 15-digit number that indicates the device's location. Once the location is operational, Key1 is transferred to MSC, which is in charge of routing calls, SMS and other services. Key1 is sent from MSC to VLR. similar to that, the entire process might begin at VLR. By asking to open location then sending key2 to MSC and then HLR. This way both the keys: Key1 and Key2 are exchanged between the HLR and VLR. Key1 and Key2 are asymmetric keys i.e., one is public key and other is private key. This map a table of information of user related to location of user and other information too.

In the year 1985, a computer scientist from the University of California at Berkeley introduced an encryption scheme for digital signatures. This scheme, encrypt the message and the signature together. Elgamal technique (ElGamal 1985) allows only authentic user store the document privately and use it later. The algorithm is illustrated below:

```
Elgamal_algorithm ()

Step 1: Key Generation
        generation of asymmetric key
        for public key: (Y,s,w)
        for private key: (a,s,w)
        where Y=s^a mod w
        w is prime number, s = primitive root of w, a = random integer

Step 2: Encryption
        encryption will generate cipher text ($T_1$, $T_2$)
$T_{1=}s^{ki}mod\ w$
$T_2 = msg.Y^{ki}mod\ w$

Step 3: Decryption
        decryption will convert Cipher text to plain text.
$p = T_1^a\ mod\ w$
        then generate plain text by
$MSG = p^{-1}T_2\ mod\ w$
        where msg = MSG
```

Further the above algorithm is converted by the use of fuzzy concepts and proposed a Fuzzy ElGamal encryption scheme that uses a unique public-private key pairs with some extra parameters to generate its own private key. The receiver will have the associated private key in strict confidence while the public key can be disclosed publicly. This scheme has lower computational complexity than other encryption schemes but still achieves higher security compared to traditional encryption schemes. The fuzzy based Elgamal algorithm is described below in brief:

```
Fuzzy_Elgamal_algorithm ()

Step 1: Key Generation
generation of asymmetric key
for public key: (Y,s,w)
for private key: (a,s,w)
where Y= $s^a mod\ w$
w is prime number, s = primitive root of w, a = random integer
```

Step 2: Encryption

```
using public key and a random key, the cipher text is generated
encryption will generate cipher text (ct)
x=np.arrange(51)
mfx=fuzz.trimf(x,[0,10,50]
for i range (0, len(ct))
  ct[i]=s*ord(c[i])
return ct, mfx
```

Step 3: Decryption

```
defuzzify the fuzzy key into private key
converted the cipher text to plain
mfx=fuzz.defuzz(x, mfx, 'centroid')
for i in range (0, len(ct)):
   p.append(chr(int(ct[i]/h)))
return p
```

The use of fuzzy set is extremely done by the researchers and scientists to solve the complex researcher problems as it gives the optimized results. In the above algorithm, the private and public keys are obtained by the key generation through Elgamal cryptographical algorithm, thereafter the private key is converted through the fuzzy value and called as private fuzzy key. Further the cipher text is generated through the public key and finally defuzzification is done through private fuzzy key to receive the plain text. The interesting results from fuzzy based Elgamal technique is elaborated into the next section.

4. Result and Discussion

Let us first describe the system attributes which are considered here to demonstrate the results obtained by the fuzzy based Elgamal technique. A string of IMSI number is considered as partitioned into 404 (Country Code) 137 (MNC) 483061926 (MSIN) as shown in Table 2, thereafter, the breakup plain texts are first encrypted through public key in both the algorithms i.e., Elgamal and Fuzzy Elgamal algorithms, further, the private and fuzzy private keys are used for conversion of strings cipher text into the original components of plain texts. Hence, the table has two sets of data, one for Elgamal and another for Fuzzy Elgamal.

Table 2 Results of Encryption and Decryption of IMSI number

Components of IMSI number (Plain Text)	Elgamal cryptography				Fuzzy Elgamal cryptography			
	Public Key	Cipher Text	Private Key	Plain Text	Public Key	Cipher Text	Private Key	Plain Text
404 (Country Code)	557	659366086465936	1268	404	1397	759207008075920	766	404
137 (MNC)		621326466869740		137		715407446080300		137
483061926 (MSIN)		65936, 71008, 64668, 60864, 68472, 62132, 72276, 63400, 68472		483061926		75920, 81760, 74460, 70080, 78840, 71540, 83220, 73000, 78840		483061926

