ITRAFFIC

SMART TRAFFIC IDENTIFYING SYSTEM

Evaluate the best existing secure data transmission and storing methods

Project ID:19-127

Preliminary Progress Review (PPR) Report

Author: S.D Wijewickrama

IT16048638

Bachelor of Science Special (Honors) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

May 2018

ITRAFFIC

SMART TRAFFIC IDENTIFYING SYSTEM

Evaluate the best existing secure data transmission and storing methods

Project ID:19-127

Preliminary Progress Review (PPR) Report

(Preliminary Progress Review submitted in partial fulfillment of the requirement for the Degree of Bachelor of Science Special (honors) In Information Technology)

Author: S.D Wijewickrama

IT16048638

Ms. Shashika Lokuliyana

……

Name of the Supervisor

Ms.Thilmi Anuththara

……

Name of the Co-Supervisor

Bachelor of Science Special (Honors) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

May 2018

Declaration

I declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
S.D Wijewickrama	IT16048638	

The supervisor/s should certify the proposal report with the following declaration.

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the supervisor: Date

Signature of the co-supervisor: Date

TABLE OF CONTENTS

1.0 Introduction…….. 06

1.1 Purpose……. 06

1.2 Scope…… 06

1.3 Definitions, Acronyms and Abbreviations……... 08

1.4 Overview…….. 08

2. Statement of the work……. 09

2.1. Background information and overview of previous……... 09
work based on literature survey

2.2. Identification and significance of the problem……11

2.3. Technical objectives (specify s/w and h/w requirements)…….. 11

3.0 Research Methodology……. 12

4.0 Test data & analysis…….. 15

5.0 Anticipated Benefits……. 15

6.0 Project Plan or Schedule…….. 15

7.0 References…… 17

LIST OF FIGURES

Figure 1.1 – System Overview……. 08

Figure 3.1 – Execution time……. 13

Figure 3.2 – Memory Usage……. 13

Figure 3.3 - Time consumption for encrypt different images…… 14

LIST OF TABLES

Table 1.1 Definitions…….. 08

Table 1.2 Abbreviations……. 08

1.0 Introduction

This Preliminary Progress Review Report provides detailed and complete description of all the functions and specifications all the component of our iTraffic application. iTraffic application is connect the drivers and other parties in the road. The document will explain the purpose and how the system will react to various conditions and objectives, goals and the functions of the system.

Preliminary Progress Review document will be acting as a legal contact between the client and the developer and on the other perspective. It will serve as a validation document for the customer and the developer.

1.1 Purpose

The purpose of this document is to give a detailed description about the progress of our research which is, “ITRAFFIC, SMART TRAFFIC IDENTIFYING SYSTEM ”. This will explain the purpose and complete expression for the development of the approach, including explanations of previous work and outcomes, background, research constraints, anticipated benefits and so on. The motivation trailing this document is to state a clear explanation of the research. This research will be concentrated on, in terms of expanding on the aspect of how the result will be achieved for we will working on and to explain the particular exploration issues. However, this document will make a submission with precisely illustrating set of past work finished, what are the results they have indicated and how they might be applied, in procedure to further development or make different technique relying upon the results found in those past examines.

1.2 Scope

This research is focused on developing an application for vehicle drivers and passengers to reach their destination in efficient way. iTraffic is a mobile application which gives different types of new services to passengers and drivers.

In this iTraffic mobile application, There are four sub function.

- Vehicle detection and informing process.
- Server side data manipulation and tracking process.
- Evaluate the best existing secure data transmission and storing methods.
- Intelligent Driver Assistant.

But we will give the description of the "Evaluate the best existing secure data transmission and storing methods". This function is very important for this system.

Data are transferred through various communication mediums. Among them smartphone has become the most typical and popular mobile device in recent years. With the rapid growing of internet and network applications, data security becomes more important than ever before. The proposed application is based on GPS technology. It traces the location of the users to get rid of traffic congestion. In database users locations and private data will be saved. So there is a major requirement to keep this data in a secure way to prevent the unauthorized access and attacks. For that we compare data encryption algorithms and choose the best one and do following tasks.

