A New Strategy to Enhance the Security of GPS Location by PGP Algorithm in Smart Containers

Mehrunnisa Saleem[1], Salman Ahmad[1], and Safdar Nawaz Khan Marwat[1]

[1]*Department of Computer Systems Engineering, University of Engineering and Technology, Peshawar, Pakistan*

Correspondence Author: Mehrunnisa Saleem (Mehro48@gmail.com)

Received February 23, 2022; Revised May 01, 2022; Accepted May 06, 2022

Abstract

Dynamic navigation devices like Global Positioning Systems (GPSs) are deployed for various purposes in different areas and these devices are usually the central point of interest of various groups like hackers to exploit the data sent and received by GPS systems. The GPS data is usually manipulated using spoofing attacks. This paper proposes a robust solution to the spoofing attacks carried out to manipulate, control and modify the location sharing of smart containers. The primary focus of this paper is securing the GPS information shared by the smart containers. The location shared by the smart containers is secured by encrypting it with Pretty Good Privacy (PGP) algorithm to avoid spoofing attacks in particular. The encrypted GPS location is sent across any communication channel. The receiver side will decrypt the encrypted GPS location at the receiving end. Hence, using this method of PGP encryption will ensure the safe and secure sharing of GPS location by the smart containers. As a result, GPS security has been improved by 80%.

.

Index Terms: *Global Positioning System, Pretty Good Privacy, Spoofing, Encryption, Decryption.*

I. INTRODUCTION

The capability to trace the locations of devices is significant in today's world from the perspective of security-critical applications. Smart containers are the fundamental and integral part of logistics and supply chain management companies which control different commodities ranging from as simple as daily use goods to as complex and high-value commodities to expensive electronic products [1-3]. Similarly, apart from smart containers location of public transport vehicles has also become important and needs to be constantly monitored [4-6]. The majority of the location tracking devices used in the above-mentioned, devices make the usage of Global Positioning System (GPS) location [7]; which is calculated to be used by almost 8 billion devices in 2020 [8]. Twenty-four satellites revolving in six orbits at the height of about 20,200 km from the Earth’s surface are a part of the space segment. These have an inclination angle of 55 degrees. The primary purpose is the assurance that 24 satellites are available. On the contrary, master control stations and the control uplink stations are a part of the control segment. The master control stations are located in Colorado, containing 3 control uplink stations [9]. Despite the wide range of usage of GPS for tracking, still it is not considered safe and secure due to its vulnerability to spoofing attacks. The vulnerability of GPS attacks comes as a result of lacking the authentication mechanism of its incoming signals to the receiver. Spoofing attacks on machines using GPS device for navigation has become common. It has become easy to misguide a ship using GPS location for navigation purposes [10], or land an Unmanned Aerial Vehicle (UAV) by an intruder [11], or forge the present location in a road safety navigation system [12], as a result of GPS signal spoofing attempts. Spoofing attacks can be carried out using different radio hardware devices. There have been various solutions proposed including cryptographic [13-15], and non-cryptographic [16-22] techniques to stop and reduce spoofing attacks. The countermeasures adapted against the mitigation of spoofing attacks have proven to be futile due to two main reasons. Firstly, these methods are mostly not reliable and mostly don't address spoofing attacks correctly which leads to an unnecessary and large number of false notifications of spoofing attacks. Secondly, the countermeasures implemented are proven to have been effective against inexperienced attackers that are unable to find the loopholes in software and hardware systems. Different anti-spoofing techniques [23]; have been also used to counter the spoofing attacks are given as to be using Wide Area Augmentation System (WAAS) message authentication, time arrival approaches, an antenna to differentiate arrival direction, and differentiating and utilizing estimation models ‘PyCode’ [24]; is yet another improved anti-spoofing particle filter. It has also been used for the detection of spoofing-jamming and spoofing jamming suppression. Regarding GPS design, the Substrate Integrated Waveguide (SIW) technique holds immense importance as it enlightens the productivity-based aspects in multiple ways. Implementing a Band Pass filter done through the SIW technique results in compact sizing for the filter [25].

