QR Code Encryption, Location Verification and User Authentication Based Human Resource Management System

R. Krithika Sowbarnika
SNS College of Technology, India

Dr. J. Rajeshkumar
SNS College of Technology, India

Abstract

Human Resource Management system is made to automate the manual work done by Human resource managers. In this paper, a smart attendance system for industry using QR code, Geo Location and OTP processing is proposed with objective of reducing the deployment cost for tracking employee's attendance. Attendance is automated using the location by detecting the employee location to make attendance and it generates QR code of employee. Based on the QR Code, OTP is send to his/her registered mobile number to ensure that employee with their authenticated mobile number can mark attendance with log time. It also maintains separate leave record, in which the employees can make leave request and on acceptance they can avail it along with which they can view their leave options available for them. Each employee leave report, attendance report and pay slip reports are automated and send to HR Manager. HR can automate the email of these reports and any official information by which Events, Alerts, Circulars are being notified accordingly to particular person or group of separate category. The method of developing the system is a web app and it could be used by employee, admin and HR to manage and automate various operations in this system by decreasing the human's routine tasks with reduced error rate.

Keywords: OTP (One Time Password), HRM (Human Resource Management System), QR Code (Quick Response Code)

I. Introduction

In today's era smartphones are widely in usage among everyone which paves us the way of cost efficient system. This makes the system dynamic with the latest technologies to make it much easier in terms of implementation and installation. It is one of the simple ways of implement the attendance system, which makes it easier for employees to make the entry and exit time with the QR code scan by verifying the authentication of employee. The major advantage of the system is it reduces the deployment cost and the implementation is easier which performs the required tasks in a better way.

This system is to be implemented with simple implementation techniques that are to be compromised with high computation power. Some of the commonly used technologies are Bluetooth, Barcode Scanner, RFID, etc. In our project we use the QR Code scanner which can be one of widely used method of application development that is used with reduced cost and reduced complexity of implementation. This system automates the tasks which can be made manually and it automatically sends all the task details to the HR Manager and automated mail to employee regarding his/her progress.

The attendance management system module is to mark attendance with various forms of authentication such as by verifying the location which could be taken from the geo location, Employee QR Code carrying employee details in encrypted form and it is decrypted by the server side implementation and to check the phone number of authenticated person it is been given with a verification process that sends OTP (One Time Password) to the authenticated person's mobile number. In this employee management it gives the maintenance of the employee record with various employee management operations, such as leave management, attendance management, recruitment management, interview scheduling, etc.

II. Related approaches/work

In the attendance management system there are many approaches, which are with highly complicated implementation process. Some of the systems using biometric devices are being implemented with high implementation cost and these approaches are given below.

In [1], it allows the software installation in the mobile phone and the attendance is marked by enabling the Bluetooth option. In this system it makes the attendance process by storing the MAC address with the user's name. It gathers the MAC address of user and it makes the entry of attendance.

In [2], it makes the face detection algorithms to detect the faces of user while making entering and exiting. It detects the face and matches with the registered face by which the corresponding attendance of the user is made. But the authentication does not support the system with changes in the face for longtime.

In [3], it uses the biometric system with the fingerprint scanner to verify the user. In this system the fingerprints of the users are stored in the database. In the server side implementation it matches the fingerprint of the user and displays the information of the user such as user name for confirmation. After confirming the details, attendance is made along with the current time.

In [4], face recognition is used to identify the faces of registered user. It uses Eigen face methodology for recognizing the face of the users, by training the system with the dataset of the registered user face pictures. They are also failing to assure the long term recognition with minimized rate of error in real time computation with high security level.

In [5], "RFID based student monitoring and attendance tracking system". In many of the colleges there is a lack of management system of attendance and it is very difficult to maintain, store and retrieve records. So, here is one of the easier but expensive way of maintaining the records is with RFID. It tracks the attendance od students and faculties without its implementation. RFID Scanner is used to scan the code which is responsible to enter the login and login time of the user.