- Compare data transmission algorithms for finding the most suitable method for the proposed application. These things will be considered when selecting the method.
- Implement the system using the selected method.
- Finding the best ways to protecting the confidential details of the users and compare these methods for evaluating most suitable way to protect server details from unauthorized accesses
- Implement the selected security mechanism for server.
- Implementing other access control mechanisms for the system.

1.3 Definitions, Acronyms and Abbreviations

Definitions

iTraffic	Name of the proposed service.
Preliminary progress review	

Table 1.1 – Definitions

Abbreviations

3DES	Triple Data Encryption Algorithm
AES	Advanced Encryption Standard
RSA	*Rivest–Shamir–Adleman*
PPR	Preliminary Progress Review

Table 1.2 - Abbreviations

1.4 Overview

The proposed system consists of a mobile application mostly focused on drivers and passengers. It will be helpful to drive vehicles on the road very safety. Our mobile application can interact with passengers, drivers and others who like. This application is connected via cloud server to connect with in build RESTful server in our application and connect to the google map. Below figure explains how our application works briefly.

Figure 1.1 – System Overview

2.0 Statement of the work

2.1. Background information and overview of previous work based on literature survey

Despite the fact that significant amount of literature has been referred, this document includes only the most appropriate information discovered regarding to the current state of the research.

Blowfish

Blowfish: Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, a key and data-dependent substitution. [1]

AES

AES: AES is based on a design principle known as a substitution permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state. [2]

RSA

RSA- RSA is founded in 1977 is a public key cryptosystem. RSA is an asymmetric cryptographic algorithm named after its founders Rivest, Shamir & Adelman.[3] RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys size is 1024 to 4096 bits. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it by using his own private key.[4]

3DES

3DES - Triple DES was developed from DES, uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. In 3DES, DES encryption is applied three times to the plaintext. The plaintext is encrypted with key A, decrypted with key B, and encrypted again with key C. 3DES is a block encryption algorithm.

Performance analysis of data encryption algorithms.

The main goal of any design data encryption algorithm is to protect the data from unauthorized people. When using this data encryption algorithms to practical applications, mainly we have to concern in performance and speed wise. In this research paper they provide a comparison between most commonly used algorithms. They are DES (Data Encryption Standard),3DES(Triple DES), BLOWFISH and AES(Rijndael). In this research paper the comparison has been conducted through these algorithms by running in several processes in various sizes of data blocks. Then they evaluate the speed of data encryption and decryption. Also, these algorithms running through in different software and hardware platforms. So they conclude the research paper by mentioning BLOWFISH is the best performing algorithm among other algorithms that used to do comparing. It concerns security against unauthorized attacks and the speed to data encryption.[6]

DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis

Security is the most challenging problem in the network applications. In this paper provides a comparison between DES, AES and Blowfish algorithms. It mainly concern about the behavior and the performance of the algorithm with different data loads are used. The comparison is made on the basis of these parameters. They are speed, block size and the key size. Simulation program is implemented by using Java.[7]

2.2. Identification and significance of the problem

Data are transferred through various communication mediums. Among them smartphone has become the most typical and popular mobile device in recent years. With the rapid growing of internet and network applications, data security becomes more important than ever before. The proposed application is based on GPS technology. It traces the location of the users to get rid of traffic congestion. In database users locations and private data will be saved. So there is a major requirement to keep this data in a secure way to prevent the unauthorized access and attacks.

2.3. Technical objectives (specify s/w and h/w requirements)

Hardware Requirements

- Processor: Core i3 2.4 GHz or later.
- Hard drive: 120GB or more.
- RAM: 4GB or more.

Software Requirements

- JAVA IDE

3. Research Methodology

This section explains the expected activities to be carried out in order to achieve the primary goal of the proposed research area. Expected outcome of the project is finding the best data encryption algorithm that has fast performance.

Initially a comprehensive literature review was done having the aim to understand the studies already done on the components which are expected to be used in the research.