The process of cryptography is carried out using the process of encryption and decryption. The process of encryption is also termed' scrambling' and the process of decryption is also termed 'unscrambling'. So fundamentally plain text is converted into cipher text. The plain text can be explained as the original text or original data. Certain mathematical rules are used to carry out the process of encryption and decryption. Pretty Good Privacy or PGP, in other terms, uses the principle of cryptography to convert plain text into cipher text. Electronic mail is encrypted with PGP and the concept was introduced by Phil Zimmermann in the year 1991. The initial PGP algorithm introduced in 1991 didn't get wider acceptance as it didn't contain distinguished techniques for encryption. The PGP has recently achieved wider acceptability due to more secure algorithms, its existence on the web, and most importantly being freeware. Similarly, one of the reasons for its wider acceptability is the fact that it is neither controlled by any organizational standard and government nor it is in extensive development. Any process of encryption that involves a PGP algorithm for the conversion of plain text into cipher text involves the following four main steps:

1. Authentication
2. Confidentiality
3. Compression
4. Compatibility with Email

All the above steps are implemented to design the Android application. Each step is explained briefly in the following section as to how they can be related in this case. The purpose of this project is to design an Android application that hides GPS positions. PGP is the best encryption system available, secondly only to military-grade encryption, as previously mentioned. As a result, to hide GPS location, the PGP encryption technology is used. The purpose of hiding GPS position is to prevent spoofing attacks, which alter the substance of GPS signals. This application encrypts the GPS coordinates with the PGP encryption technique using a public key on the sender node, and the private key is used to decrypt the GPS coordinates on the receiver node. This method of protecting information between two legitimate stations is highly realistic.

II. PROBLEM STATEMENT

The data that is processed on software, hardware, and other electronic devices has vulnerabilities that can be exploited to inflict system damage. In smart cars, GPS transmission is a must-have feature. In the digital supply chain, intelligent cars are crucial machines. In order to manage the supply chain properly, it is important to share the location of smart cars. The location signals, on the other hand, can be gathered, altered, or regenerated, leading to erroneous smart container location sharing. The major purpose of this study is to use PGP encryption techniques to provide a solid defense against GPS spoofing assaults. According to this research, the smart container has a GPS tracking device installed, which will extract the GPS location, and the smart container's location will then be encrypted using the public key of the receiving station. The GPS signals are encrypted before they are sent over the communication channel. A GPS signal encrypted with the PGP approach is indecipherable without a private key. The GPS location of the smart containers will be protected in this way from GPS spoofing efforts.

III. PROPOSED ALGORITHM

A. Analysis and Design

In the first step, a thorough analysis of the encryption and decryption process is carried out to obtain a better understanding of scrambling and unscrambling of data. Subsequently, the PGP algorithm is studied to understand the process of conversion of plain text to cipher text and vice versa. For the design step, a Flutter-based application is designed for the Android operating system to implement the PGP algorithm for the encryption of GPS location sent by smart containers. The application designed for the implementation of the PGP algorithm generates a pair of keys termed as the public key and private key on both ends. The private key of the user is kept in the application, while the public key of the users is exchanged with each other. The application designed needs an email ID and a password for signing up. The application uses the email ID to generate the public key and the password to generate the private key for the user. For the authentication of a user, a firebase administrator has to approve and authenticate the request of a user for signing up. The authentication process gives more control and security to applications to avoid harmful intruders.

B. Strategy Adapted in Android Application

The following steps are taken while implementing the application design in Flutter. The encryption process as the application is designed will be installed on both the stations including the smart containers and the user that is requesting the location of the smart container. Both the user and the smart containers are assigned public and private keys. The public keys are exchanged with a requesting user if the authentication of the user is approved by the database administrator. Once requested by a user for sending the GPS location, the application installed on the smart containers will encrypt the GPS. The encrypted file is provided to the requesting party, along with the location of the smart container and the user's public key as shown in Figure 1.

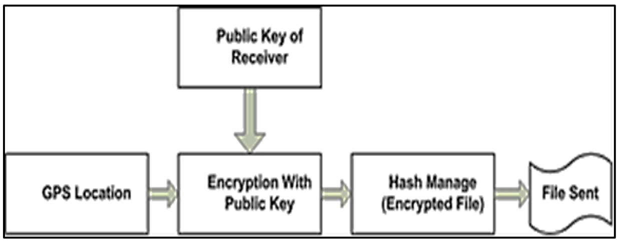


Figure 1: Block Diagram Showing Encryption Process

In the decryption process upon receiving the encrypted GPS location from the smart container, the user decrypts the encrypted file. Figure 2 shows how to extract a file with its private key and the smart container's actual location.

