

Mobile based Anti-Phishing System using Secure QR Code

Amar Bhegade

Department of Computer Engineering,
MESCOE,
SPPU, Pune, Maharashtra, India 411007

Saurabh Shinde

Department of Computer Engineering,
MESCOE,
SPPU, Pune, Maharashtra, India 411007

Anita Salve

Department of Computer Engineering,
MESCOE,
SPPU, Pune, Maharashtra, India 411007

Chitra Bhosale

Department of Computer Engineering,
MESCOE,
SPPU, Pune, Maharashtra, India 411007

Prof. Shalaka Deore

Department of Computer Engineering,
MESCOE,
SPPU, Pune, Maharashtra, India 411007

Abstract— As the Internet era is increasing now a day results in developing of information and communication technology. As the result of this users are using online facilities for the different purpose like banking transaction. Due to this, protecting sensitive information from malwares or web phishing is becoming difficult from attackers. Using only the username and password for authentication and security is not sufficient to protect our data. Attackers can collect personal information from computer infection or web phishing. Therefore this requires more advanced version of security mechanism. In this paper, we propose the prevention from web phishing by using secure QR code as Anti-Phishing mechanism.

Keywords— *QR code, Secure Communication, Mobile Authentication, Anti-Phishing, Two factor authentication.*

I. INTRODUCTION

The glory of internet and its advantages are highly being marked by the disadvantages associated with it. The main issue is Internet vulnerability which is leading to data modification and data thefts. There could be various types of phishing attacks which are causing insecurity to internet. Internet is widely used information infrastructure and insecure channel for exchanging information. Attackers are all too familiar with the fact that traditional security methods do not stop attacks against Web Application that are, developed to allow users to access data that drives the Website. By exploiting simple vulnerabilities in Web Application, an attacker can go through the security even when the traditional firewall and ID systems are in place to prevent the application. Web application need to transfer content from web application to the server site, which makes the websites vulnerable to various types of phishing attacks.

It looks obvious that any online service that has target to be secure nowdays should seriously consider implementing a powerful authentication method. This system mainly represents the design and implementation of QR code, an open source, proof of concept authentication system that uses a two level authentication by combining a camera-equipped smartphone and password which acts as an authentication device. QR code is secure as all the personal information transmitted and stored is encrypted, and it is also a cost efficient solution and that too easy to use. QR code is portable and can be used securely in suspicious computer.

II. QR CODE

In 2002, Clarke et al. was the first who has suggested the usage of camera-based devices as a most secured authentication method for critical and confidential transaction such as banking transaction and when connecting from untrusted computers. In 1994, the Japanese company 'Denso-Wave' has invented a QR code i.e. Quick Response Code.

QR code are two dimensional barcodes, that have ability to read from any direction in 360, it can store up to 4,296 alphanumeric characters, which is more than the 20 digits that the traditional barcode can store. It is easy to read even they are partially damaged and they are easy and quick to read with a camera-based device. QR codes have a feature called versatility that has made them quiet popular among some industries. On the other side QR code are only understood by machines and not by human beings. This states that scanning the QR code include some issues like user doesn't really know what is behind the QR code, so user might be scanning malicious code.

III. RELATED WORK

This Section represents an overview of related papers and techniques used in those papers.

Shoji Shakurai and Shinobu Ushirozawa[1], "Input Method against Trojan Horse and Replay Attack" Proposed a new interactive input method of sensitive information such as credit card numbers and account numbers against Man In the Middle attacks. This method takes decision about the input value that user puts using GUI with two or more cursor which to different direction at a time. Then the user fills the details rely on shared secret between the user and a server and moves one of the cursor from shared secret to the input value, and server changes the cursors' position at which the user cursors points and asks the question about the value. The server takes decision about user's input value though the response from the question. This method is strong and does not give any hint about which cursor is used to the attacker unless both the user and the server releases the shared value and the input value.

Raed M. Bani-Hani, Yarub A. Wahsheh, Mohammad B. Al-Sarhan[2], "Secure QR Code System" has proposed a system which is implemented and tested by using mobile phone based on android application. The system generates the QR code that can be used in terms of objects tracking. Executing suspicious code, attacking on users' personal details and violating user's identity and privacy theft are some important security risks that a user might be subject to in the background while user is just reading the QR code in the

foreground. In this paper [2], a security system for QR codes that guarantees both generators and users security concerns is implemented. The system is backward compatible with ongoing standard used for QR code encoding. The system is developed and tested using mobile phone based on android by using android application. It was found that the system has a burden of the delay required for verification of integrity and validation of content.

