ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

DATA PARTITIONING METHOD TO IMPROVE DATA SECURITY IN CLOUD FOR THE APPLICATION OF AMBULANCE SERVICE USING GPS

Atleena.A[1], Athirsta Lakshmi.N[2], S.Gururagavendran[3]
UG Scholar, Department of IT, SriVidya College of Engineering & Technology, Virudhunagar[1]
UG Scholar, Department of IT, SriVidya College of Engineering & Technology, Virudhunagar[2]
Assistant Professor, Department of CSE, SriVidya College of Engineering & Technology, Virudhunagar[3]

Abstract: Ambulance is the emergency one that has to be accessed without any delay. The main drawback in the existing system is delay in calling the ambulance. GPS based ambulance service helps to call the ambulance without any delay. This application helps to call the ambulance directly by the user. The Cloud storage enables users to remotely store and retrieve their data. The cryptography technologies offer encryption and decryption of the data. The Ambulance details are stored in cloud. The application for searching the nearby ambulance, based on effective search algorithm and GPS tracking system the nearby ambulance can be found easily. The next drawback in the existing system is in mapping the route to the user location, hat also rectified by this application. The path will be generated between the ambulance location and the user location.

Key words: GPS, Cryptography, Data partitioning, Cloud Storage, AES

Introduction

An ambulance is a vehicle for transportation of sick or injured people to, from or between places of treatment for an illness or injury and in some instances will also provide out of hospital medical care to the patient. The word originally meant a moving hospital, which follows an army in its movements. Cloud computing enables companies to consume compute resources as a utility and maintain computing infrastructures in-house. Cloud computing promises several attractive benefits for businesses and end users [1].

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data [2].

The Global Positioning System (GPS) is a space based navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites [14].

In this project, the user can directly call the ambulance by using this application. The user has to ON the GPS in their mobile phone. By getting the user location, nearby ambulances will be displayed to the user. The user can select anyone of the ambulance from the list; the call will be made to the ambulance. After the call, the map will be generated between the user location and the ambulance location. The path helps the ambulance driver to reach the location easily. The ambulance location is stored in the cloud because; the ambulance location has to be taken for every 5 minutes. It has to store large number of data. That is why the data are stored in cloud. To provide security to the data in cloud AES algorithm is used. It helps to increase the security to the data in cloud.

Related Work

Swapnil V.Khedkar, et al. [4], has proposed the information garage, which avoids the local replica at the user side by

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

using partitioning technique. This method guarantees high cloud storage integrity, improved error localization and easy recognition of misbehaving server. To achieve this, remote data integrity checking idea is used to enhance the overall performance of cloud storage.

Smita Y.Aparadh, Mahesh P.Takale [5], has proposed a survey at the attainable security deserves via adapting data splitting approach in multi cloud architecture. By introducing multi cloud, it makes more difficult in Multi cloud structure to improve safety and privacy for an outside attacker to retrieve or harm the hosted facts or applications of a specific cloud user.

Prakash G L, et al. [6], has proposed an efficient data encryption to encrypt responsive data before sending to the cloud server. This exploits the block level information encryption by using 256-bit symmetric key with rotation. Similarly, data users can reconstruct the requested data from cloud server using shared secret key. The privacy protection of outsourced data using test is performed on the repository of textual content files with variable length. The security and overall performance analysis indicates that the proposed approach is highly efficient than existing methods overall performance.

Nisha D. Dable, Nitin Mishra [7], has proposed that employing the idea of multiple cloud storage together with more suitable security using encryption techniques wherein as a substitute storing complete file on single cloud machine. The system will split up the file in different chunks then encrypt it and store. The records required for decrypting and rearranging that file can be stored in metadata management server for efficient retrieval of original file.

M.Rathamani, Dr. P.Sivaprakasam [8], has proposed specific levels of security over sensitive information the use of cryptographic algorithms and enhances the statistics protection in clouds.

Methods

AES Algorithm

AES relies on a style principle referred to as a substitution-permutation network, combination of each substitution and permutation. [2] AES may be a variant of Rijndael that contains a fastened block size of 128 bits, and a key size of 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes. [3]

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round

Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

- SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey

4. Final Round (no MixColumns)

- SubBytes
- ShiftRows
- AddRoundKey.

Searching Algorithm

The searching algorithm, which is used here, is the effective searching algorithm. That is used to select the ambulances from the database, which are in idle mode.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

Algorithm:
If ambulance_state == idle
display ambulance _list
Else if ambulance_state==Busy &&distance <=20
display ambulance_list
Where ambulance_state == busy
End if

Architecture of the proposed system

The architecture of the proposed model is Fig 1.