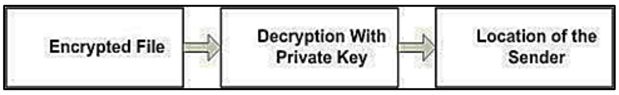


Figure 2: Block Diagram Showing Decryption Process

The machine running the application will wait for the request to be received from the user and approved by the administrator. Once an approved user's request is received, the program will fetch its GPS coordinates using the embedded GPS device. The GPS requesting the user's public key will be used to encrypt coordinates using the PGP technique. The encrypted GPS coordinates will be subsequently shared with the requesting user and the program control loop will again go to the waiting loop to receive a request from the next user.
When the user requests the GPS location of the smart container. The smart container sends an encrypted GPS location back to the requesting user, this time the location sent is an encrypted location, encrypted with the user's public key. The user on receiving the encrypted location uses its private key to decrypt the location coordinates.

C. PGP Steps

The following steps are ensured for the implementation of the PGP algorithm:

a) Authentication:

Authentication is the rudimentary step in implementing the PGP algorithm. It is fundamentally a validation step that is used to authenticate a genuine user and avoid unwanted intruders. This step is important to safeguarding the data. In this paper, the authentication step is implemented using a firebase administrator. The requests coming from users are approved by the firebase administrator after validating the identity of the user. Once the request of a user is approved by the firebase administrator, public and private keys are assigned to the user for encryption and decryption of data respectively. The process of authentication in the application design is explained in Figure 3. In which a user submits data for a signup, and the status of the user goes pending until the firebase administrator validates the user.

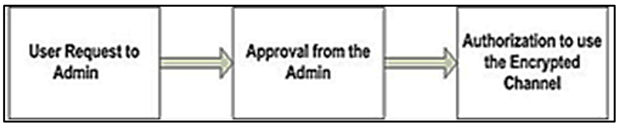


Figure 3: Block Diagram Showing the Authentication Process

b) Confidentiality:

Confidentiality is the second step in the implementation of the PGP algorithm. The symmetric block encryption as shown in Figure 4 explains the confidentiality process in PGP.

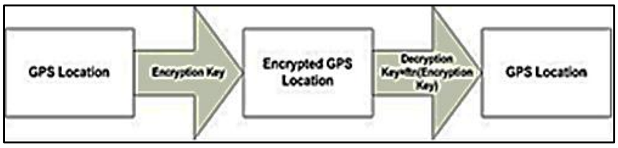


Figure 4: Block Diagram Showing the Implementation of Confidentiality Process

c) Integrity:

Integrity is when the GPS location is encrypted by using the PGP algorithm. The encrypted location shared on the channel cannot be changed or modified. The integrity of GPS location in the application design is ensured by the usage of a digital signature. The digital signature is the combination of private key encryption and hashing as shown in Figure 5 and Figure 6 respectively. To obtain the digital signature, hashing process is used to make a hashed GPS location. The user's private key sent is combined with the hashed GPS coordinates and hence the digital signature is obtained in this manner.

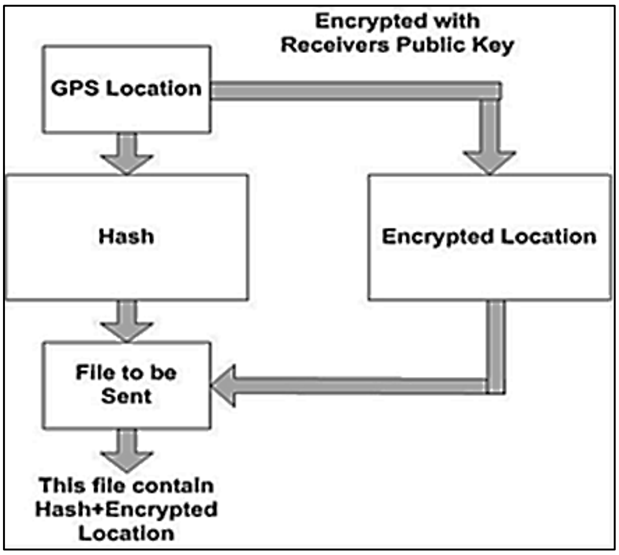

Encrypted with Receivers Public Key
GPS Location
Hash
Encrypted Location
File to be Sent
This file contain Hash+Encrypted Location

