

SECURING IoT DEVICES BY GENERATING QR CODES

Vaidhyesh P.S

Department of Computer Science and Engineering,

Amrita School of Engineering, Coimbatore

Amrita Vishwa Vidyapeetham, India

Email: CB.EN.H4CSE15001@cb.students.amrita.edu

Mukund W N

Department of Computer Science and Engineering,

Amrita School of Engineering, Coimbatore

Amrita Vishwa Vidyapeetham, India

Email: CB.EN.U4CSE15335@cb.students.amrita.edu

Shree Varshni G

Department of Computer Science and Engineering,

Amrita School of Engineering, Coimbatore

Amrita Vishwa Vidyapeetham, India

Email: CB.EN.U4CSE15150@cb.students.amrita.edu

Dr. N. Harini

Department of Computer Science and Engineering,

Amrita School of Engineering, Coimbatore

Amrita Vishwa Vidyapeetham, India

Email: n_harini@cb.amrita.edu

Abstract:

Classical solutions to security problems are not applicable for the communicating entities in the IoT platform. To prevent illegitimate users access to information systems, authentication using different cryptographic schemes have become an integral part of IoT. This paper discusses the applicability of a multi-factor authentication scheme based on Elliptic Curve Digital signature algorithm and QR Code to enhance the security considerations. The outcome of the experiment clearly proved its efficiency in terms of guaranteeing high security without compromise in versatility.

Keywords —Digital Signature, Elliptic Curve Cryptography, Internet of Things(IoT), QR Code, Multi-factor Authentication

I. INTRODUCTION

IOT (Internet of Things) is any non-standard computing device that can be connected wirelessly to a network and can send real time data back to the host computer. In the past decade this has gained focus of research because of the fact that security and privacy issues are not completely resolved in this field as of today. This fact is oblivious from the reports that are listed below.

1. Vulnerability and security flaws were found in the pacemakers and defibrillators that belonged to St.Jude Hospital, USA.
2. Webcam information from the available webcams was leaked as a part of TRENDnet attack. The

security firewall was so poor that people who had access to the IP address of the webcam could view the feed from the web camera.

3. The automobile manufacturer Jeep experienced an security attack where vehicles controls could be easily manipulated by the hacker.

Any damage to the IOT device can cause inconsistency in the data sent to the host computer. Since there is continuous flow of real time data, data management is an issue for all IOT devices. The growing number of devices needs us to monitor each and every IOT device that we possess including watches, cars etc. making it very difficult.

The concept being proposed in this paper is a Multi factor Authentication scheme that could be used to enhance the security of an IOT device. The scheme also has the

advantage of preserving minimal user intervention with the usage of QR code[10].

The rest of the paper is organised as follows: Section II presents Literature review. Section III of the paper discusses the architecture of the Proposed System. Section IV presents the experimentation results and discussions and finally Section V presents the conclusions and scope for the future work.

II. LITERATURE REVIEW

1. Authentication: The concept of authentication is used to explain if someone or something is who or what it is declared to be. In other words, it is a mechanism to confirm if the item claimed by the claimant is actually theirs. It is done at the starting of any process and is used to check the identity of the user before any other action takes place. There are different methods to authenticate a user: a password, a fingerprint etc. One could use what one has in order to authenticate themselves with the system. These credentials are secretive to the individuals as well as the system.

The whole process of authentication is divided into two major steps: Identification and actual Authentication. The first phase of the process consists of providing the user identity to the system. The security system searches the abstract objects that it already knows and finds the specific one that the user is applying to. Then the user provides his authentication credentials which are verified by the system after which the user is granted permission to the system[5][11].

2. QR code: is expanded as Quick Response code system. It is basically a matrix barcode that is generated in order to authenticate a user or device. The QR Code is a two-dimensional barcode while the traditional bar code is only one-dimensional. QR codes can hold data in two dimensions, both horizontal and vertical enabling it to hold larger amount of data. Statistically, QR code has the capability to store 4296 alphanumeric characters in it, which is 20 characters more than what can be stored in a traditional barcode.