A security attack can take place on any communications link. There are tow types of attacks in basic. They are active attacks and passive attacks. In active attacks, attackers are adding, updating, editing or deleting the resources of the systems. In passive attacks, attackers are just reading or using the data and other resources of the system without disturbing the normal operations. These both types of attacks can be prevented by using of various cryptography algorithms to applications.

The effect of changing file size for cryptography algorithm

Performance of AES,3DES,DES,RSA and Blowfish will be check by using two parameters. They are, 1) Execution time

2) Memory Usage

All the implementations will be implement by using java language. Separate customize programs are develop to calculate the execution time and memory usage. Also every program will be execute 25 data files which has different sizes. Then each data file will run 3 times and get the average execution time of the each data file.[8]

Small data files File name (size in bytes)	Execution time (milliseconds)		
	AES	DES	Blowfish
Data1.txt (100)	191	176.8	182.6
Data2.txt (200)	192.4	177.0	183.6
Data3.txt (300)	198.8	182.0	183.8
Data4.txt (400)	196.8	184.2	183.8
Data5.txt (500)	198	185.4	184.8
Data6.txt (600)	195.6	186	184.6
Data7.txt (700)	202.6	188.8	185.8
Data8.txt (800)	202.8	189.2	185.2
Data9.txt (900)	201.2	187.4	188.4
Data10.txt (1000)	206.6	189	189

Figure 3.1 – Execution time [8]

Small data files File name (size in bytes)	Memory usage (in bytes)		
	AES	DES	Blowfish
Data1.txt (100)	1,263,019	1,271,074	1,258,267
Data2.txt (200)	1,263,026	1,271,061	1,258,197
Data3.txt (300)	1,263,026	1,271,061	1,258,210
Data4.txt (400)	1,263,026	1,271,061	1,258,197
Data5.txt (500)	1,263,019	1,271,061	1,258,174
Data6.txt (600)	1,263,013	1,271,102	1,258,203
Data7.txt (700)	1,263,019	1,271,123	1,258,168
Data8.txt (800)	1,263,069	1,271,032	1,258,237
Data9.txt (900)	1,263,026	1,271,123	1,258,203
Data10.txt (1000)	1,263,054	1,271,123	1,258,197

Figure 3.2 – Memory Usage [8]

The effect of changing file type for cryptography algorithm.

In the above section, the comparison between Performance Evaluation Algorithms has been conducted at text and document data files. In this section we will make a comparison between other types of data (Images) to check which one can perform better in this case.[9] In here also we use these file types in to all above mentioned algorithms.

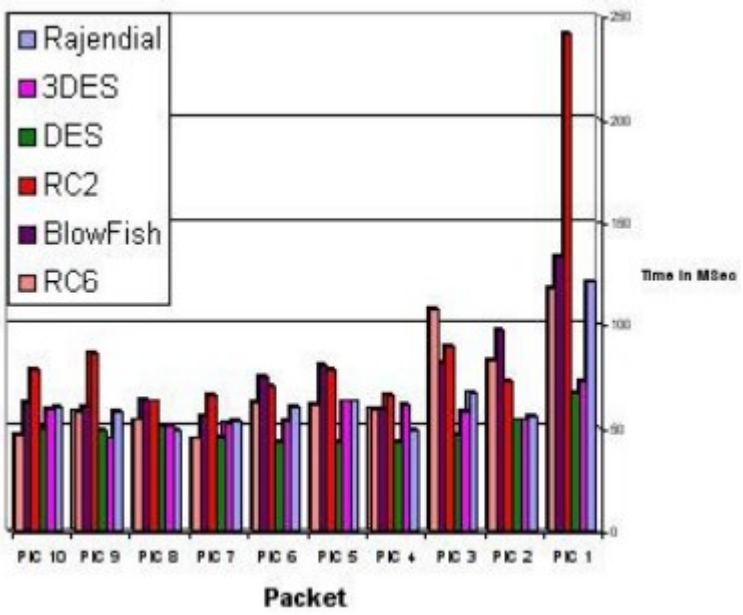


Figure 3.3 - Time consumption for encrypt different images [9]

4. Test data & analysis

Lots of hackers making their attacks to the data when the time of data transmitted. The D DOS attack is widely used for making these attacks. So by doing a D DOS attack to the implemented application, we can check whether the application is in secure level.