Figure 5: Block Diagram Shows Creation of Digital Signature on the Sender's End

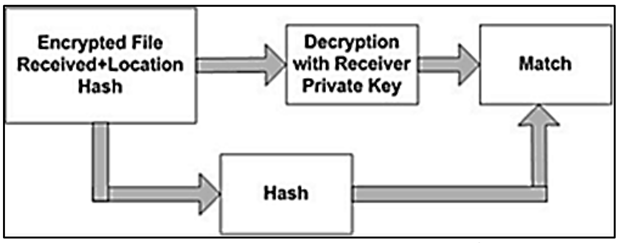

Encrypted File Received+Location Hash
Decryption with Receiver Private Key
Match
Hash

Figure 6: Block Diagram Shows Digital Signal Verification on the Receiver's End

D. Mathematical Background

a) Creation of a Cypher Text:

PGP encryption algorithm ciphers or transforms the original data into a cypher text, the mathematical expression for creating cypher text in the PGP algorithm is, the
'Set of keys' are generated for every user. This set of keys contains a combination of private and public keys where the public keys of every user are present in the public key register.

Cipher text is generated by:

$$c = \text{ENCRYPT}(m) = m^e \bmod n$$

where;
input m is the message,
e is the receiver's public key and
output c is the generated cipher text.

The actual message is encrypted with the shared key using a traditional encryption algorithm. This construction makes it possible to encrypt a message of any length with only one exponentiation.

b) The decryption of a Cypher Text:

Formula for decryption of cypher text is:

m = DECRYPT (c) = c ^{d} mod n

The relationship between the exponents e and d ensures that encryption and decryption are inverses, so that the decryption operation recovers the original message m, without the private key n, d. Consequently, n and e can be made public without compromising security, which is the basic requirement for a public key cryptosystem.

c) Digital Signature:

The fact that the encryption and decryption operations are inverses and operate on the same set of inputs also means that the operations can be employed in reverse order to obtain a digital signature scheme following "Diffie and Hellman's" model.

A message can be digitally signed by applying the decryption operation:

s = SIGN (m) = m d mod n

The digital signature can then be verified by applying the encryption operation to it and comparing the result with and/or recovering the message:

m = VERIFY (s) = s e mod n

IV. RESULTS

A. Implementation of PGP Encryption in Software

Results are obtained via methodology as defined above in which the PGP encryption algorithm is implemented using an Android application. The authorized users will have an access to share encrypted locations using this application. After getting a request of sharing a GPS location the sender will share its encrypted GPS location, this location before sharing is encrypted using the public key of the requesting user. Upon receiving the encrypted location, the receiver will use its private key to decrypt the encrypted location. In this way, the communication is made secure without the possibility of an intruder spoofing or interfering with the GPS packets between the sender and the receiver. The Android application designed for the secured sharing of GPS location is tested thoroughly and there is no loss of data packets or integrity loss found during the process of sharing location. The Android application is explained in the following sections.

B. Applications

The Android application designed for the encryption and decryption of the GPS location of the smart container using the PGP algorithm can be utilized in a variety of applications ranging from encryption of GPS location for quad copters to surveillance drones to safeguard its safe and secure operations.

C. GPS Sharing without PGP Encryption Application

Without the use of the encryption application, there is always a vulnerability factor of the GPS packets sent across the communication channel to spoofing attacks. In the case of smart containers, it will not be possible to continue the operations smartly if subjected to spoofing attacks.

D. GPS Sharing with PGP Encryption Application

With the inclusion of PGP encryption in the GPS communication of smart containers, it is a highly time-consuming and arduous task for the intruders to carry out spoofing attacks as the PGP encrypted GPS location can only be possible or extracted and spoofed if the private key is available. Without the private key, it is not possible to decrypt the GPS location.

E. Authentic Encryption

As the application is executed by an Android operating system, a request inbox is opened; it lists the requesting users, who are requesting the approval to be authenticated for the usage of the application for encrypted sharing of GPS location. Once these users are authenticated by the administrator, they are eligible for sending and receiving encrypted GPS locations using the Android application. By clicking on any of the requesting users will show the user's public key which is generated from the email address of the requesting user as shown in Figure 8. If the public key is selected, the application will retrieve the GPS coordinates from the smart container's inbuilt GPS device and encrypt them using the requesting user's public key. A share button is clicked to share the encrypted GPS coordinates of the smart container. When the asking user receives the encrypted GPS location, the user's password is used as a private key, and the user can decode the GPS location using the private key.

Similarly, the following are the results shown in Figure 7 i.e., the input bits as input to the encryption model, and the time taken in seconds. The graph increases linearly with the input bits versus time. At the breaking point in the linearity, the time taken is significantly reduced.

