IMPROVING MOBILE SECURITY OF QR CODE ECOSYSTEM WITH PKI AND HASH ALGORITHM (REVIEW)

Harpreet Sandhu[1], Manpreet Kaur[2]
[1]Department of Computer Science & Engineering,
CT Institute of Technology & Research, Jalandhar, India
[2]Department of Computer Science & Information Technology, Doaba College
Jalandhar, India

Abstract

Significance of quick responses has been growing for the past few years because of its practical applications in mobile devices. These codes are very frequent in uses because they are easy to use and store more data. So generating quick responses is very smart idea. As according to digital life and business point of view QR codes gaining vast attraction. Because of the usage. They stored the data more as compare to bar codes because bar codes are one dimensional while QR codes are two dimensional. Quick response codes also increase the security of mobile phones due to of hidden information in it. Usage of mobile phones increases vastly. Therefore security of these devices is also very important. If this security achieved by concatenation of PKI(Public Key Infrastructure) and hash algorithm than the data used for encoding and decoding in quick response code is very much secured. In this paper we includes the information about QR codes, public key encryption and hash algorithms to increase the security of mobile phones.

Keywords: QR codes, PKI, Hash algorithm, RSA,SHA-1.

I. INTRODUCTION

A. QR codes first developed by Denso-Wave patented in 1994. Denso-Wave Patented designed software (quick response code) which is read or scanned by camera. The data encoded in these codes according to ISO/IEC 18004:2006. Basically they are in black and white colors with white background and blacks dots which are in square form. Also there are colored QR codes which stored more data instead of black and white due to their RGB (red, green, blue) property. These codes are not in black/white and red/green/blue color, also there are some light color QR codes. Quick response codes are portable and handy. They stored data in two dimensions about 3000 characters. The wide usage of these codes is in digital area. Because these codes support PNG, JPG/JPEG, GIF, SVG, EPS, PDF files. The interesting thing about these codes is that there are different QR codes for same content or data because there are total 8 possible masks for single data which guidance the pattern. There are many properties of these codes like high capacity upto-7089 numeric digits. They are damage resistant and have high speed reading. They are small print out size and also 360 degree reading capacity. They are flexible in structure and applications. These QR gaining lots of applications in many fields like Retailing, Warehousing, Organizations, Health care, life sciences, Transportation, Office automation and also in Advertising area. There are five steps in life cycle of QR codes:- Encoding, Distribution, decoding, Action and Decommission. Encoding means to change the bits of data but it is much similar to the original data. This encoded data tough to detect. Distribution explains the third party modified information or QR codes. Decoding means to restore the original information and encoded data back to its original form. Action means task done by decoded machines. Decommission means to remove from active services .this will help to reduce the security risk.

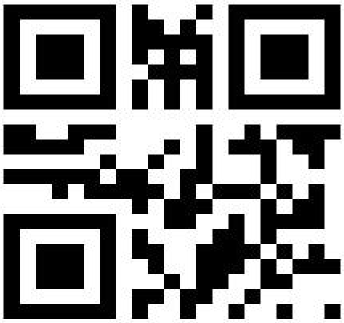

Fig. 1 QR code of any data

B. PKI (Public Key Infrastructure) includes policies, processes, server platforms, software's, and workstations which are used for conducting certificates and public key pairs which include the ability to issue, manage, and revoke public key certificates. This public key encryption is asymmetric algorithm. This encryption includes 6 main steps:- 1-Plaintext, 2- Encryption algorithm, 3- Public and private keys, 4- Cipher text, 5- Decryption algorithm. Where plain text is simply a message or any data which sender wants to be send to receiver node. Encryption algorithm is a technique to use the covert data into another form or we can say secured(secret) from. Private keys are used by both sender and receiver to secret their message and also private keys encryption are called as symmetric key encryptions. Whereas public keys are used to decrypt your encrypted data but also these keys are used to encrypt the data. Cipher text is a text which is received from encryption algorithm and is converted data which is converted from plain text. Similarly decryption algorithm is a technique which is used by receiver to convert that cipher text into plain text so that it becomes readable and under stable. In public key encryptions there are 2 keys (pair of keys) used first is to encrypt the data at sender side while other is used at receiver side to decrypt that data. Basically public key encryptions are used to secure the data and protect from third party nodes. Because in this case the malicious Nodes or Attackers are failed to detect the private and public keys. These encryption techniques maintain the confidentiality and authenticity. These cryptographic algorithms based on mathematical operations like integer factorization and discrete logarithms. There are many types of Public Key Encryption Algorithms:- RSA (Rivest-Shamir Adleman) algorithm, ECC(Elliptic curve cryptography). RSA used to secure the sensitive data. In RSA the integers are used from 0 to n-1 but also for some n. But basically the standard value for this is 1024 bits. Therefore the value of n should be less than 21024. Thus security of this RSA is also very important. To secure this algorithm basic attacks are which are there which can attack to destroy this algorithm. Like Brute force attack, Mathematical attacks, Timing attack, Hardware fault-based attack, Chosen cipher text attack.