5. Anticipated benefits

- When transferring data from device to device is a risky proposition. Encryption technology can help protect store data across all devices, even during transfer.

- Encryption is used to protect sensitive data, including personal information for individuals. This helps to ensure anonymity and privacy, reducing opportunities for surveillance by criminals.

6.0 Project Plan or Schedule

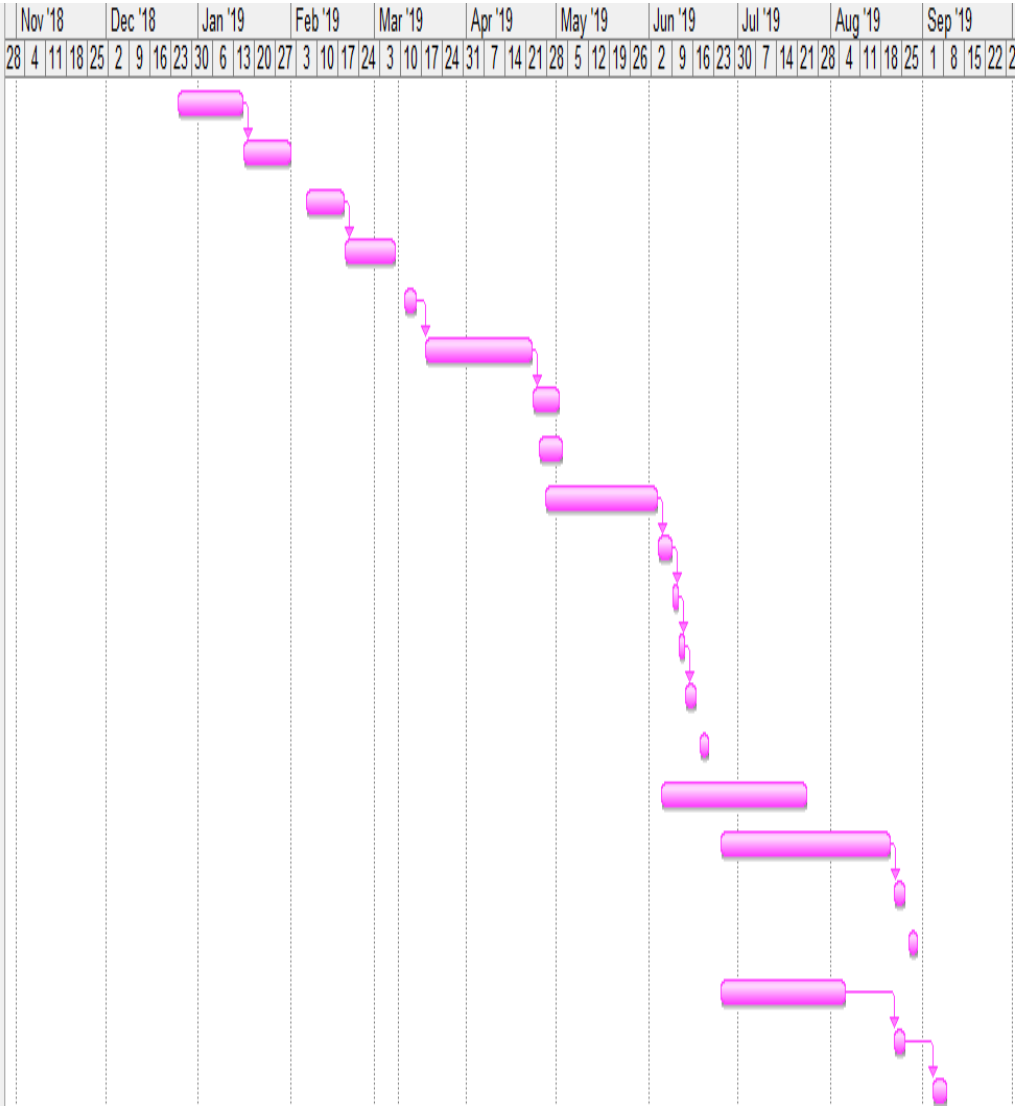
Main Tasks of the Project Plan can be categorized as follows.