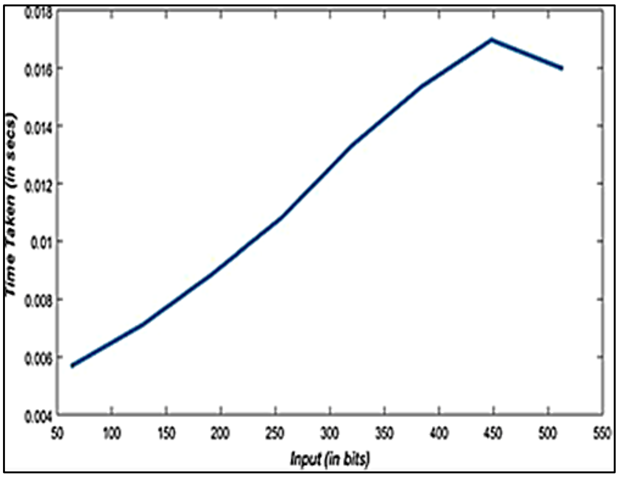


Figure 7: Encryption Process: Input Bits per Time taken

Also, the graph in Figure 8 shows the key lengths of bits against the encryption carried out by the PGP algorithm in milliseconds which are usually ranging from 10 milliseconds to 100 milliseconds approximately for a bit length of 150 bits to 500 bits approximately. The graph can also be linearized if the acknowledgment delay in receiving the bits is ignored which makes it easy to calculate the number of bits to be sent in a specific time by making the acknowledgment delay assumed to be zero.

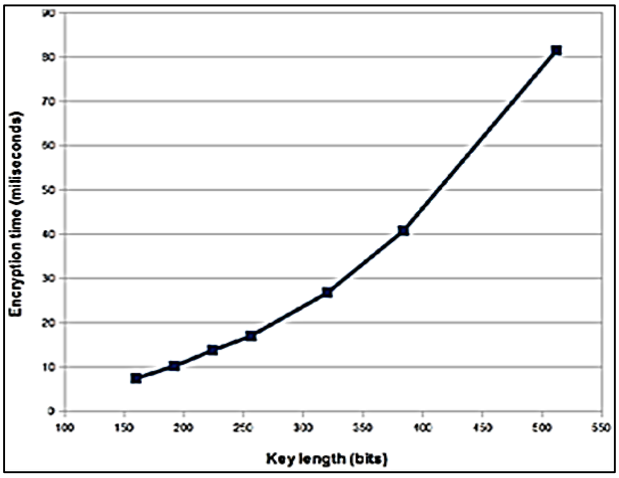
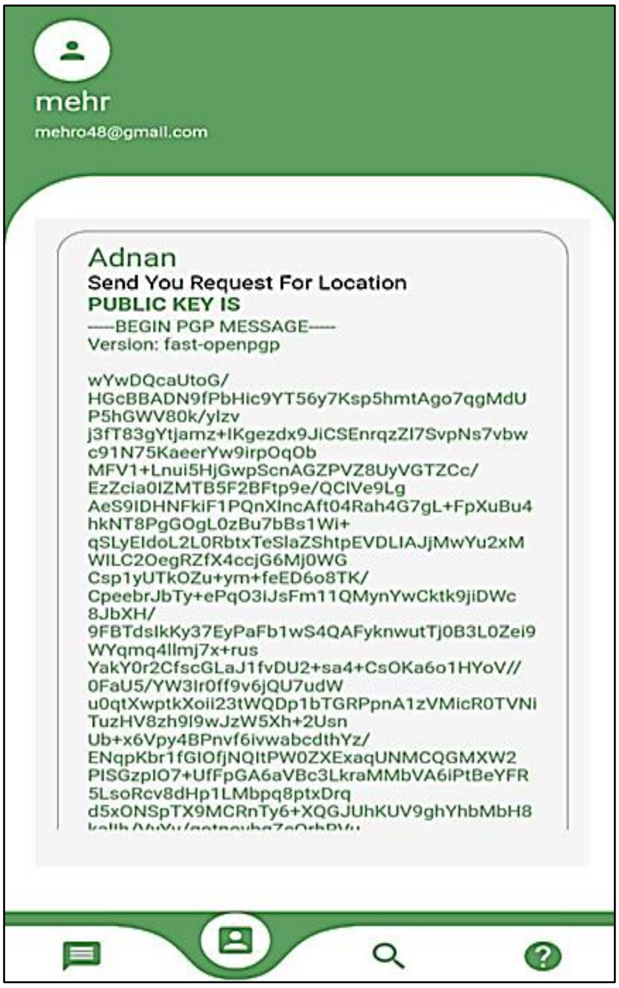


Figure 8: Showing Encryption Time Vs Key Length of Bits.