QR codes have a square structure consisting of black and white squares. Different areas of the QR code have different levels of security. Each of the modules present in the QR code are either black or white i.e. 0 or 1 respectively. In some cases, the QR codes may be damaged and therefore QR codes permit four types of error rectification levels-L, M, Q and H posing permissible limits of 7%,15%,25%,30%

respectively. The concept of QR code has been widely adopted by researchers for authenticating entities.



Figure 1. Sample of QR code



Figure 2. Parts of a QR Code

Section 1 enables the decoder software to recognize orientation of the QR Code. Section 2 separates Finder Patterns from the actual data. Section 3 determines the width of a single module through an alternating black and white sequence. Section 4 supports compensation for moderate image distortions. Section 5 stores information about the error correction level of the QR Code and the chosen masking pattern. Section 6 is the data section. Section 7 is similar to the data section error correction codes are stored in 8-bit long code- words. Section 8 consists of empty bits of data and error correction bits cannot be divided into 8-bit code words.

3. IOT Security: The traditional methods of authenticating a device may include using pre-shared secrets, public-key cryptosystems, ID or password etc. These traditional authentication and authorisation techniques may not be applicable to the highly complex and heterogeneous objects and networks in IoT. As of today, for the working of an IoT device, it essentially requires the details of not only the Internet browsing behaviour but also that of all the utilities around. This is collected for better understanding of the

environment and provides the user with a personally preferred service. Having collected the stated information, securing the same is an issue that requires attention. Security features should duly protect any kind of embezzlement[2][3][10].

Constrained Application Protocol (CoAP) is a service layer protocol, for resource-constrained devices that enable communication of nodes with the other similar nodes available with the wider Internet Protocols. IoT makes use of many resource-constrained internet devices which have limited memory space, battery capacity and computing capability. Despite the use of cryptosystems and various durable and impenetrable security protocols, the resource-constrained devices may still be vulnerable to attacks.

4. Elliptic Curve Cryptography: Elliptic Curve Cryptography is a common approach to public key cryptography, that is based on elliptic curves instead of finite fields. This elliptic curve cryptography is an Elliptic Curve Discrete Logarithm problem, which is categorized under NP-Hard problems. The general equation of an elliptic curve is given by:

$$y^2 = x^3 + ax + b$$

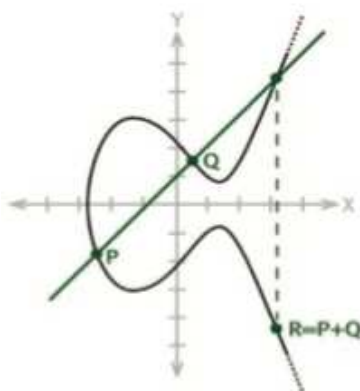


Figure 3. An elliptic curve representing $R = P + Q$

5. Elliptic Curve Digital Signature Algorithm

Operations on Elliptic Curves:

The fundamental operations on elliptic curve include point addition and point multiplication. The crucial property of an elliptic curve is that we can define a rule for adding two points which are on the curve, to obtain a third point which is also on the curve satisfying the normal properties of addition. The points and the addition law form a finite Abelian group.

To ensure that the obtained answer is well defined an extra zero point 0 at infinity is used, which does not satisfy the elliptic curve equation.

With the procedure for adding two points, one can also perform a scalar multiplication on a point where P is a point on the elliptic curve and k is any positive integer[4].

Cryptography

The communicating parties agree on a (non-secret) elliptic curve and a (non-secret) fixed curve point F. A member (say A) chooses a secret random integer A_k which is his/her secret key and publishes the curve point $AP = A_k F$ as his/her public key. The other members (say B and C) in the group perform the same operations and exchange their public keys.