- Literature Study
- Experimental Design
- Conducting Experiment
- Result Collection and Analysis
- Verification and Discussion
- Journal and Paper Writing

At the basic level, there will be comprehensive literature study (partially done) to comprehend the problem with current paths taken to solve this. With the initial study decision was made to continue with natural language processing and a machine learning based approach to solve problem.

Gantt chart will illustrate the detailed presentation of the work plane with the time frame.

Task Name	Start Date	End Date	Predeces
Research Topic Selection	Tue 12/25/18	Tue 1/15/19	
Project Charter	Wed 1/16/19	Thu 1/31/19	1
Study on Research Area	Wed 2/6/19	Mon 2/18/19	
Project Proposal Report	Tue 2/19/19	Thu 3/7/19	3
Proposal Presentation	Mon 3/11/19	Thu 3/14/19	
SRS Document/ Design Document	Mon 3/18/19	Mon 4/22/19	5
System Design and planning	Tue 4/23/19	Wed 5/1/19	6
Design Interface sketches	Thu 4/25/19	Thu 5/2/19	
Implementation of Zilla functions	Sat 4/27/19	Mon 6/3/19	
Unit Testing Level 01	Tue 6/4/19	Sat 6/8/19	9
Module Testing Level 01	Sun 6/9/19	Mon 6/10/19	10
System Integration Level 01	Tue 6/11/19	Wed 6/12/19	11
System Testing Level 01	Thu 6/13/19	Sun 6/16/19	12
Progress presentation 50%	Tue 6/18/19	Thu 6/20/19	
Prepare Research Paper	Wed 6/5/19	Tue 7/23/19	
Implementation of Zilla functions	Tue 6/25/19	Tue 8/20/19	
Testing Level 02	Thu 8/22/19	Sun 8/25/19	16
Progress presentation 90%	Tue 8/27/19	Thu 8/29/19	
Final Report	Tue 6/25/19	Mon 8/5/19	
Final Report Feedback submission	Thu 8/22/19	Sun 8/25/19	19
Website Assessment & Research Book	Wed 9/4/19	Sun 9/8/19	20



References

[1] Alabaichi, A.; Ahmad, F.; Mahmod, R., "Security analysis of blowfish algorithm," in Informatics and Applications (ICIA),2013 Second International Conference on , vol., no., pp.12-18,[23 April 2019]

[3] Preetha M, Nithya M. A study and performance analysis of RSA algorithm. International Journal of Computer Science and Mobile Computing. 2013;2(6):126-139.

[4] Aman K, Sudesh J, Sunil M. Comparative Analysis between DES and RSA Algorithm's. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(7):386-391.

[5] Pushpendra Verma, Dr. Jayant Shekhar, Preety, Amit Asthana, A Survey for Performance Analysis Various Cryptography Techniques Digital Contents, Vol. 4, Issue. 1, January 2015, pg.522 – 531, [Accessed: 02nd March 2019]

[6] Verma O. P., Agarwal R., Dafouti D. & Tyagi S, Performance Analysis Of Data Encryption Algorithm, Notice of Violation of IEEE Publication Principles Performance analysis of data encryption algorithms. 3rd International Conference on Electronics Computer Technology, 2011[Accessed: 02nd March 2019]

[7] Jawahar Thakur and Nagesh Kumar, DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, Volume 1, Issue 2, December 2011, [Accessed: 10th March 2019]

[8] Kuntal Pate , Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files , 17 December 2018 [Accessed: 2nd May 2019]

[9] D. S. Abdul. Elminaam, H. M. Abdul Kader, M. M. Hadhoud, Performance Evaluation of Symmetric Encryption Algorithms, Volume 8, 2009 ISSN: 1943-7765, [Accessed: 1st May 2019]