IV. ALGORITHM DETAILS

A. AES Algorithm

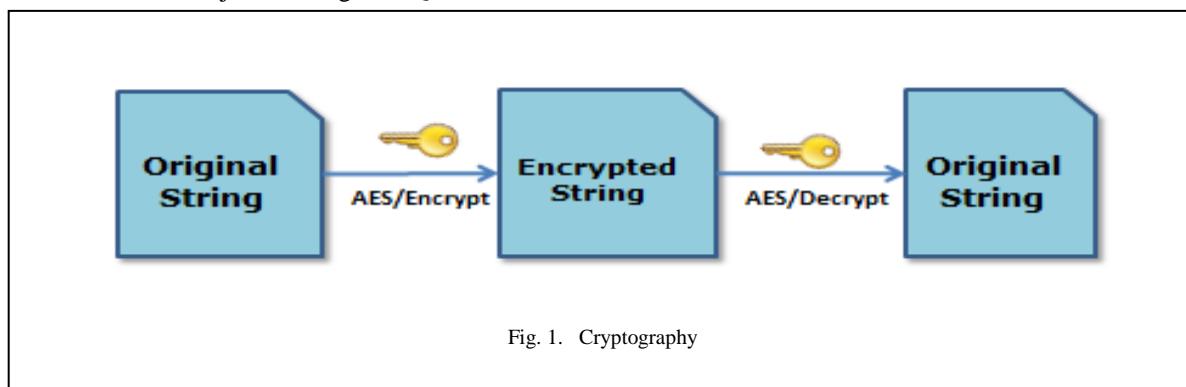
AES stands for Advanced Encryption System is based on principle known as substitution-permutation network, and it is very fast in both hardware and software. AES operates on 4*4 matrixes which is column –major order matrix of bytes, term the state. Most AES calculation is done in special finite field.

We use 128 bit key for an AES encryption which convert the input, known as Plain text, into the output, called the Cipher text.

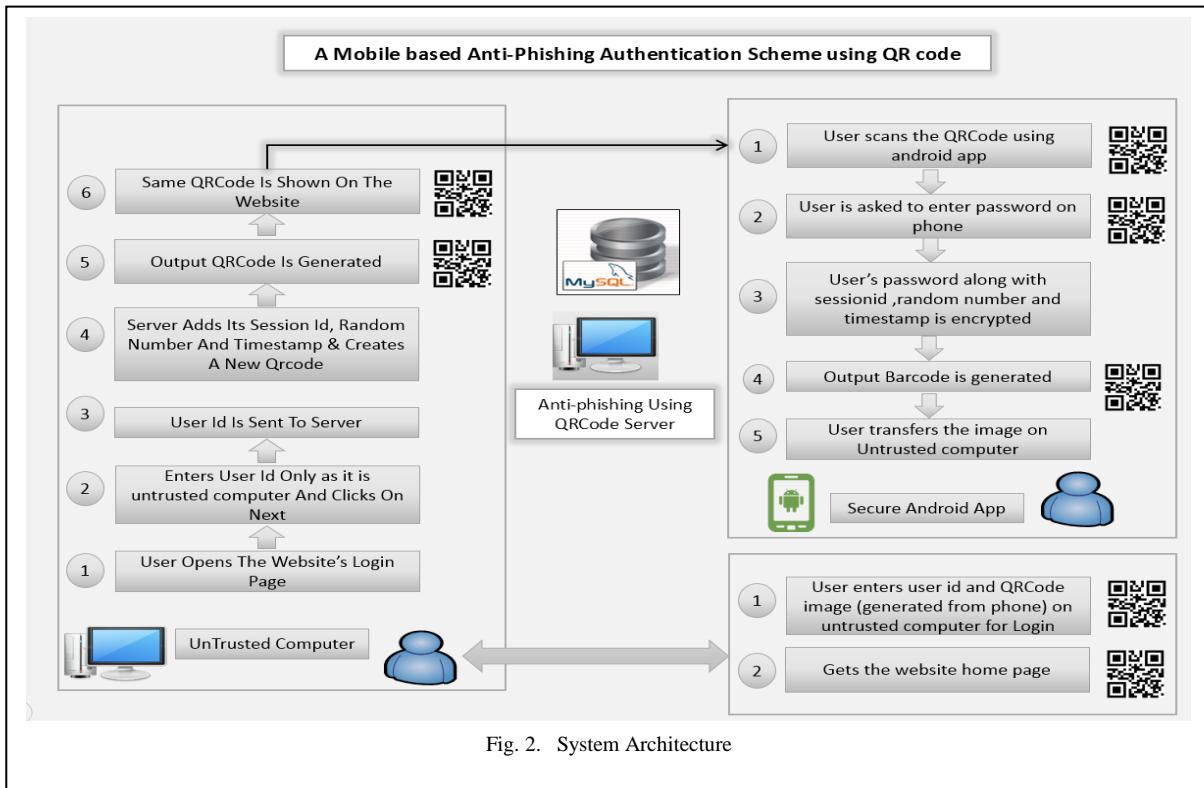
Step 1: Sender Encrypts plain text message by using AES Algorithm into cipher text using Secret Key.