The encryption time (in nanoseconds) for Elgamal and Fuzzy Elgamal algorithms for various sizes of plain text files measured in terms of kilobytes (kb). From the Table 3, it is observed that, encryption time increases as the size of the plain text file increases. The computed time for 32kb plain text size is significantly lower than that of a 4096 kb. While on the other hand, Fuzzy Elgamal algorithm encrypts plain text faster in comparison of the Elgamal algorithm, as depicted by the table. The Elgamal algorithm takes 7.67e-9 to encrypt 32kb of data while Fuzzy Elgamal algorithm takes only 2.43e-9 for the same amount of plain text. The size of the text to be encrypted affects the encryption time for both types of algorithms. When choosing between different algorithms for text encryption, it is crucial to weigh the trade-off between security and speed of the machine. In Fig. 4, similar interpretation as presented in the graph form.

Table 3 Time complexity of process of encryption

Plain Text (in kb)	Elgamal				Fuzzy Elgamal			
	1st Run	2nd Run	3rd Run	Average	1st Run	2nd Run	3rd Run	Average
32	7.63e-9	7.84e-9	7.56e-9	7.67e-9	2.41e-9	2.46e-9	2.44e-9	2.43e-9
64	9.65e-9	9.72e-9	9.69e-9	9.68e-9	2.54e-9	2.52e-9	2.56e-9	2.54 e-9
128	10.80e-9	10.75e-9	10.90e-9	10.81e-9	3.13e-9	3.14e-9	3.17e-9	3.14 e-9
256	12.02e-9	12.08e-9	12.06e-9	12.05e-9	3.33e-9	3.35e-9	3.35e-9	3.34 e-9
512	22.72e-9	22.76e-9	22.79e-9	22.75e-9	3.50e-9	3.47e-9	3.50e-9	3.49 e-9
1024	26.45e-9	26.47e-9	26.45e-9	26.45e-9	3.77e-9	3.80e-9	3.81e-9	3.79 e-9
2048	31.04e-9	31.04e-9	31.04e-9	31.04e-9	4.09e-9	4.12e-9	4.12e-9	4.11 e-9
4096	35.02e-9	35.05e-9	35.05e-9	35.04e-9	5.78e-9	5.79e-9	5.78e-9	5.78 e-9

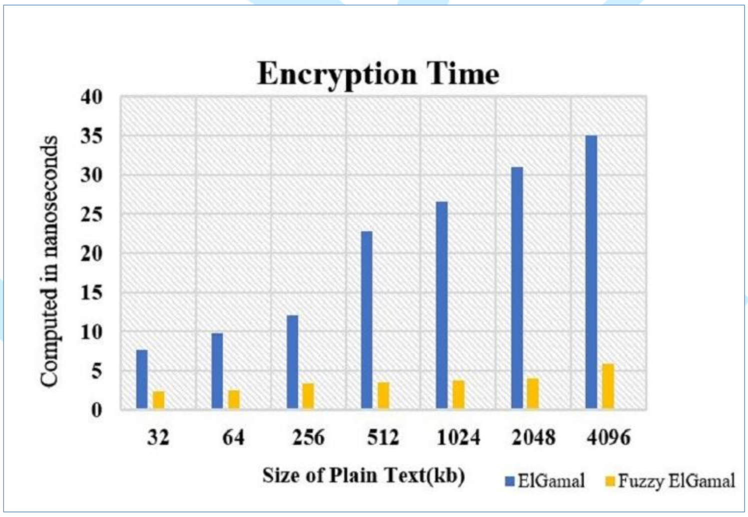

Fig. 4 Encryption Time taken by ElGamal and Fuzzy ElGamal

A comparison table between the existing technique available in the literature and the proposed technique converted into nano seconds (Table 4). The table depict the encryption time (in nanoseconds) for various text sizes (in kb). Twofish, AES, DES and RSA are the encryption algorithm used for encryption. Twofish, shows the increase in time as the size of plain text increases. From the table, Twofish takes more time in comparison to proposed technique.

Table 4 Comparison encryption time with proposed method

Name of algorithm	Encryption Time (10^{-9})							
	32kb	64kb	128kb	256kb	512kb	1024kb	2048kb	4096kb
Twofish [27]	1463712	4140075	5625297	10012910	20001135	42106688	81908320	1831738 97
AES [28]	-	-	2600000000	3500000000	4200000000	-	-	-
DES [28]	-	-	3000000000	4100000000	5100000000	-	-	-
RSA [28]	-	-	3300000000	4500000000	5400000000	-	-	-
Present	00243868	00254547	00314064	00334849	00349866	00379988	00411061	00578431

The timing of encryption for AES, DES, and RSA for text file size 32kb and 64kb are not available in the literature. Encryption timings for 128kb to 512kb for AES, DES and RSA are present in table. Observing the table thoroughly, the proposed method has the lowest encryption time in comparison to other encryption algorithms for all text file sizes. The results show that fuzzy based encryption is the fastest encryption algorithm, while Twofish is the slowest. By the use of fuzzy based Elgamal algorithm, the customer can easily share the HLR controlled by IMSI number to the delivery person. The proposed results can be used to select an encryption algorithm based on the security requirements and performance needs of a particular application.