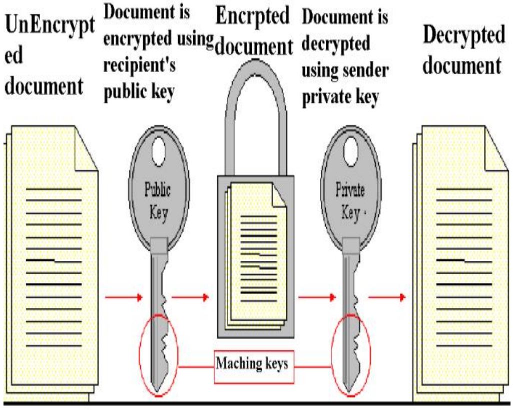
UnEncrypt ed document
Document is encrypted using recipient's public key
Encrpted document
Document is decrypted using sender private key
Decrypted document
Public Key
Private Key ·
Maching keys

Fig. 2 Public key Encryption

C. Hash algorithms and Hash functions provide message authentication which helps to maintain a security of message. They are denoted by H. These H are variable lengths. When they concatenate with message (M) which are fixed length. Then it becomes h=H (M) where h is the Hash. There are many applications of this hash function like Message Authentication, Digital Signatures, One-way password file, Intrusion Detection, Pseudo Random Function (PRF) these hash functions are used as SHA (Secured Hash Algorithm). They are like SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. There numeric shows the no of bits that areused in algorithms. SHA was developed by National Institute of Standard and Technology (NIST) and published as federal information processing standard (FIPS180) in 1993. The hash functions accept the value from message and convert it into fixed length and also add some bits to the end if necessary. Cryptanalysis of hash functions are resolve the problem of collision that's why they are also called as collision resistant. These Cryptanalysis works on internal structure of message. These Hashes which are produce from hash functions are maintain the integrity as well as authentication.

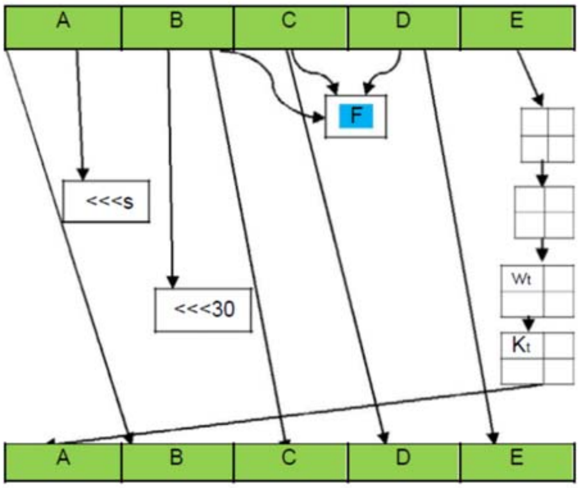

Fig. 3 Hash Algorithm

D. Security in QR codes: Security of QR codes is big issue because they hide the information in dots so it is tough to give more security to these. But this security is possible in many ways like providing Steganography and Cryptography. By applying Encryption/decryption technique we achieve larger security. There are many malicious QR codes which look like the same but they harm the security. Similarly there are some intended users who are unable to detect these types off attacks. Attacks possible only in case of malicious cases. There are many ways which gives the security to these codes as like by providing tracing codes, by authentication methods, by securing the information, by providing benefits in digital education system, by using AES and DES, security against malicious codes, by embedding encrypted techniques etc.

II. OBJECTIVES OF PAPER

The objective of the paper is to design a technique to invalidate any malicious attack on the mobile phone information with the help of malicious QR codes, which is done by the help of PKI and Hash Algorithms. Further objectives are summarized below:

1. Basic functionality of QR code life cycle.
2. Exploring the security in quick responses.
3. Study the working of mobile phone applications, public key cryptography, hash algorithms.
4. Explore the security issues related to Malicious QR code attacks.
5. Develop an android phone app to read and scan Quick Response codes with the secured data which is get from PKI and Hash algorithm as output.
6. Testing the proposed Idea through simulation.