The user will request for GPS location by sending its public key for the encryption process.



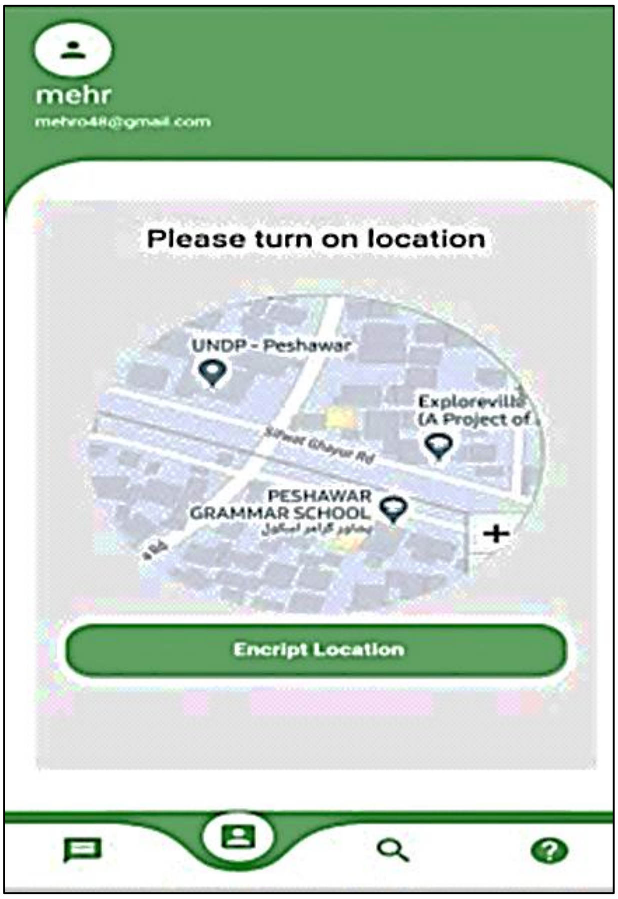
Adnan
Send You Request For Location
PUBLIC KEY IS

```
-----BEGIN PGP MESSAGE-----
Version: fast-openpgp

wYwDQcaUtoG/
HGcBBADN9fPbHic9YT56y7Ksp5hmtAgo7qgMdU
P5hGWV80k/ylzv
j3fT83gYtjamz+IKgezdx9JiCSEnrqzZI7SvpNs7vbw
c91N75KaeerYw9irpOqOb
MFV1+Lnui5HjGwpScnAGZPVZ8UyVGTZCc/
EzZcia0IZMTB5F2BFtp9e/QClVe9Lg
AeS9IDHNFkiF1PQnXlncAft04Rah4G7gL+FpXuBu4
hkNT8PgGOgL0zBu7bBs1Wi+
qSLyEldoL2L0RbtxTeSlaZShtpEVDLIAJjMwYu2xM
WILC2OegRZfX4ccjG6Mj0WG
Csp1yUTkOZu+ym+feED6o8TK/
CpeebrJbTy+ePqO3iJsFm11QMynYwCktk9jiDWc
8JbXH/
9FBTdsIkKy37EyPaFb1wS4QAFyknwutTj0B3L0Zei9
WYqmq4llmj7x+rus
YakY0r2CfscGLaJ1fvDU2+sa4+CsOKa6o1HYoV//
0FaU5/YW3Ir0ff9v6jQU7udW
u0qtXwptkXoii23tWQDp1bTGRPpnA1zVMicR0TVNi
TuzHV8zh9l9wJzW5Xh+2Usn
Ub+x6Vpy4BPnvf6ivwabcdthYz/
ENqpKbr1fGIOfjNQItPW0ZXExaqUNMCQGMXW2
PISGzpIO7+UfFpGA6aVBc3LkraMMbVA6iPtBeYFR
5LsoRcv8dHp1LMbpq8ptxDrq
d5xONSpTX9MCRnTy6+XQGJUhKUV9ghYhbMbH8
```