The decryption time (in nanoseconds) for Elgamal and Fuzzy Elgamal algorithms for various sizes of plain texts measured in terms of kilobytes (kb). For different text sizes (in kb), the decryption time computed in nanoseconds of Elgamal and Fuzzy Elgamal, are displayed in the Table 5. With the increase in text file size, the decryption time for both algorithms also increases. The table demonstrates that Fuzzy Elgamal has a notably quicker decryption time than Elgamal for all text sizes. Since Fuzzy Elgamal decrypts data more quickly than Elgamal, it is a superior choice for situations where speed is a key consideration and exchanged between the sender and receiver. Fuzzy Elgamal decodes data faster than Elgamal and the selection of best decryption technique can be chosen based on the presented information to meet the performance needs of a specific application. In Fig. 5, similar interpretation as presented in graph form.

Table 5 Time complexity of process of decryption

Plain Text (in kb)	Elgamal				Fuzzy Elgamal			
	1st Run	2nd Run	3rd Run	Average	1st Run	2nd Run	3rd Run	Average
32	10.42e-9	10.45e-9	10.46e-9	10.44 e-9	3.08e-9	3.07e-9	3.09e-9	3.08 e-9
64	13.78e-9	13.76e-9	13.76e-9	13.76 e-9	3.37e-9	3.35e-9	3.35e-9	3.35 e-9
128	15.39e-9	15.37e-9	15.37e-9	15.37 e-9	3.72e-9	3.68e-9	3.68e-9	3.69 e-9
256	20.04e-9	20.06e-9	20.04e-9	20.04 e-9	4.19e-9	4.17e-9	4.19e-9	4.18 e-9
512	28.08e-9	28.07e-9	28.07e-9	28.07 e-9	4.55e-9	4.56e-9	4.57e-9	4.56 e-9
1024	32.54e-9	32.53e-9	32.56e-9	32.54 e-9	4.67e-9	4.67e-9	4.66e-9	4.66 e-9
2048	34.05e-9	34.05e-9	34.02e-9	34.04 e-9	4.97e-9	4.97e-9	4.98e-9	4.97 e-9
4096	35.23e-9	35.23e-4	35.26e-9	35.24 e-9	5.21e-9	5.26e-9	5.26e-9	5.21 e-9

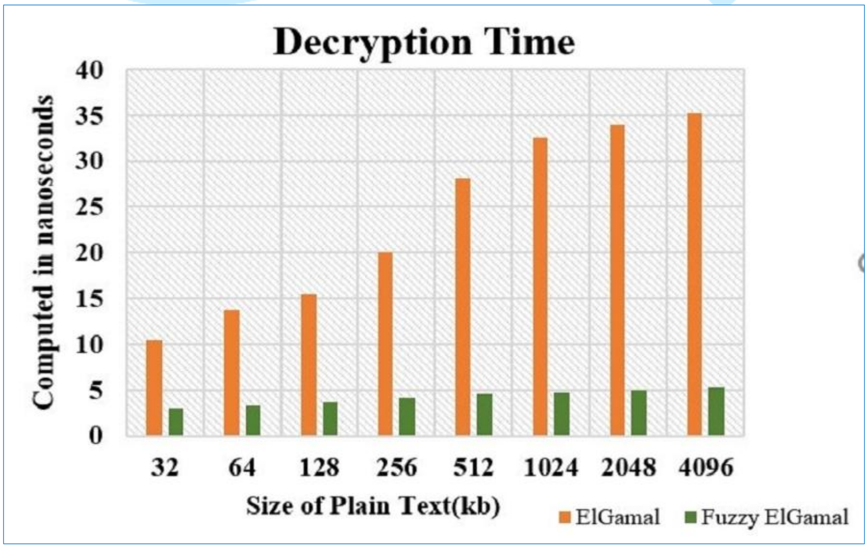

Fig. 5 Decryption Time of ElGamal and Fuzzy ElGamal

The decryption time in nanoseconds of different sizes of text file, showing the impact of existing techniques and proposed technique (Table 6). All of these algorithms are being evaluated: Twofish, AES, DES, and RSA. The data for AES, DES and RSA originates from Ali et al.'s (2020) study while Twofish data is derived from Jintcharadze and Iavich's (2020) research. The table shows that Twofish takes more decryption time for all plain text file sizes. For all plaintext size ranging from 128 kb to 512 kb, these encryption techniques share a decryption time. This study's computation of decryption time shows a consistent lowering compared to other algorithms across various plain text sizes.