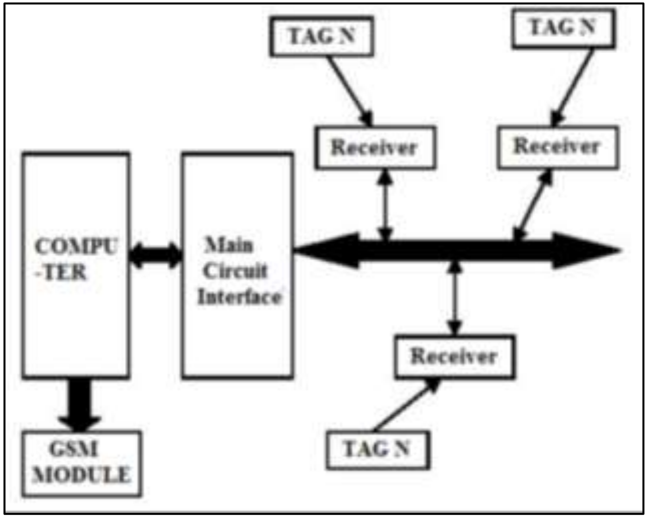


Fig. 2.1: RFID Attendance System

III. EXSISTING SYSTEM

In the existing systems the attendance is marked by means of biometrics such as finger print recognition which takes in higher deployment cost and implementation process. The other face recognition systems require higher end processing with complex implementation process. One of the major disadvantages of face recognition systems are they need to fed with input and trained frequently to adapt with the extended course of period in recognition.

Difficulties in existing attendance management system are given as follows,

- Lots of paperwork: Existing system requires lot of paper work. Loss of even a single register/record led to difficult situation because all the papers are needed to generate the reports.
- Time consuming: Every work is done manually so we cannot generate report in the middle of the session or as per the requirement because it is very time consuming.
- Manual control: All calculations to generate report is done manually so there is greater chance of errors.

IV. PROPOSED SYSTEM

A. *System Architecture*

Employee can get the QR Code after the confirmation of location and it can be used within the system to mark the entry and exit time of each and every employee. It gives automatic acquisition of employee timings and used to calculate the employee work hours. In the attendance management the employee has the QR Code this is generated only when his/her location matches with the given location in the system and after the verification of location the corresponding QR Code of the employee is generated in his phone. The QR Code is encrypted and decrypted with the RSA Cryptographic algorithm and it could be made in this system. The employee specific information is then decrypted and the employee details are obtained. Then the OTP is given to the registered phone number of the particular employee. This validates the verified user and the attendance is marked with the current timestamp.

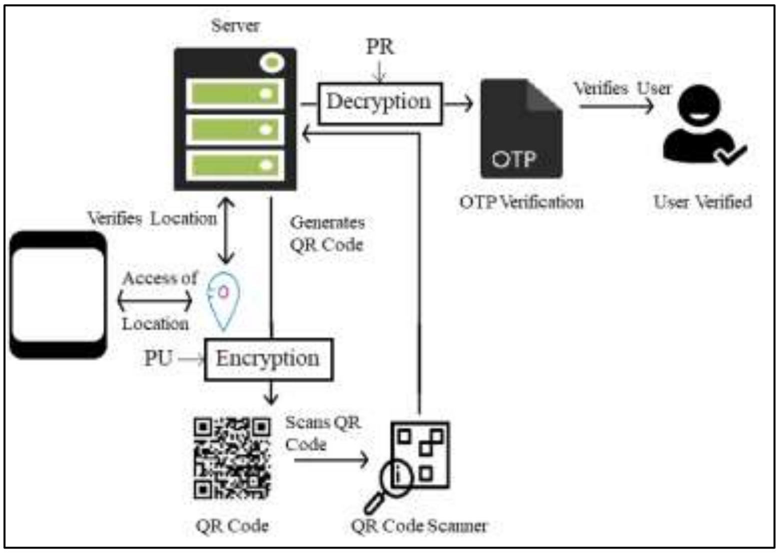


Fig. 4.1: System Architecture

B. Algorithm

The Algorithm used for encryption and decryption is RSA. It ensures that the user details are not retrieved by the middle man by enabling the secured way of processing the details.

1) RSA Algorithm (for Encryption and Decryption Process):

Choose two large primes p and q, $p! \leftarrow q$
Compute $n \leftarrow p*q$ and $\phi(n) \leftarrow (p-1)*(q-1)$
Choose an integer e with $\gcd(e, \phi(n)) \leftarrow 1$, $0<e<\phi(n)$.
Compute $d \equiv e -1 \pmod{\phi(n)}$.
Public key is $PU \leftarrow (n, e)$.
Private key is $PR \leftarrow (n, d)$.
Encryption function: $E(M) \leftarrow M^e \pmod{n}$, $M<n$.
Decryption function: $D(M) \leftarrow M^d \pmod{n}$, $0 \leq M<n$.