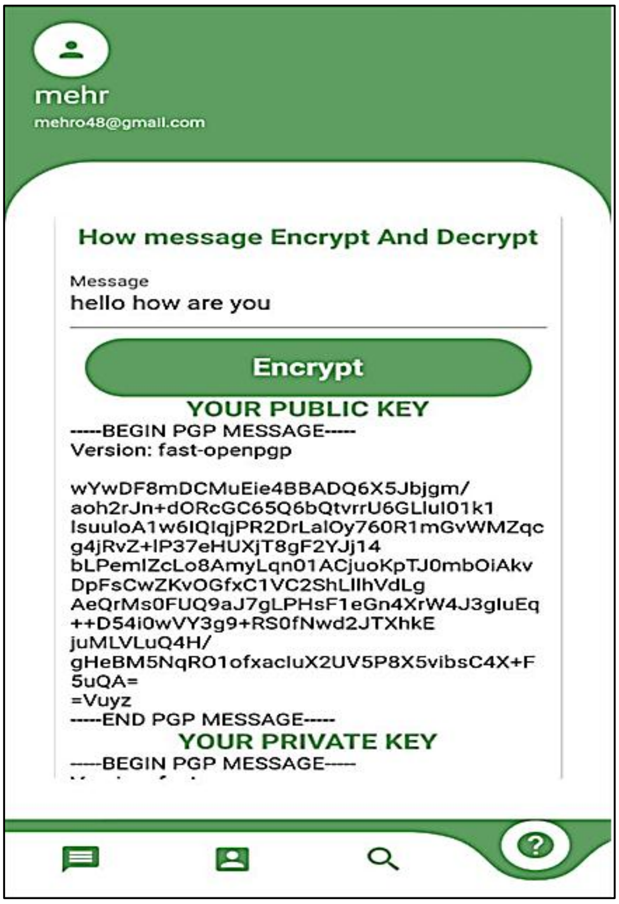
Figure 9: User Request for Location by Sharing its Public Key

Sender before sharing its location will encrypt the GPS coordinates of the device.



Please turn on location

Figure 10: Location Extracted from the Device Ready for Encryption



How message Encrypt And Decrypt

Message
hello how are you

YOUR PUBLIC KEY

```
-----BEGIN PGP MESSAGE-----
Version: fast-openpgp

wYwDF8mDCMuEie4BBADQ6X5Jbjgm/
aoh2rJn+dORcGC65Q6bQtvrrU6GLlul01k1
IsuuloA1w6IQIqjPR2DrLalOy760R1mGvWMZqc
g4jRvZ+lP37eHUXjT8gF2YJj14
bLPemlZcLo8AmyLqn01ACjuoKpTJ0mbOiAkv
DpFsCwZKvOGfxC1VC2ShLIlhVdLg
AeQrMs0FUQ9aJ7gLPHsF1eGn4XrW4J3gIuEq
++D54i0wVY3g9+RS0fNwd2JTXhkE
juMLVLuQ4H/
gHeBM5NqRO1ofxacluX2UV5P8X5vibsC4X+F
5uQA=
=Vuyz
-----END PGP MESSAGE-----
```

YOUR PRIVATE KEY

```
-----BEGIN PGP MESSAGE-----
```

Figure 11: Message Encrypted Showing Both the Public and Private Key of the User

V. CONCLUSION

In this paper, a complete overview of secured GPS coordinates using the PGP encryption algorithm is explained. The primary objective of this research is to protect the confidentiality of the GPS location of the smart containers. PGP encryption used in this research work is to provide secured data transmission at both ends. GPS signals can only be accessed by the sender and the authorized receiver bearing respective private and public keys. Smart containers will use the application developed during this research work, which will provide them immunity against any type of spoofing attacks. PGP encryption will decrease the likelihood of finding a vulnerability to exploit.

The PGP algorithm used in this application enables end-to-end encryption of the GPS packets sent across the communication channel to ensure the safety and security of the data packets from spoofing attacks. The approval and disapproval of selective users by the administrator will ensure that only authorized users are allowed to access the system. The sharing of GPS coordinates of smart containers between authorized users is secured.

Acknowledgment

The authors would like to thank; the University of Engineering and Technology Peshawar, Pakistan for all the support provided to accomplish this research work.

Authors Contributions

Mehrunnisa Saleem's contribution to this study was the concept, performed data collection, methodology, data compilation, and correspondence. Safdar Nawaz Khan Marwat performed the data validation and paper writing. Salman Ahmed's contribution was administration, and supervision of the project.