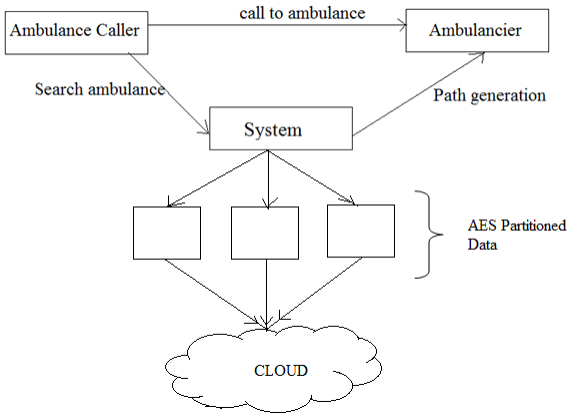
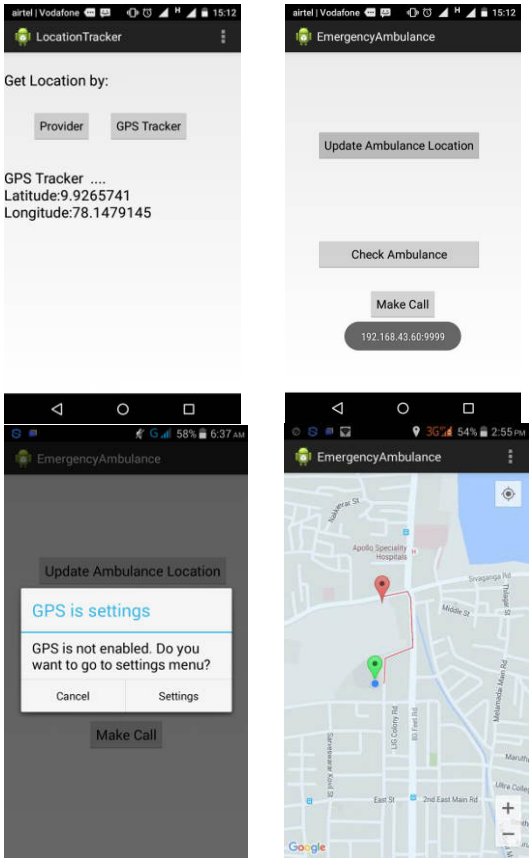


Fig 1: Architecture

The architecture explains the working of the proposed system. First, the user requests the system to show the ambulances, which are in, idle mode. The system gets all the details from the cloud storage. While requesting the data from cloud the encryption and decryption process will takes place. This helps to increase the security of data in cloud. The system finally produces the map between the user location and the ambulance location. This helps the ambulance driver to reach the destination easily.

Result



Conclusion

Thus, the application for searching an ambulance near to the user location by using the GPS has been implemented. That helps in increasing the security of data in cloud. The larger key size makes the algorithm more secure, and the larger input block increases the throughput. This application also helps in finding the nearby ambulance without any delay. There is no time delay in calling the ambulance. The drawbacks in the existing system have been rectified in the proposed system.

Future Work

The future work is to enhance the security of data in cloud through more encryption algorithms and to store the data

in multi cloud environment to secure the data.

References

[1].https://en.wikipedia.org/wiki/Ambulance , Ambulance, From Wikipedia, the free encyclopedia.
[2]. http://aesencryption.net/,AES Encryption, Encrypt and Decrypt the text with AES algorithm.
[3].https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf , Lecture 8: AES: The Advanced Encryption Standard Lecture Notes on "Computer and Network Security" by Avi Kak (kak@purdue.edu) February 25, 2016.
[4].Swapnil V.Khedkar , A.D.Gawande, Data Partitioning Technique to Improve CloudData Storage Security, in (IJCSIT) International Journal of Computer Science and Information Technologies, 2014.
[5].Smita Y.Aparadh, Mahesh P.Takale, Security Prospects Through Multicloud Computing By Adapting Data Splitting, In Journal Of Information, Knowledge And Research In Computer Engineering, 2014.
[6].Prakash G L, Dr. Manish Prateek and Dr. Inder Singh, Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System, in International Journal Of Engineering And Computer Science ISSN:2319-7242, 2014.
[7].Nisha D. Dable, Nitin Mishra, Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment, in International Journal on Advanced Computer Theory and Engineering (IJACTE), 2014.
[8].M.Rathamani, Dr. P.Sivaprakasam, Enhanced Data Security on Storage Cloud Using Cryptographic Techniques, in International Journal of Advanced Research in Computer Science and Software Engineering, 2013.
[9].https://www.android.com/ , android, 2015.
[10]. http://www.coreservlets.com/android-tutorial/ Android Programming Tutorials Developing Mobile Apps in Java, 2015.
[11].http://developer.android.com/training/basics/firstapp/index.html , Building your first APP, 2014.
[12].https://www.linux.com/learn/docs/683628-android-programming-for-beginners-part-1, Android Programming for Beginners, 2016 Linux.com
[13].http://www.xda-developers.com/want-to-learn-how-to-program-for-android-start-here/ , Want to learn how to program for Android? Start Here.
[14].http://www.gsmarena.com/glossary.php3?term=gps, GPS(Global Positioning System), 2016.
[15].Manpreet Kaur, Rajbir Singh, Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing, in International Journal of Computer Applications, 2013.