Employee can make attendance, in which the system checks for the corresponding location and generates the QR Code. This QR Code can be scanned in the scanner and it sends the OTP to their mobile number which has to be entered in the system to provide authentication. It is used to maintain leave records of employee, where the leave request is made by employee and system checks for valid request, which can be accepted by authorized official. After the decrypting process the system obtains the details of the employee in the process. To ensure the authentication of user an OTP is generated and send to the user. By entering the generated OTP in the system it authenticates the user and makes the user's attendance with the time. Thus managing the total work hours, it calculates the performance and maintains the attendance reports.

C. Location Verification

The location of the user is verified by taking the latitude and longitude points of current location and it is verified with the location of company. It is to ensure whether the user is in corresponding location or not.

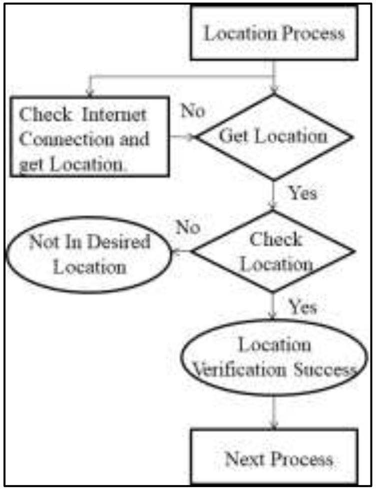


Fig. 4.2: Location Verification Process

The system makes use of the current user location, where it prompts for the location access during the process. The user can access the portal only when the location is enabled and when the system is able to access the location details with the access of geo-location. The location is obtained and the values as set with the user's latitude and longitude points. The default value is set as the location of place where attendance should be made within the given specific location. The values of latitude and longitude points are set with the default values of the client specific location. These values are generated by taking the latitude and longitude points explicitly by the administrator and are given in the system as the required location for the employee to get into further process.

2) *Algorithm for Distance Calculation (between two latitude and longitude points):*

```
Access ←Set with the default value as -1
Lat1←Set to default location's latitude point
Lon1←Set to default location's longitude point
Lat2←Obtain user Location's latitude point
Lon2←Ontain User Location's longitude point
function getDistanceBetweenPointsNew(lat1, lon1, lat2, lon2)
Theta←lon-lon2
distance←(sin(deg2rad(lat1)) * sin(deg2rad(lat2))) + (cos(deg2rad(lat1)) * cos(deg2rad(lat2)) * cos(deg2rad(theta)))
distance←acos(distance)
distance←rad2deg(distance)
distance←distance * 60 * 1.1515
Return intval(distance)
dist ←getDistanceBetweenPointsNew(lat1,lon1,lat2,lon2)
if(dist<=1000)
Access ←1
Else
Access ←0
```

The main idea of this is to obtain the distance between the employee logged in current location and the location of the client/company where the employee is supposed to be present. The distance is calculated between these two co-ordinates. If the distance is less than 200m then the employee is present within the location of the company. The system checks for this distance and if it is not within the specified distance then the location verification process will not be successful for the employee.