In the case where A wishes to send a message to B (another member of the group) whose public key is known to A. A can compute his/her shared secret key $A_k B_p$ as and use any conventional block cipher like DES, AES etc. To encrypt the message.

The receiver computes the shared key by calculating $B_k A_p$ and perform decryption operation. The security of the scheme is based on the assumption that it is difficult to compute k given F and kF .

Choosing the Fixed Point

The careful choice of the point on the elliptic curve will ensure the level of security provided.

Usually a large prime number is chosen in elliptic curves for prime fields.

For higher security levels, the curve and fixed point are chosen in such a way that the order of the fixed point F is a large prime number and the order of the curve is determined by Schoof's Algorithm. This can probably mitigate different forms of attacks and this has been the prime factor which has made the elliptic curves more attractive. Other factors include smaller key sizes without any compromise in security levels provided by other standard cryptographic algorithms like RSA. It has been reported that computing k from kF and F takes roughly $2^{(n/2)}$ operations.

Algorithm:

1) a) Point addition

$A(x_1, y_1)$ and $B(x_2, y_2)$ are two points such that $A \neq B$

$A + B = C(x_3, y_3)$ is given by:

$$x_3 = \{\lambda^2 - x_1 - x_2\} \bmod p \quad (1)$$

$$y_3 = \{\lambda(x_1 - x_3) - y_1\} \bmod p \quad (2)$$

$$\text{Where, } \lambda = \left\{ \frac{y_2 - y_1}{x_2 - x_1} \right\} \bmod p \quad (3)$$

b) Point doubling:

$A(x_1, y_1)$ and $B(x_2, y_2)$ are two points such that $A \neq B$

$A + B = C(x_3, y_3)$ is given by following calculation

$$x_3 = \{\lambda^2 - 2x_1\} \bmod p \quad (4)$$

$$y_3 = \{\lambda(x_1 - x_3) - y_1\} \bmod p \quad (5) \quad \text{Where,}$$

$$\lambda = \left\{ \frac{3x_1^2 + a}{2y_1} \right\} \bmod p \quad (6)$$

c) Point multiplication:

Consider a point A on an elliptic curve. Multiplication over A is defined as repeated addition i.e., for multiplying a point A by a factor k, A is added K times[1].

2) KEY PAIR GENERATION:

a) Choose a random integer 'd' [0, n-1] and a generator point G, and a public key B is computed as follows.

b) Compute $B = d * G$ which is obtained by point multiplication. Check whether B, G are points on the elliptic curve.

c) Key pair is (G, B) where G is the private key and B is public key.

3) SIGNATURE GENERATION:

The signer uses private key and G for signing a document. He/She signs using the following procedure/steps:

a) Choose the random integer k where $1 \leq k \leq n-1$ and compute $k * G = (x_1, y_1)$

b) Compute $s = (h(m) * d) * k^{-1} \bmod n$. If $s = 0$, then go to step-1

c) Signature is (s, x_1)

4) SIGNATURE VERIFICATION:

The signer uses private key and G for signing a document. He/She signs using the following procedure/steps:

a) Verify that 's' is an integer in the interval [1, n-1]

b) Compute $w = s^{-1} \bmod n$

c) Using 'w' compute the point $(x, y) = w * Q$ such that (x, y) lies on the curve and find authenticity by checking the equivalence $x = x_1$ holds or not. If holds, signature is verified otherwise reject.