III. LITERATURE REVIEW

In this paper [1] the author explains life cycle of QR codes which resolve the security issues. With this scheme security risk is decreased. In this scheme two main steps meanwhile in first step firstly the message pass to valid date then apply algorithms(Public Key Algorithms) and then passed to certificates after that at last the signature is generated. Message- that could be any text. Valid Date- this is a date at which message is valid. Algorithms- these includes all the public key algorithms. Certificate- these certificates are related to information and certified by public key of QR code issuer. Signature- the encrypted data using public key. In second step three operations are played. In this paper [1] they discuss about life cycle of QR codes.

1. Message - that could be any text.
2. Valid Date- this is a date at which message is valid.
3. Algorithms - these includes all the public key algorithms.
4. Certificate- these certificates are related to information
5. Signature - the encrypted data using public key.

2) In this paper [2] which explains that there are many applications in our mobiles that does not need any security. This paper explains the literature review of different papers on mobile security. It explains that certain applications are not come under mobile authenticity. But when we install them they tell us that accept certain terms and conditions which are not necessary. They summarized their literature study in 5 main steps which explains the authentications (Keystroke Based, Gate Based, Touch Based, and Device Sensor Based Behavioral Profiling Based). This paper also indicates the future work in which they want to tell that how to categories these application of mobile according to their sensitivity level.

3) This paper [3] explains the different applications of QR codes and compares them

with Bar codes. This is a survey paper. Like Capacity, Durability, Speed, Space and Language supported. It explains the different colors of QR codes difference between QRC and SQRC where QRC are quick response codes and SQRC are secured quick response codes. When compare the properties of QRC and SQRC like capacity, durability, security, readability then it is found that SQRC is more efficient and secured than QRC.

Table no: 1 Comparison between QR code, Bar code and SQR source:-[3]

Features	QR code	Bar code	SQRC
Data Capacity	Up to 7089 numeric digit	10-20 digits	7089 numeric digit
Security Function	No	No	Yes
Durability	Yes (max 30%)	No	Yes (max 30%)
Readability	Yes	No	Yes
Language Supported	Numeric, alphanumeric , Eric, kanji, kana	Numeric, alphanumeric	Numeric, alphanumeric, kanji, kana

4) This paper [4] explains the basic features of QR codes and Proxy Re-Encryption. Well Proxy Re-Encryption is nothing it is same as encryption done on any message. Transform information is secured with QR codes but this Proxy Re-encryption helps to maintain double security on that information because it is very hard to detect that what message is converted into cipher text. It explains that Bar codes are stored the information in one directional that's they are known as one dimension but QR codes save the information in two directions (from left to right and from bottom to top). These Quick Response codes contains the following six main steps –

1. Information investigation analyses those information.
2. Information encoding methods will encode the information.
3. Error correction coding means to check the error.
4. Structure final message means design the final message.
5. Module placement in matrix means placed the modules.
6. Data masking means prepare a mask to cover that data.
7. Format and Version information explains the version.

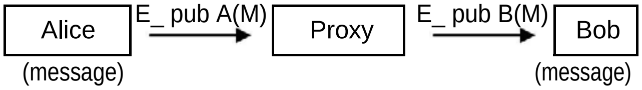

Fig. 4 Proxy Re-Encryption(Public key Encryption). source:-[4]

5) This paper [5] focuses on the security of some usable applications from malicious codes. These Malicious QR codes are big problem. Because they are hard to detect and resolve. Malicious codes are very much same as like original codes that's they are hard to detect. But the main motive of attacker or malicious codes are to destroy the security of data. They covered the following terms in their paper Modification and Detection, Website Analysis, URI Display. Modification means to modify the data into another form. Website analysis means to check the local website that runs on browser. URI display means to secure the display of social site link. In this paper they detect that Usage of these QR codes are resolve the problem of external communication, User Tracking, and Location data. Any communication does not need any external data like messages and images of mobile phone. Similarly in user tracking there is no need of any user appearance. In the conclusion of this message the author properly defined that original QR codes does not need above information of particular User. If any app or QR code ask you to tell these information's than defiantly that code is malicious code.