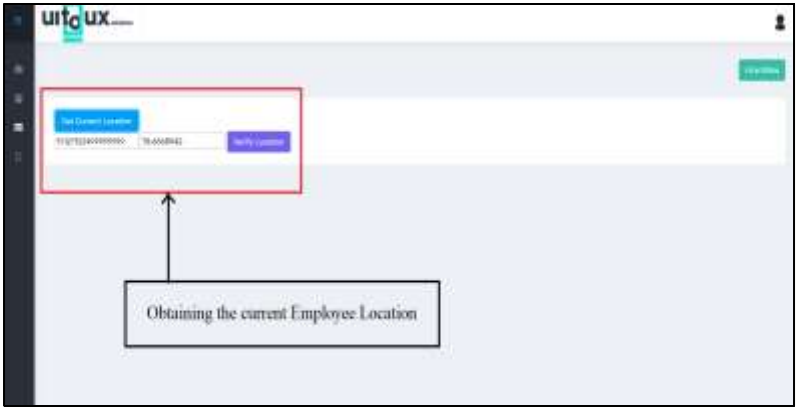
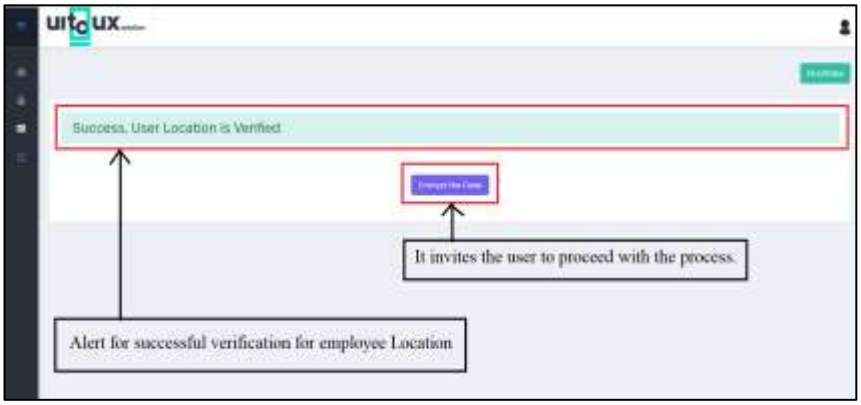


Fig. 4.3: Getting the Current User Location

In this module the location verification is implemented using the Haversine formula. The shortest distance between two points on a sphere using their latitudes and longitudes measured along the surface. Thus, the location of the user is verified by limiting to certain distance such as below specific distance that the client location holds with the system is taken and this distance is taken as required distance. The system after confirming that the user is within the specific location within the specific distance, the user is prompted with the success message stating that the location access is successful. This alert is given after performing various operations in which the location of the employee is taken and the distance between the company location and the employee location is computed with the haversine formula as specified above. The variable 'Access' is by default set the value as -1 and it is modified as 1 when the calculated distance is within the distance of the company. This distance is set explicitly and can be modified by the administrator of the system generating the default location of the system in the location access process.



Success, User Location is Verified

It invites the user to proceed with the process.

Alert for successful verification for employee Location

Fig. 4.4: Verifying User Location

D. Encryption Process

RSA algorithm is used for its asymmetric cryptography method. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private Key is kept private.

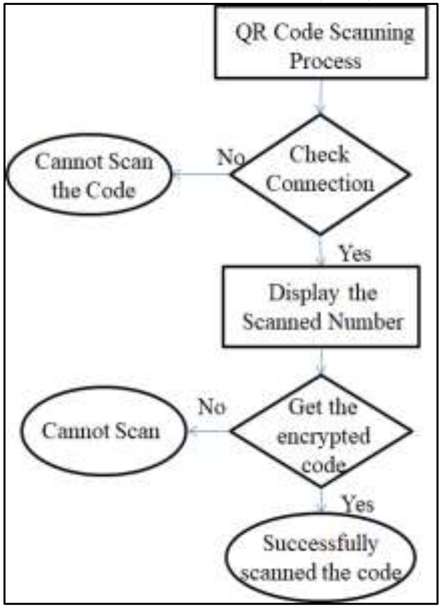
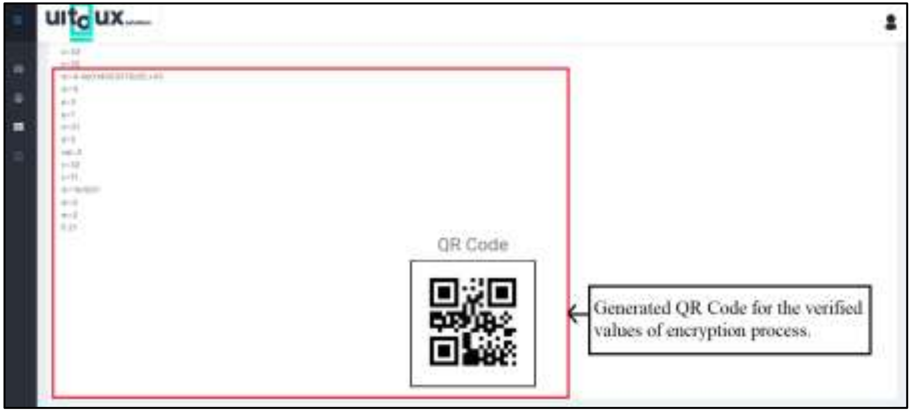


Fig. 4.5: Encryption Process

- A client (for example browser) sends its public key to the server and requests for some data.
- The server encrypts the data using client’s public key and sends the encrypted data.
- Client receives this data and decrypts it.