Solved Example to illustrate ECDSA:

Using ECDSA:

$d = X_p$ $d=3$; $A=29$

Considering the curve: $y^2 = x^3 - x + 16 \bmod 29$

Key Pair Generation:

After applying point addition and point doubling to the numbers, we get:

$$B=3G \text{ where } G=(5,7)$$

$$2G=G+G \quad 2G=(28,4)$$

$$3G=2G+G=(18,1)$$

$$\text{Now, } B=(18,1)$$

Signature Generation:

$$k * G = (x_i, y_i)$$

selects random $k=3$ and calculates

$$k * G = (x_i, y_i)$$

$$(x_i, y_i) = (18,1)$$

$$r = 18 \bmod 29$$

$$r=18$$

$$s = (h(m) * d) * k^{-1} \bmod n$$

$$s = 3^{-1}(46 + 3*18) \bmod 29$$

$$s = 10(100) \bmod 29$$

$$s = 1000 \bmod 29$$

$$s=14$$

$$\Rightarrow (r, s) = (18, 14)$$

Signature Verification:

$$w = s^{-1} \bmod n$$

$$w = 14^{-1} \bmod 29$$

$$w=27$$

$$u_1 = 46 * 27 \bmod 29$$

$$u_1=24$$

$$u_2 = 18 * 27 \bmod 29$$

$$u_2=22$$

$$w * B = (x, y)$$

$$X = u_1 * G + u_2 * k * G$$

$$X = 24(5,7) + 22(18,1)$$

$$X = (x_3, y_3) = (18, 28)$$

System parameters:

A	Field(x,y)
G	Generator point
a,b	Coefficients of elliptic curve
K	Random number
B	Field(x,y)
(r,s)	Signature of signer
X_a	Private Key of UserA
Y_a	Public Key of UserA
X_b	Private Key of UserB
Y_b	Public Key of UserB

C	Resulting point
$\frac{y}{x}$	Slope of line
D	Private Key
M	Message
$h(m)$	Hashed Message

Summary of Findings:

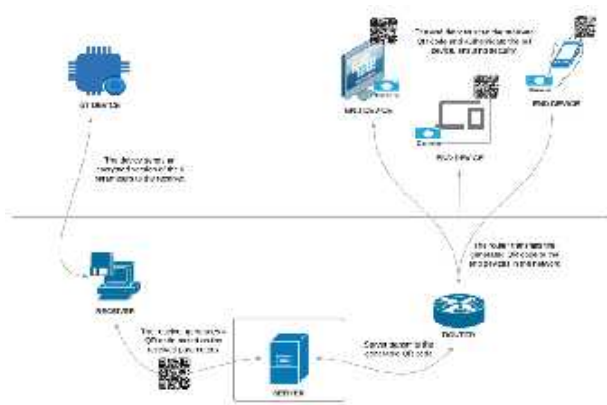


Figure 4. The architecture diagram illustrating essential functionalities

Literature has proposed many schemes to enhance the security of IoT. One of the challenges is to identify a security principle that would uniquely suit an IoT context. IoT brings with it everything from microwaves to pacemakers say an estimated 25 billion devices to come online in the next 5 years, thereby making it an indispensable part of life. The protocols in their present form are rarely sufficient to provide a high level of security. To combat this security crisis we need a robust model that would enable devices to be used for end users in a secure manner. An attempt has been made in this work to study the effectiveness of ECDSA combined with bar coding techniques enhancing the security of IoT devices. The application of this could probably facilitate the IoT devices in the network to authenticate efficiently in a resource constraint environment.

III. PROPOSED SYSTEM

The architecture of the proposed model to enhance the security using multi-factor authentication is presented in the Figure 4. The devices in the architecture have a QR Code tag which could be scanned by the server for authenticating the device and vice versa. The QR code would contain information regarding the MAC address of the device and of the destination, IP address and the names of the communicating devices, with a pre shared key and Time stamp. The handshake for authentication can be initiated by the server at any point of time. The contents of the QR code

also ensure that the basic forms of attacks on IoT network are thwarted. The experimentation results are presented in section IV.

IV. EXPERIMENTATION RESULTS AND DISCUSSIONS

A thorough experimentation was carried out on the architecture set up to evaluate the performance of the system. The results clearly brought out the effectiveness and the versatility of the scheme in terms of authenticating devices in IoT network satisfying resource scarce criteria of the network. The Figure 5 is a screenshot of the source code that generates the QR Code that contains the parameters that have been passed, Figure 6 shows the encryption of the parameters, Figure 7 is a sample of one of the generated QR codes on the side of the claimant and Figure 8 shows the verification of the QR Code by an authenticator.