6) In this paper [6] the author explains the capacity of storage in QR code. They invent new algorithm which increase the capacity of these codes and named as compression algorithm. After that they apply multiplexing on bits of data which increase more capacity of Quick response codes.

In Compression algorithm there are total 5 steps.

1. The text is converted into ASCII values.
2. Convert these ASCII values into binary.
3. Apply zip compression on these binary digits.
4. Take this compressed data.
5. Last step is to collect the data.

Afterwards, Second algorithm is Multiplexing algorithm.

1. Take simple any QR code.
2. Multiplex 5 QR codes and take as input than generate single output.

3. Collect that single QR code.
4. Than stop the algorithm.

As future work we can consider the message as audio and video for applying compression algorithm.

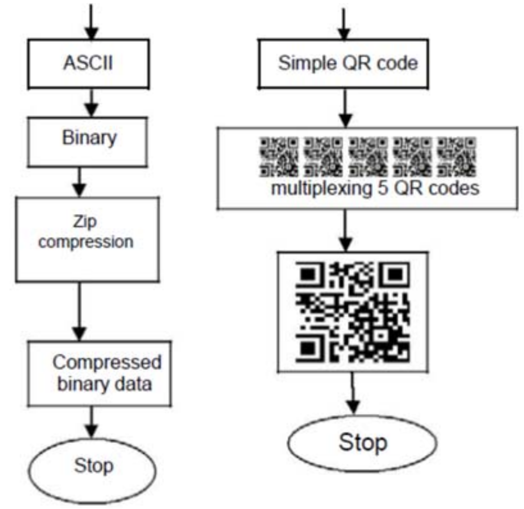

Fig. 5 Compression algorithm and multiplexing. source[6]

7) In this paper[7] the author explains the capacity and efficiency of color QR codes. The simple 2d structure of QR codes contains two main parts function pattern and encoding region. But the author used HSV in his model. This HSV is Hue, Saturation and Value where Hue explains the no of colors from 00 to 360 0 , Color explains the range of color like red start from 00 and so on, Similarly saturation explains the amount of gray in all colors. Here value depicts the brightness of any color. In black/white where the color capacity of 100 modules, but in color ones that capacity may be 360 particles.

Table no: 2 Color QR codes with HSV. source[7]

Image	Device	Source	Accuracy (%)
	Mobile device(android)	Camera	75
	Personal computer	File	100
	Mobile device(android)	Camera	100
	Personal computer	File	100

8) In this paper [8] the author explains the security of Steganography with using QR codes and encryption techniques. The word Steganography depicts the image processing. The author given two models first for sender and another for receiver. These steps increase the security very well because it is very hard to detect these encrypted data's and also quick responses for that.

The model for sender side in this paper having 6 steps:

1. Is taking any message.
2. Is encrypted that message with the help of AES-128.
3. Is converted that encrypted data into QR code which means encoding is done at here.
4. Is scramble that encoded data into any form so that security increases
5. Is hide most significant bit (MSB) with least significant bit (LSB).
6. Is creating a stego-image with this secured data.

Similarly, the model for receiver side is also having 6 steps.

1. Is taking that stego-image from sender.
2. Is extracting the original image from stego-image.
3. Is descrambling that image into original.
4. Is scanning the QR code.
5. Is decryption which means using AES-128 message will be decrypted
6. Is collecting the original message. At the end the author also given some indications for future work like there may be security enhanced with adding some modification in modules.

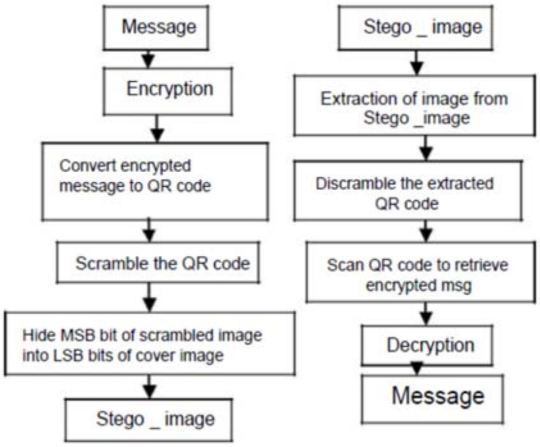
Message
Encryption
Convert encrypted message to QR code
Scramble the QR code
Hide MSB bit of scrambled image into LSB bits of cover image
Stego _ image
Stego _ image
Extraction of image from Stego _image
Discramble the extracted QR code
Scan QR code to retrieve encrypted msg
Decryption
Message

Fig. 6 Algorithm for sender and receiver side. source[8]

9) This paper [9] is on public key encryption with using of standard of PKI. The author explains a sender and receiver share their data with using of secret sharing key which is very much insecure. That's why author purposed a model in which first step is to generate personal signature of sender. After that generate a hash function of that personal signature of sender. After that using secret key of that function generate a new function, which is consider as a second part of signature. Then comparison is done if the both values are same then receiver take as original message otherwise it will be consider as message send by malicious node.