Generated QR Code for the verified values of encryption process.

Fig. 4.6: Encryption process running with p and q values for 3 and 7 with QR Code.

This encrypts the Plain text given as input and it generates the cipher text by storing the secret keys in the file systems.

E. *QR Code Generation*

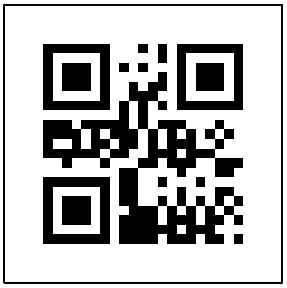


Fig. 4.7: Sample Generated QR Code in the system

QR Code is generated based on the employee login. The system checks for the authenticated employee during the logging process of the system. Employee can get the QR Code after the confirmation of location and it can be used within the system to mark the entry and exit time of each and every employee. It gives automatic acquisition of employee timings and used to calculate the employee work hours. The encryption process takes place with RSA Algorithm using the public secret key which is the given as the variable 'e' in the encryption process. This is later encrypted with the verification of user credentials. It checks for the user after verification with the encrypted code in the process. If the user is proved to be authenticated then the system generates the QR Code for the encrypted code that is being verified.

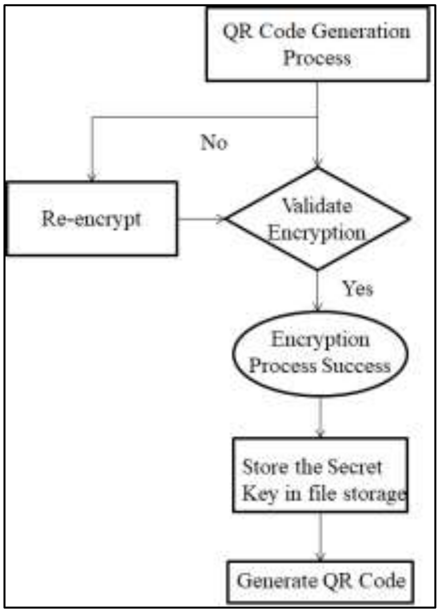

QR Code Generation Process
No
Re-encrypt
Validate Encryption
Yes
Encryption Process Success
Store the Secret Key in file storage
Generate QR Code

Fig. 4.8: QR Code Generation

This QR Code is saved in the temporary directory/ temporary location given for storing the QR Code of the logged in user. The user QR Code has the following advantages,

- It is secure, as it is encrypted with the RSA Encryption algorithm.
- It is encrypted with the random generated prime number and employee ID based random number.
- It ensures that reuse of the existing QR Code is not possible.
- Its secret keys are stored in the file systems to ensure the security of the system and accessing of keys.
- Regeneration of existing QR Code is not possible.
- Reuse of the existing QR Code is not applicable to access the system with the scanning process.
- QR Code is generated after the encryption process, by preserving the authenticity of the system.

F. *Decryption Process*

The Algorithm used for encryption and decryption is RSA. It ensures that the user details are not retrieved by the middle man by enabling the secured way of processing the details.