Figure 5. The source code to generate QR Code



Figure 6. Encrypted parameters



Figure 7. Generated QR Code

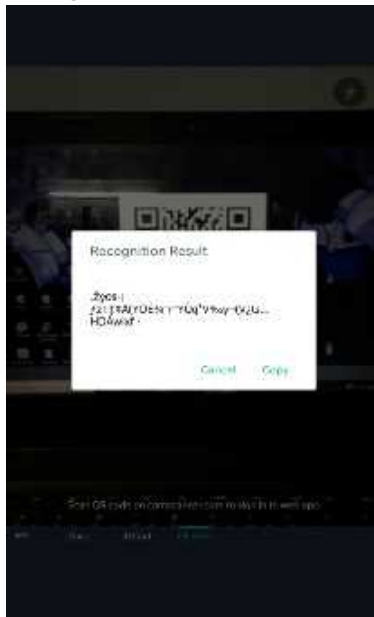


Figure 8. Recognition of the QR Code

V. CONCLUSIONS

In this paper, it has been shown that IoT devices can securely communicate using the proposed signature scheme integrated with QR code verification mechanism. The model that has been proposed and developed is found to provide much bigger random data ranges that might mitigate the relevant possible cryptographic attack risks (Man in the Middle Attack, replay attacks etc). It is also planned to develop a new version of this system with an improved colour QR code as a future study that would be more effective with its capability of storing information in multiple-layers.

REFERENCES

- [1] Li, H., Zhang, R., Yi, J. and Lv, H. (2013) A Novel Algorithm for Scalar Multiplication in ECDSA. 5th International Conference on Computational and Information Sciences, Shiyang, 21-23 June 2013.
- [2] IoT Security: Ongoing Challenges and Research Opportunities, Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shihpyng Shieh, IEEE Fellow.
- [3] An Overview of Privacy and Security Issues in the Internet of Things, Carlo Maria Medaglia- Springer Link Journal 2013.
- [4] Optimized ECC Implementation for Secure Communication between Heterogeneous IoT Devices Leandro Marin 1, Marcin Piotr Pawlowski and Antonio Jara, 2016.
- [5] Dr.N.Harini, Dr T.R Padmanabhan and Dr.C.K.Shyamala, "Cryptography and security", Wiley India, First Edition, 2011.
- [6] J.-Y. Lee, W.-C. Lin, Y.-H. Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next-Generation Electronics, ISNE 2014, Kwei-Shan, 2014.
- [7] G.Sharmam, S. Bala, A.K. Verma, Security frameworks for wireless sensor networks-review, in: 2nd International Conference on Communication, Computing & Security, ICCCS-2012, 2012.
- [8] Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma A security transmission model for internet of things JisuanjiXuebao/Chin. J. Comput., 34 (8) (2011).
- [9] J. Yang, B. Fang Security model and key technologies for the internet of things J. China Universities Posts Telecommun., 8 (2) (2011).
- [10] Dr. Senthil Kumar M., Aishwarya, M., K. Vaishnavi, S., Sukanya, R., Aiswariya, C., and Dr.Harini N., "An Improved Authentication Scheme Using Colour QR Codes", in Proceedings of International conference on Adaptive Technologies for Sustainable Growth (ICATS-2014), 2014.
- [11] Dr.Shyamala C. K., Dr.NHarini, and Padmanabhan, T. R. Dr., "Arithmetic on Elliptic Curves Over Finite Fields", National Conference on Advanced Computing Technologies, ACT '08. pp. 25-26, 2008.
- [12] Development of IoT Security Component for Interoperability Se-Ra Oh Dept. of Computer and Information Security Sejong University Seoul, South Korea published in IEEE Journal, 2013.