Conflict of Interest

There is no conflict of interest between all the authors.

Data Availability Statement

The testing data is available in this paper.

Funding

This research received no external funding.

References

[1] Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE access, 6*, 18209-18237.

[2] Carn, J. (2011, November). Smart container management: Creating value from real-time container security device data. In *2011 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 457-465). IEEE.

[3] Jedermann, R., Poetsch, T., & Lang, W. (2014, July). Smart sensors for the intelligent container. In *Smart SysTech 2014; European Conference on Smart Objects, Systems and Technologies* (pp. 1-2). IEEE.

[4] US-DoT. (2019). US Department of Transportation. *Washington, DC, USA*. Retrieved From: https://www.transportation.gov/mission/health/In-vehicle-Performance-Monitoring-and-Feedback

[5] Mintsis, G., Basbas, S., Papaioannou, P., Taxiltaris, C., & Tziavos, I. N. (2004). Applications of GPS technology in the land transportation system. *European journal of operational Research, 152*(2), 399-409.

[6] CIVITAS.EU. (2011). Developing GPS monitoring for the public transport fleet. Retrieved From: http://civitas.eu/measure/developing-gps-monitoring-public-transport-fleet.

[7] Misra, P., and Enge, P. (2006). Global Positioning System: Signals, Measurements and Performance. Second Edition: Lincoln, MA: Ganga-Jamuna Press.

[8] GSA. (2017). Market Report Issue 3. Retrieved From: https://www.gsa.europa.eu/.

[9] Fränti, P., & Mariescu-Istodor, R. (2021). Averaging GPS segments competition 2019. *Pattern Recognition, 112*, 107730.

[10] UT News. (2013). UT Austin Researchers Successfully Spoof an 80 million USD Yacht at Sea. Retrieved From: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

[11] Humphreys, T. (2012). Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing. *University of Texas at Austin (July 18, 2012)*, 1-16.

[12] Zeng, K. C., Shu, Y., Liu, S., Dou, Y., & Yang, Y. (2017, February). A practical GPS location spoofing attack in road navigation scenario. In *Proceedings of the 18th international workshop on mobile computing systems and applications* (pp. 85-90).

[13] Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems, 49*(2), 1073-1090.

[14] Kuhn, M. G. (2004, May). An asymmetric security mechanism for navigation signals. In *International workshop on information hiding* (pp. 239-252). Springer, Berlin, Heidelberg.

[15] Lo, S., & Enge, P. (2010, May). Authenticating aviation augmentation system broadcasts. In *Proceedings of IEEE/ION PLANS 2010* (pp. 708-717).

[16] Wesson, K., Rothlisberger, M., & Humphreys, T. (2012). Practical cryptographic civil GPS signal authentication. *NAVIGATION, Journal of the Institute of Navigation, 59*(3), 177-193.

[17] Akos, D. M. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *Journal of the Institute of Navigation, 59*(4), 281-290.

[18] Ranganathan, A., Ólafsdóttir, H., & Capkun, S. (2016, October). SPREE: A spoofing resistant GPS receiver. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking* (pp. 348-360).

[19] Psiaki, M. L., Powell, S. P., & O'Hanlon, B. W. (2013, September). GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In *proceedings of the 26th international technical meeting of the satellite division of the Institute of Navigation (ION GNSS+ 2013)* (pp. 2949-2991).

[20] Wesson, K. D., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2011, September). An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In *Proceedings of the 24th International Technical Meeting of the Satellite Division of The institute of navigation (ION GNSS 2011)* (pp. 2646-2656).

[21] Warner, J. S., & Johnston, R. G. (2003). GPS spoofing countermeasures. *Homeland Security Journal, 25*(2), 19-27.

[22] Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J., & Lachapelle, G. (2012, April). GNSS spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of IEEE/ION PLANS 2012* (pp. 479-487).

[23] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation, 2012*. Retrieved From: https://gps.stanford.edu/research/current-and-continuing-gpspnt-research/cyber-safety-transportation/anti-spoofing

[24] Li, Y., Guo, X., Zhang, T., & Sun, Q. (2018, July). GPS Anti-spoofing Algorithm Based on Improved Particle Filter. In *2018 USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)* (pp. 17-18). IEEE.

[25] Fathoni, A., Ismail, N., Risnanto, S., & Munir, A. (2020, November). Design of compact SIW bandpass filter for GPS application. In *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*) (pp. 1-4). IEEE.