Smart Road Maintaince Portal

Rutuja kadam, Komal Kolhe Harshada Kangane, Vrushali Parad,

Prof. Rushikesh Bhalerao

Dept. of. IT, Sir Visvesvaraya Institute of Technology, Maharashtra, Nashik, India

ABSTRACT: An information system is a very famous tool in this digital era. People all over this world use this tool to get and share information. Computer based system is one type of information system that very often to use in this era. It touches over all the sides of life now a days. In our country we have government bodies (Municipal Corporation) which are responsible for maintaining and running cities. It's all their responsibilities to address the complaint of citizens. For this municipal could Corporation has 2 ways, in first cameras or other surveillance devices have to be installed and second way is that citizens report their problem to the municipal corporation. The second way is mostly used because it is cheaper as compared to first one. But it takes paper work and time too because the citizens has to visit the ward office and report problem faced by them which can be solved by municipal corporation or as due to the emergence of internet and its various capabilities ,there has been rise in the number of complaint sites which provides citizens a platform to lodge a complaint online. As mobile application is mostly used by people ,this app will help people to lodge a complaint through it and can attach a picture of things which are causing problem and location will be tracked using GPS(Global Positioning System).The application also provides a user facility to view status of lodge complaint until is resolved , while online system will help officers at Municipal Corporation to solve/reject complaint with reasons and monitor the status of complaint. The Aim for creating this Application is to simplify the process of lodging complaint to respective Municipal Corporation and make it quick and cheaper.

KEYWORDS: Municipal Corporation, GPS, Mobile Application, Cameras Internet, Online, Complaint, Citizen.

I. INTRODUCTION

In India we don't have any direct communication between the government and public in an efficient way for solving the problems i.e. for getting a problem solved in our place we have to bribe the officials and get them solved in 2 months which can be solved actually in 1 month of time. In order to overcome this problem previously National Informatics Centre has launched a site named Prajavani through which public can post the petitions or complaints in the site and get them solved in a specified time and can also know the status of the complaint   or petition he has lodged at any time. NIC has launched this site with the goal of Right to Information Act (RTAct) i.e. providing the complete information of a place to the user at any time. But it failed in providing the complete information to the public and is providing only the complaint lodging facility to the public. There are four modules for this system are

- Admin
- Department
- User/Public
- Supervisor Department

II. IMPLEMENTATION

1. LOGIN MODULE:

The main activities in the application are the user login page for user. The other modules are followed by this loginpage. This module records only user and password of the user.

2. REGISTRATION MODULE:

Another main function of our proposed system is registration, in order to register with the unique application detailssuch as name; password, email, place and time are required.

3. ADMIN (WEB APP):

- Who has a valid login id and password. The operators will get the complete information about the place including the problems from the survey officials. These operators are spread throughout the district and will process the information to the corresponding authorities and will update the system with current information.
- Admin is the end user who has a valid login id and password. To perform Technical administrative work like to Create Logins, Add and Modify Officer information and to solve the technical problems etc. Each District has one Super User.

4. DEPARTMENT (WEB APP):

- Can View complaints.
- Can close complaint with reason or comment
- Can update status
- Will get notification as per schedule added by admin.
- Department is the end user who has a valid login id and password. Department will monitor a place without going to their and get the information and takes the corresponding action. Then discusses it with higher officials.

5. USER/PUBLIC (WEB APP):

- Can Register & Login.
- Can Complaint with Images / Information with Department.
- View all complaint.
- Comment option on complaint.
- Can check status of complaints.
- User is the end user who has a valid login id and password. user can loginto the system and know the complete information and can post the problem. User can login to the system and know the complete information and can post the problem.

6. SUPERVISOR DEPARTMENT:

- Supervisor is the who has a valid login id and password.
- View deadline crossed complaint.
- Can Comment on status f complaint Change priority can change

## III. PROPOSED ALGORITHM

A. Design Considerations:
- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

B. Description of the Proposed Algorithm:

AES is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

STEP 1: CREATION OF ROUND KEY:

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.
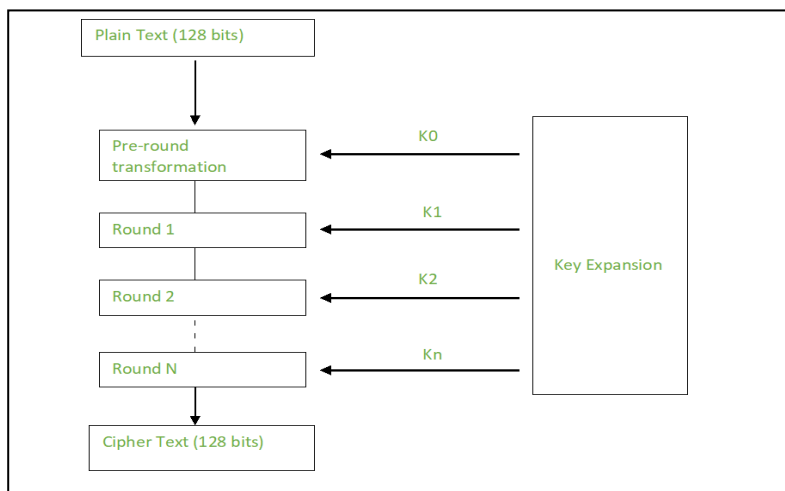
Encryption :

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

STEP 2: LEFT SHIFT OPERATION:

SubBytes:

This step implements the substitution.

In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows:

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.(A left circular shift is performed.)

[b0 | b1 | b2 | b3]   [b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
| b8 | b9 | b10| b11| | b10| b11| b8 | b9 |
[b12| b13| b14| b15]   [b15| b12| b13| b14]

MixColumns:

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

This step is skipped in the last round.[c0] = [2 3 1 1] [b0]
| c1 | = | 1 2 3 1 | | b1 |
| c2 | = | 1 1 2 3 | | b2 |
[c3] = [3 1 1 2]   [b3]

Add Round Keys :

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes isnot considered as a grid but just as 128 bits of data.
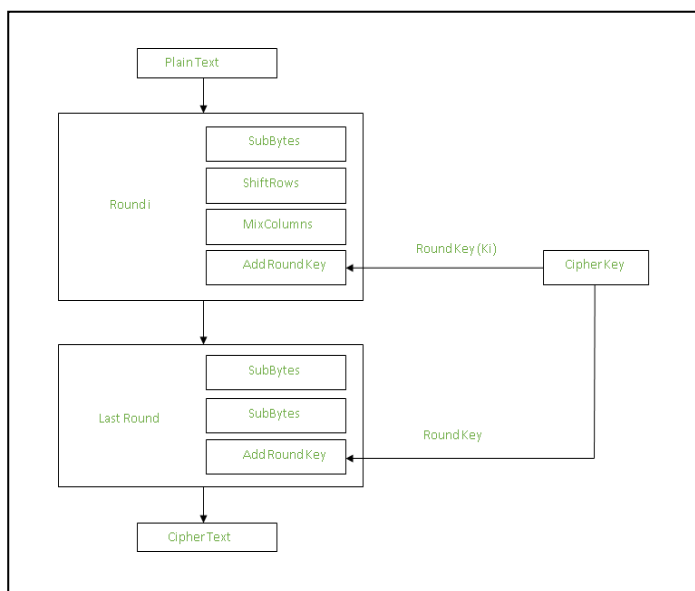
STEP 3: DECRYPTION :

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns :

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.
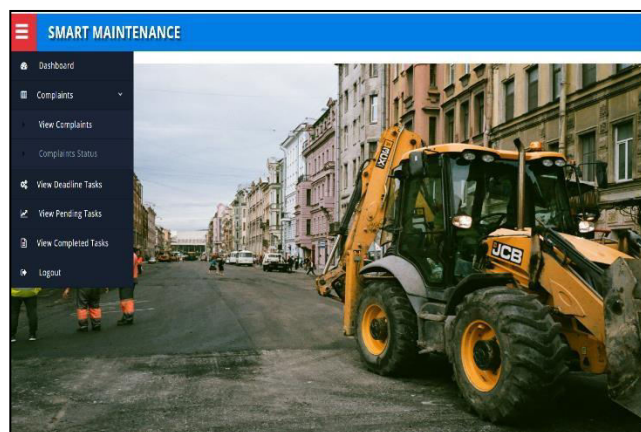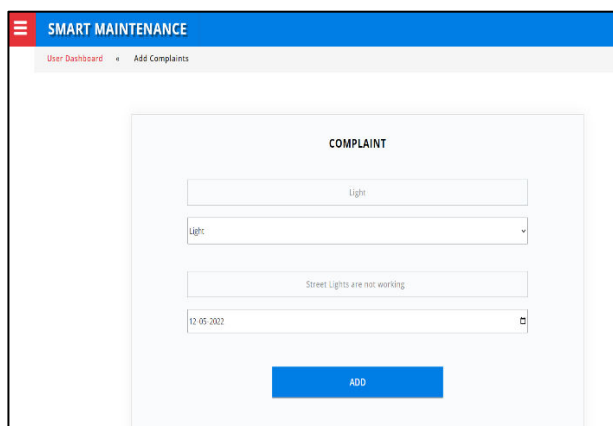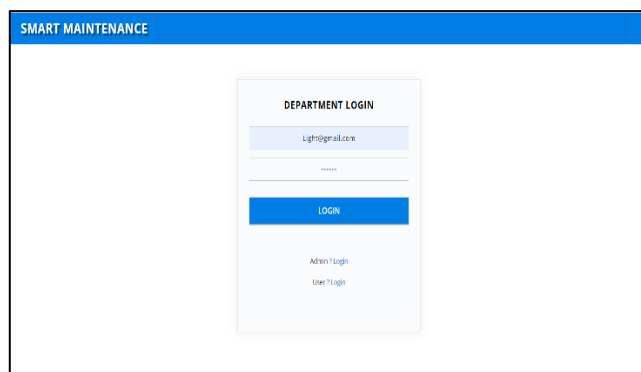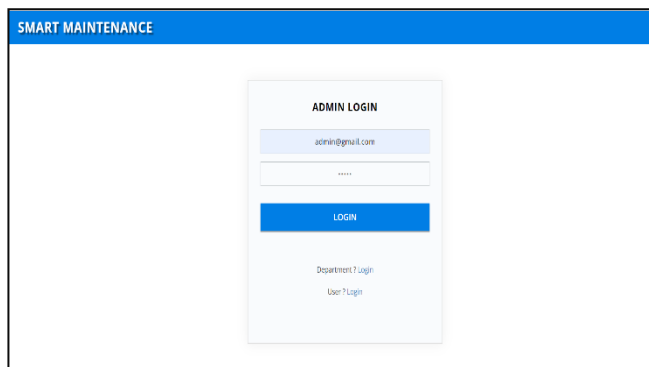
[b0]=[14 11 13 9] [c0]
| b1 |=| 9   14 11 13 | | c1 |
| b2 |=| 13 9   14 11 | | c2 |
[b3]=[11 13 9   14]   [c3]

Inverse SubBytes :

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

IV. RESULTS

V. FUTURE WORK

- Incorporate Level:
  This demo based smart road maintenance system is based on a small project which can be extended with extra feathers like -incorporate order information, internal work details etc.
- Same complaints redundancy:
  There should be a algorithm to reduce same complaints from a same area. This will lead to morecomplexities for the complaint resolution.
- Real time implementation:
  This project should be implemented at state level for all cities so that all cities complaints will be register ona single portal.
- Sentimental analysis:
  Using the sentimental analysis concept we can get the severity oof the public complaints by which we can give priorities to all the complaints.

VI. CONCLUTION

The system has the benefits of easy access because it is be developed as a platform independent web application, so the admin can maintain a proper contact with their users, which may be access anywhere .All communications between the user and administrator has done through the online, so this communication cost also be reduced. It is user friendly , and has required option, which can be utilized by the user to perform the desired operations. Application software meets

the information requirements specified to a great extent. The system has been designed keeping in view the present and future requirements in mind and made very flexible. The goals that are achieved by the software are Instant access, improved productivity, Optimum utilization of resources, Efficient management of records, Simplifications of the operations, Less processing time and getting required information, User friendly, Portable and flexible for further enhancement.

REFERENCES

[1]. Complaint", International Journal for Research in Engineering Application & Management (IJREAM), Vol- 01, Issue 03, June 2015.

[2]. Aditi Mhapsekar "Voice enabled Android application for vehicular complaint system using GPS and GSM- SMS technology," in World Congress on Information and Communication Technologies, 2012, pp. 520-524.

[3]. Aaditeshwar Seth, Abhishek Katyal, Rohit Bhatia, Dinesh Kapoor, Balachandran C, Vidya Venkat, Aparna Moitra, Sayonee Chatterjee, Mayank Shivam, Z. Koradia, Praveen Naidu, "Application of Mobile Phones and Social Media to Improve Grievance Redressal in Public Services", m4dposition.

[4]. Patrícia Abreu, Sérgio Sousa, Member, IAENG, and Isabel Lopes, "Using Six Sigma to Improve Complaints Handling", Proceedings of the World Congress on Engineering 2012 Vol IIIWCE 2012, July 4 - 6, 2012, London,

[5]. Dilip B. Gupta, Dr. Sujit G. Metre, "Decentralization and Delegation of Authority at Nagpur Municipal Corporation (NMC) Nagpur", International Journal of Management (IJM) Volume 6, Issue 3, March (2015), pp. 38-49

[6]. Trupti Bomble Int. Journal of Engineering Research and Applications android Based Complaint Management System For Municipal.ISSN:2248-9622,vol.5,issue 4,(part-3),April 2015,pp64-636.