Table 6 Comparison of Decryption Time with Present Method

Name of algorithm	Decryption Time (10^{-9})							
	32kb	**64kb**	**128kb**	**256kb**	**512kb**	**1024kb**	**2048kb**	**4096kb**
Twofish [27]	1758853	3235260	4745870	4745870	18426348	44281630	129439314	176583136
AES [28]	-	-	2600000000	3500000000	4200000000	-	-	-
DES [28]	-	-	3000000000	4100000000	5100000000	-	-	-
RSA [28]	-	-	3300000000	4500000000	5400000000	-	-	-
Present	00308938	00335883	00369986	00418945	00456799	0046697	00497997	00521550

5. Conclusion

From the above work, it is concluded that the sender and receiver are treated as customer and delivery person, respectively and the devices of sender and receiver are connected via high-speed internet connectivity and attached through GSM. The customer who desires to order items through online shopping is controlled by the HLR which is treated as the stationary while the delivery person controlled by VLR and is moving from one location to another location. The two devices have the IMSI number and mutually exchanged via communication channel through the proposed method. The security of the Elgamal algorithm has been proven as excellent, hence widely used for encryption and decryption. In the proposed method, Elgamal technique has been converted into the fuzzy based Elgamal technique which produces more optimized results in comparison of the Elgamal technique hence recommended for the user's living in the high security zone. It is proved in the present work that IMSI of each device is transmitted through fuzzy based Elgamal technique which produces the minimum time of encryption and decryption in comparison of the existing algorithms as mentioned in the work, and therefore, it is secure transmission, hackers or intruders are not able to hack the information about the IMSI number of both the devices. The above work can be further extended through machine learning concept for matching the locations of the HLR and VLR.

Funding Information

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Conflict

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Afzal, R. and Murugesan, R-K. (2022). Implementation of a Malicious Traffic Filter Using Snort and Wireshark as a Proof of Concept to Enhance Mobile Network Security. *Journal of Telecommunication and Infor. Tech.*, *1*, 64-71.
2. Ali, K., Akhtar, F., Memon S-A., Shakeel, A., Ali, A. and Raheem A. (2020). Performance of cryptographic algorithms based on time complexity. In 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (Sukkur, Pakistan), 1-5. 2020. DOI= 10.1109/iCoMET48670.2020.9073930.
3. Arulprakash, M. and Jebakumar R. (2022). Towards developing a Block Chain based Advanced Data Security-Reward Model (DSecCS) in mobile crowd sensing networks. Egyptian Informatics Journal, 23(3), 405-415. DOI= 10.1016/j.eij.2022.03.002.