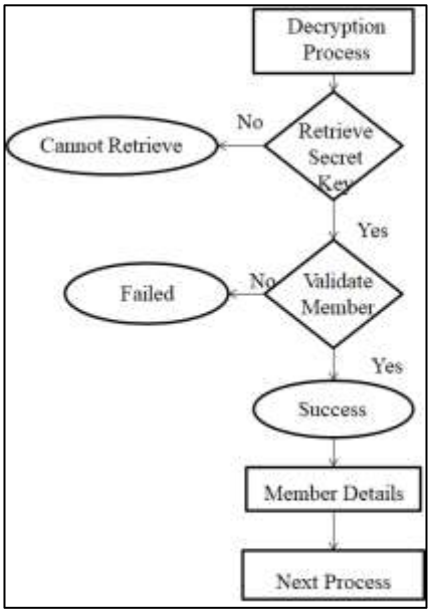
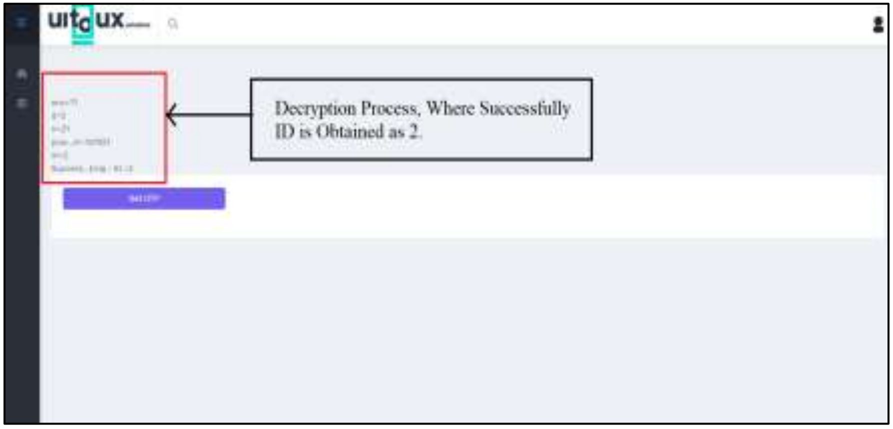


Fig. 4.9: Decryption Process

I) Decryption Key

Compute, d ≡ e −1 (mod ϕ (n)).

Considering the values which are verified for the encryption process, decryption occurs by storing the keys credentials in a separate file that cannot be accessed by the middle man. These values here are the decryption key and the ‘n’ value. As mentioned in the encryption process it is obtained as given below,



Decryption Process, Where Successfully ID is Obtained as 2.

Fig. 4.10: QR Code Decryption Process where it successfully rendered member ID.

User details are found valid with the verification of their authenticated phone number. This process authorizes to the final process of user detail verification. During the encryption process itself it is checked with the valid encryption id. It is done with the verification process by verifying the current status of the user with their ID. The process does not allow the users without appropriate credentials with the user data that is being given at the time of registration process. The QR Code decryption process is verified by the system at the client end itself before the generation of the QR code.

G. User Authentication

Employee can make attendance, in which the system checks for the corresponding location and generates the QR Code. This QR Code can be scanned in the scanner and it sends the OTP to their mobile number which has to be entered in the system to provide authentication.

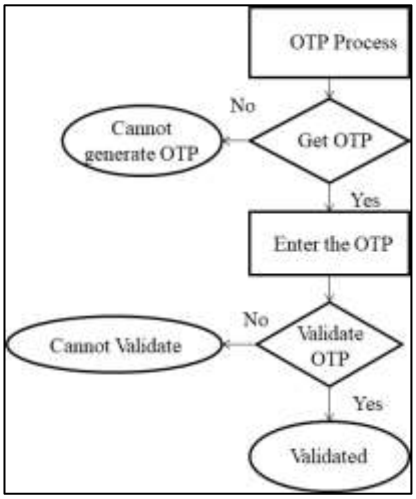


Fig. 4.11: OTP Generation Process

It is used to maintain leave records of employee, where the leave request is made by employee and system checks for valid request, which can be accepted by authorized official. An auto generated email for each official notification is given to concerned person, with the leave reports attached to it.

V. Conclusion and Future Work

Attendance is made easy through the encrypted QR Code scan, which verifies employee location and mobile number. This is the system that holds employee information with the permissions for HR Manager to view working hours of the employee in the database accordingly for each employee with respect to their punch in and punch out activities. The manual work of HR Manager is minimized with automation.

- This system can be made available with more efficient encryption and decryption process to increase the security.
- It can be integrated with cost efficient face detection system with technology up gradations to improve the process and its efficiency.

References

[1] Jamil, T.; Dept. of Electr. & Comput. Eng., Sultan Qaboos Univ., Al Khod, Oman, “Automatic attendance recording system using mobile telephone” , Telecommunications Forum (TELFOR), 2011.

[2] Shehu, V.; Contemporary Sci. & Technol., South East Eur. Univ., Tetovo, Macedonia ; Dika, A. , “Using real time computer vision algorithms in automatic attendance management systems”, Information Technology Interfaces (ITI), 32nd International Conference, pp. 397 – 402, 2010.