Step 2: Sender sends cipher text to Receiver.

Step 3: After Receiving Cipher text Receiver decrypts the Cipher text into plain text using same secret key.



V. PROPOSED SYSTEM



A. Registration on local computer

- User accesses website through local PC.
- User enters User ID and click on submit button.
- Users ID save on web server.

B. Server Verification

- Server verifies user Information
- Server provides QR code with session ID, Random Number and Timestamp to user.
- If verification phase request is invalid and session abort.

C. Information Exchange

- Generated QR Code shown on Website.
- User scans the QR Code through Android mobile phone and access data using Shared Secret Key.
- Once QR Code scan by mobile device then user is asked to enter password on phone.

D. Login

- When user enter password on Mobile phone then new QR Code is generated with Session ID, Random no, Timestamp.
- QR Code is converted into image then user transfer image to local computer through webcam.
- Server verifies the password.
- Then user gets Successful login.

VI. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

Most of the existing system uses a common login technique for banking transaction which is not too much safe as the attackers becoming intelligent in growing internet world. Common login technique just need to put login ID and password which could be fetch by attacker. There could be a fake website on which user can try to login and provides his/her personal information to the attacker through fake website which can be harmful to user and user can lost his/her valuable money. But the proposed system is not having general login method because the proposed system is introducing secure QR Code technique for successful login. The main advantage of proposed system is that user need not have to put the password on local system instead user enters the password on to android based smart phone.

Because of this facility there is no chance for attacker to fetch the sensitive information of user. There are some existing system which uses QR Code which are backward compatible with ongoing standard used for encoding of QR code. This system might have burden of verification of integrity and verification of content. Instead the proposed system is faster than existing system as the user just need to put user ID without entering much more details and server just need to verify user ID and generate QR code with some constraints like session ID, Random number, Timestamp. The proposed system provides two level security by generating two QR Codes one at server which shows it on website and another is on user's smart phone which need to transfer it to server by using Advanced Encryption System Algorithm.

VII. CONCLUSION

In this paper, We proposed a mobile based anti-phishing technique to provide higher level security to the user by using secure QR code. Nowadays, User can access the data from various website through different local computer but that data is not secure because there could be a fake website. In this paper we have proposed the Two Level Security by generating two QR codes one on website and another on user's mobile phone. Attacker cannot obtain the user's personal information because user data is encrypted in mobile device. Server can check the User's authentication information on computer and mobile device. Only authorized user with password can login and retrieve the secret data. Our main aim of developing technology is to provide scalability, flexibility for secure communication between mobile device and untrusted computer

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on 'MOBILE BASED ANTI-PHISHING SYSTEM USING SECURE OE CODE'. We would like to take this opportunity to thank our internal guide Prof. S.P.DEORE. For giving us all the help and guidance. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. We are also grateful to Prof. N.F.Shaikh, Head of computer Engineering Department, MES

college of Engineering, Pune for her indispensable support, suggestions. In the end our special thanks to other person proving various resources such as laboratory with all needed software platforms, continuous Internet Connections, for our Project.

REFERENCES

- [1] Shoji Sakurai,Shinobu Ushirozawa, "Input Method against Trojan Horse and Replay Attack", IEEE 2010.
- [2] Raed M. Bani-Hani, Yarub A. Wahsheh, Mohammad B. Al-Sarhan, " Secure QR Code System", IEEE 2014.
- [3] Ms. Dhanashree Patil, Mrs. Shanti K. Guru, " Secure Authentication using Challenge-Response and Quick- Response Code for Android Mobiles", IEEE 2014.
- [4] Pei-Yulili, Yi-Hui Chen, Eric Jui-lin lu, Ping-Jung Chen, " Secret Hiding Mechanism using QR Barcode", IEEE 2013.
- [5] Hsiang-Cheh Huang, Feng-Cheng, Wai-Chi Fang, " Reversible Data Hiding with Histogram-Based Difference Expansion for QR Code Application", IEEE 2011.
- [6] Syamantak Mukhopadhyay, David Argles, " An Anti-Phishing mechanism for Single Sign-On Based on QR Code ", IEEE 2011.
- [7] Kyeongwen Chai, Changbin Lee, Woongryul Jeon, Kwangwoo lee, Dongho Van, " A Mobile based Anti-Phishing Authentication Scheme using QR Code", IEEE 2011.
- [8] Macro Vanetti, Elisabeth Binaghi, Elena Ferrari, Barbara Corminati, Mereno Corulla, " A System to Filter Unwanted message from OSN User Walls", IEEE Transaction on Knowledge and Data Engineering, vol:25, Year 2013.