4. Asimi, Y., Asimi, A., Guezzaz, A., Tbatou, Z. and Sadqi, Y. (2018). Unpredictable cryptographic primitives for the robust wireless network security. Procedia computer science,134, 316-321. DOI= 10.1016/j.procs.2018.07.178.
5. Asrani, C. and Kar, A-K. (2022). Diffusion and adoption of digital communications services in India. Information Technology for Development. 28(3), 488-510.
6. Chen, L., Tang, S., Balasubramanian, V., Xia, J., Zhou, F. and Fan, L. (2022). Physical-layer security based mobile edge computing for emerging cyber physical systems. Computer Communications, 194, 180-188, DOI= 10.1016/j.comcom.2022.07.037.
7. Cinar, A-C. and Kara, T-B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. Multimedia Tools and Applications, 1–13. DOI= 10.1007/s11042-023-14400-6.
8. Danquah, P. and Kester, Q-A. (2019). Enhanced Security Assessment Method for USSD Based Mobile Applications. International Conference on Computer, Data Science and Applications (ICDSA), 1-4. DOI= 10.1109/ICDSA46371.2019.9404234.
9. ElGamal T. (1985). A subexponential-time algorithm for computing discrete logarithms over GF (p^ 2)' IEEE transactions on information theory, 31(4), 473-481. DOI= 10.1109/TIT.1985.1057075.
10. Elza, J. and Iavich, M. (2020). Hybrid implementation of Twofish, AES, ElGamal and RSA cryptosystems. In 2020 IEEE East-West Design & Test Symposium (EWDTS), 1-5. DOI= 10.1109/EWDTS50664.2020.9224901.
11. Ettiane R., Chaoub A. and Elkouch R. (2021). Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions. Journal of Information Security and Applications, 61, 1-10. DOI= 10.1016/j.heliyon. 2021.e07108.
12. Fraunholz, D., Brunke, D., Beidenhauser, S., Berger, S., Koenig, H. and Ret, D. (2022). IMSI Probing: Possibilities and Limitations. In Secure IT Systems: *27th Nordic Conference NordSec Proceedings*, 80-97. DOI=10.1007/978-3-031-22295-5_5.
13. Gope P., Ghayvat H., Cheng Y. and Kabir S. (2021). An enhanced secure delegation-based anonymous authentication protocol for PCSs. *International Journal of Communication Systems,* 36(12). DOI= 10.1002/dac.4199.
14. Haddad Z. (2023). Blockchain-enabled anonymous mutual authentication and location privacy-preserving scheme for 5G networks. *Journal of King Saud University-Computer and Information Sciences*. 35(6), 1-7, DOI= 10.1016/j.jksuci.2022.11.018.
15. Jiang C-L., Wu S-L. and Gu K. (2018). New Kind of Delegation-based Anonymous Authentication Scheme for Wireless Roaming Networks. *International Journal of Network Security*. 20(2), 235-42, DOI= 10.6633/IJNS.201803.20(2).05.
16. Kumar J. and Saxena V. (2021). Asymmetric Encryption Scheme to Protect Cloud Data Using Paillier-Cryptosystem. *International Journal of Applied Evolutionary Computation*. 12, 50-58, DOI= 10.4018/IJAEC.2021040104.
17. Kumar N., Verma V. and Saxena V. (2013). A Security Algorithm for On-Line Analytical Processing Data Cube. *International Journal of Computer Applications,* 79(14), 0975-8887.
18. Kim, J-H. (2020). Consistency preservation techniques for Location Register System in Mobile Networks. *International Journal of Internet, Broadcasting and Communication*, 12(2), 144-149.
19. Latif, I-H. (2020). Time evaluation of different cryptography algorithms using labview. *IOP Conference Series: Materials Science and Engineering.* 745(1), 1-10. DOI= 10.1088/1757-899X/745/1/012039.
20. Lema G-G., Weldemichael K-S., and Weldemariam L-E. (2021). Performance evaluation of cooperative mobile communication security using reinforcement learning. *Heliyon.* 7(5), 1-9.
21. Masram, R., Shahare, V., Abraham, J. and Moona, R. (2014). Analysis and comparison of symmetric key cryptographic algorithms based on various file features. *International Journal of Network Security & Its Applications*, 6(4), 43-52.
22. Meeuwisse, R. (2017). *Cybersecurity for beginners*, Cyber Simplicity.
23. Milenkovic, M. (1992). *Operating systems: concepts and design*. McGraw-Hill, Inc.
24. Muheidat F., Dajani K and Tawalbeh L. A. (2022). Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication. *Procedia Computer Science* 203, 32-40, DOI= 10.1016/j.procs.2022.07.007.

25. Rao S-P., Chen H-Y. and Aura T. (2023). Threat modeling framework for mobile communication systems. *Computers & Security.* 125, 1-23, DOI= 10.1016/j.cose.2022.103047.
26. Tan Z. 2019. Anonymous Delegation-based Authenticated Key Agreement Protocol for Global Mobility Networks with Communication Privacy. *Journal of Internet Technology*, 20(1), 59-73.
27. Tan, Z., (2018). Secure delegation-based authentication for telecare medicine information systems. *IEEE Access*, 6, 26091-26110.
28. Thakur J. and Kumar N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation-based performance analysis. *International Journal of Emerging Technology and Advanced Engineering*. 1(2), 6-12.
29. Thirupalu U. and Reddy E-K. (2020). Performance Analysis of Cryptographic Algorithms in the Information Security. *International Journal Engineering Research Technology.* 8(2), 1-6.
30. Waqas, M., Tu, S., Wan, J., Mir, T., Alasmary H. and Abbas, G. (2023). Defense scheme against advanced persistent threats in mobile fog computing security. *Computer Networks*. 221, DOI= 10.1016/j.comnet.2022.109519.