[3] Saraswat, Chitresh; Kumar, Amit, “An Efficient Automatic Attendance System using Fingerprint Verification Technique”, International Journal on Computer Science & Engineering, Vol. 2 Issue 2, pp. 264-269, 2010.

[4] N. Thillaiarasu, S. Chenthur Pandian, G. Naveen Balaji, R. M. Benitha Shierly, A. Divya, and G. Divya Prabha, “Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems”, Lecture Notes on Data Engineering and Communications Technologies, Book Series, Springer Nature Switzerland, Vol. 26, December 2018, DOI:10.1007/978-3-030-03146-6_175.

[5] Alagarsamy Gautami, G. Naveen Balaji, “A Homogenous Prototype Design for IED Detection Using Subsurface Ground-Penetrating RADAR”, Computational Vision and Bio-Engineering 2018 (ISMAC-CVB), Lecture Notes in Computational Vision and Biomechanics, Book Series, Springer Nature Switzerland, Vol. 30, December 2018, DOI:10.1007/978-3-030-00665-5_156

[6] B. Indhumathi, K. Ishwarya, K. Jamuna, G. Naveen Balaji & T. Prabhu, “Low Power and High Speed Carry Select Adder using Skip Logic”, International Journal for Innovative Research in Science & Technology, Vol. 5, No. 6, November 2018, pp: 58-62, ISSN : 2349-6010

[7] Qinghan Xiao; Interdept. Biometrics Working Group, Gov. of Canada, ON ; Xue Dong Yang, “A facial presence monitoring system for information security”, Computational Intelligence in Biometrics: Theory, Algorithms, and Applications, pp. 67-69, 2009.

[8] ChatratiSaiKrisha, Naidu Sumanth, C. Raghava Prasad, “RFID based student monitoring and attendance tracking system”, IEEE- 31661, 4th ICCCNT 2013 July 4-6, 2013.

[9] G.Naveen Balaji, V.Aathira, K. Ambhikavathi, S. Geethiga, R. Havin "Combinational Circuits Using Transmission Gate Logic for Power Optimization" International Research Journal of Engineering and Technology,Vol. 3, Issue 5 (May 2016) pp: 649-654, ISSN: 2395 -0056

[10] R. ArunSekar, G. Naveen Balaji, A. Gautami, B. Sivasankari “High Efficient Carry Skip Adder in various Multiplier Structures” Advances in Natural and Applied Sciences (Annexure II), Vol. 10 Issue 14 (Special) (Oct 2016) pp: 193-197, ISSN: 1995-0772

[11] M. Srinivasaperumal, K. Boopathi Raja, G. Naveen Balaji, E. Christina Dally “Concurrent Node Recovery From Failure In Wireless Sensor-Actor Networks” KARI Research Journal, Vol. 1 Issue 4 (Oct - Dec 2016) pp: 28-33, ISSN: 2456-6136

[12] Naveen Balaji, V. Narayanan,V.S. Nivash “Low Power and High performance JK Flip – Flop using 45 nm Technology” International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) Vol 3, Issue 10, October 2016, pp:26-29, ISSN: 2394-6849

[13] M. Srinivasaperumal, K. Boopathi Raja, G. Naveen Balaji, E. Christina Dally “Concurrent Node Recovery From Failure In Wireless Sensor-Actor Networks” Advances in Natural and Applied Sciences (Annexure II), Vol. 10 Issue 17 (Dec 2016) pp: 240-246, ISSN: 1995-0772

[14] G. Naveen Balaji, R. Prabha, E. Shanthini, J. Jayageetha, Mohand Lagha “Rapid low power Synchronous circuits using transmission gates” Advances in Natural and Applied Sciences (Annexure II), Vol. 10, Issue 17 (Dec 2016) pp: 287-291, ISSN: 1995-0772

[15] G. Naveen Balaji, S. Chenthur Pandian, D. Rajesh “Fast Test Pattern Generator using ATALANTA M 2.0” Asian Journal of Research in Social Sciences and Humanities (Annexure I) Vol. 7 No. 2 (Feb 2017) pp. 721-729 ISSN: 2249-7315 DOI: 10.5958/2249-7315.2017.00124.1