10) In this paper [10] the author reviews the different SHA algorithms. SHA means secured hash algorithm. SHA is a hash function but it is secured form. There are SHA-0, SHA-1, SHA-2224, SHA-256, SHA-384, and SHA-512. Author firstly makes comparison between these algorithms after that give a purposed model. This purposed model explains the efficiency, time consuming, amount, collision and bit wise operations of these algorithms. In SHA-0 there are many shortcomings, therefore SHA-1 come in market. In SHA-1 error correction is there with simple one bit wise rotation. After that SHA-224,256,384 and 512 were launched. In end author gives his profile.

11) In this paper [11] author with desktop applications which deals with the question paper they proposed a technique which uses AES for question paper Encryption and Decryption is done with the help of DES. Furthermore, Author tried to reduce the memory storage by redirecting to a webpage by the transmission and online acceptance of data. This paper research is very helpful for large organizations and companies.

IV. PUPOSED MODEL

In this section we are discussing about the methodology in such way that reader should understand that in what way the author design his research implementation. Purposed model is simply author's analysis regarding research, motivation in research, significance of research, research process and hypothesis. Research analysis is study of different papers and books that author completed to define his new research topic. Motivation in research is simply the work efficiency that has to complete your work. Significance of Research is usage and effectiveness of your work Hypothesis is simply mean by your expectation from research. Due to this point the reader should clear and get detailed knowledge about author's research plan. Discussing about your work into well format either it is flow chart or it is pseudo code. Make points of research and implementation into the particular format.

- ❖ At sender side firstly take original message which may be any text and alphabets. Than in second step converted it into ASCII value just for data security.
  After that apply PKI which may be RSA or ECC and Hash Algorithm any Secured Hash Algorithm for data authentication and confidentiality. Afterwards take that encrypted data as a input and encoded it with programming in Android Studio. Last step of sender side is to take that input and generate a QR code in android studio.
- ❖ Similarly, at receiver side firstly take encoded data(QR code) and converted it into decoded form(Scanned QR code). After that decrypt with applying PKI and Hash Algorithm for converting it into ASCII value. Afterwards take that ASCII value which is found from decrypted data and converted it into original message. Hence Encryption/Decryption takes place.

Pseudo code for sender side algorithm:

```
Step 1: Take simple message text.
Step 2: Converted above message into ASCII code.
Step 3: Applying PKI (RSA) on ASCII code (encryption done).
Step 4: Applying Hash algorithm (SHA-1) on encrypted message.
Step 5: Generating QR code with above hash produced (encoding done).
Step 6: Stop.
```

Message could be any text or alphabet. PKI technique may be RSA or ECC. Hash algorithm is SHA-1 and afterward generating QR code with the help of coding done in android studio. Generated Quick response code taken as final output data from sender side.

Pseudo code for receiver side algorithm:

```
Step 1: Take encoded message from sender and scan it (decoding done).
Step 2: Matching the message with above hash.
```

Step 3: Decrypt the message with RSA (decryption done).
Step 4: Found ASCII value.
Step 5: Converted into original text.
Step 6: Stop.

PKI and Hash Algorithms are used to achieved data authentication and confidentiality. Afterwards, use android studio to design the application with above input.

V. IMPLEMENTATION IN ANDROID STUDIO

For Implementation and for my complete research work, we are using Android studio. Android studio is a tool used for programming and creation of android phones applications. As my topic is security in android phones so this tool is very much effective for output and throughput. As we know Java language is base of Android studio so Java language is also used to complete this research. Programs of PKI and Hash algorithms are also taken in Java language.

In addition, Android studio supports java language so if we encrypt and decrypt our message in java programming than it should increase the efficiency of our work. When we design our android application we used that encrypted data which increases the data authentication, confidentiality and Authorization.

As studied the research paper on QR codes, mobile security, public key infrastructure and hash algorithms the net conclusion is found that secure data transformation is the main key feature which is noticeable point. But all the paper taken the simple alphabetic text as input to encode in the formation of QR codes. Android studio helps to take Android application that input easily and encode it into a QR code formation.

VI. FUTURE DIRECTION

After Studying all above papers it is clearly confirm that there are many more options to do work to increase the security of QR codes. Because these codes hide lots of information which is not easily readable. In future work we can design an algorithm which contains the any cryptographic techniques along with Steganography techniques. Also we can increase the storage space of these codes using with some algorithms.

VII. CONCLUSION

Storage data with QR codes is very much effective because it appears only black and white dots but under them store lots of secret data so security of these codes is also very important. If this security increases with some cryptography algorithms then there must be data security achieved. In this paper we will increase security in quick responses using PKI and Hashing technique. Then usage of these secured QR codes the mobile ecosystem is also effected in good manner and with all steps this purposed technique also increased the efficiency, integrity, authentication, confidently and TTL (time to live) value too.

REFRENCES

[1] L. Roger Yin Dept. of Information Technology and Supply Chain Management University of Wisconsin-Whitewater Whitewater, WI 53190 USA yinl@uww.edu. Jiazhen Zhou Department of Computer Science University of Wisconsin-Whitewater Whitewater, WI 53190 USA zhouj@uww.edu. Maxwell K. Hsu Department of Marketing University of Wisconsin-Whitewater Whitewater, WI 53190 USA hsum@uww.edu I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.(2015)

[2] Saud Alotaibi1, Steven Furnell1, 2 and Nathan Clarke1, 2 1Centre for Security, Communications and Network Research Plymouth University Plymouth, UK 2Security Research Institute Edith Cowan University Perth, Western Australia.saud.alotaibi, steven.furnell,nathan.clarke.@plymout h.ac.uk.(2015)

[3] K.Saranya, Assistant Professor-I Department of Computer Science and Engineeering Kumaraguru College of Technology Coimbatore, Tamilnadu saranya.k.cse@kct.ac.in. R.S.Reminaa, Student Department of Computer Science and Engineeering Kumaraguru College of Technology Coimbatore, Tamilnadu reminasukumar@gmail.com.

S.Subhitsha, Student Department of Computer Science and Engineeering Kumaraguru College of Technology Coimbatore, Tamilnadu subhitsha96@gmail.com.(2016)

[4] Akhil N.V, Athira Vijay, Deepa S Kumar. Department of CSE College of Engineering ,Manuuar kerala India. akhilnambiyath54@gmail.com, athiravknair@gmail.com, deepamsk@gmail.com.(2016)

[5] Katharina Krombholz∗, Peter Fr¨uhwirt∗, Thomas Rieder†, Ioannis Kapsalis‡, Johanna Ullrich∗ and Edgar Weippl∗ ∗SBA Research, Vienna, Austria Email: kkrombholz,pfr¨uhwirt,jullrich,eweippl@sba-research.org
†Vienna University of Technology, Austria Email: thomas@rieder.io ‡Aalto University, Helsinki, Finland E-Mail: ioannis.kapsalis@aalto.(2015)

[6] Mona M Umaria Department of Computer engineering and Technology Parul Institute of Engineering and Technology Vadodara, India. G.B Jethava Department of Information and Technology Parul Institute of Engineering and Technology Vadodara, India.(2015)

[7] NutchanadTaveerad Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand e-mail: nutchanad.t@student.chula.ac.th. Sartid Vongpradhip Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand e-mail: vsartid@chula.ac.th.(2015)

[8] B Karthikeyan SASTRA University Thanjavur-613401, India. Abhilash Choudary Kosaraju SASTRA University Thanjavur-613401, India. Sudeep Gupta S SASTRA University Thanjavur-613401, India.(2016)

[9] Nikolay Moldovyan1 , Androy Berezin,2 Anatoly Kornienko3, Alexander Moldovyan4, 1Saint Petersburg Electro technical University "LEIT", 2Petersburg State Transport University, 4ITMO University st. Petersburg, Russian Federation. nmold@mail.ru, pgups, maa1305}@yandex.ru

[10] Priyanka Vadhera1, Bhumika Lall2, 1, 2Department of Computer Science B.S. Anangpuria Institute of Technology and Management, India.(2012)

[11] Partiksha Mittra , Nitin Rakesh Department of Computer Science and Engineering Amity University Uttar Pradesh Noida, India pratikshamittra@gmail.com , nitin.rakesh@gmail.com