[7]. Anuj bhardwaj. b ,arul murugan k, Mr.Ramkrishnan," Android based regulatory complaint system", International Journal of Scientific Research in Science, Engineering and Technology, IJSRSET.
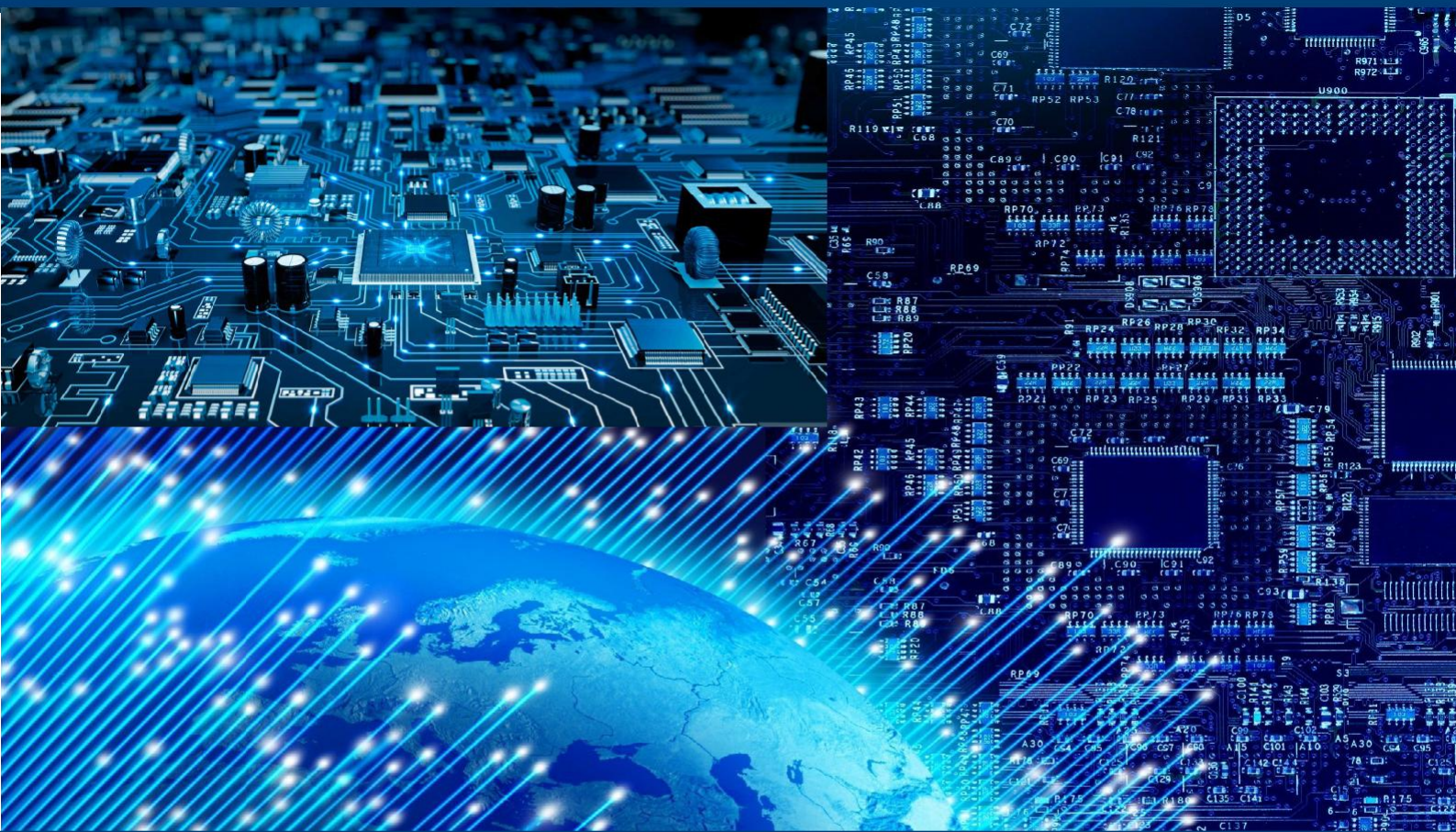
INTERNATIONAL JOURNAL OF

MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY