International Journal of Recent Trends in Engineering & Research

ISSN(ONLINE) : 2455-1457 IMPACT FACTOR : 3.344

AN ANALYSIS OF RFID AUTHENTICATION SCHEMES FOR INTERNET OF THINGS (IOT) IN HEALTHCARE ENVIRONMENT USING ELGAMAL ELLIPTIC CURVE CRYPTOSYSTEM

Mr.R. Balasubramaniam[1], R. Sathya[2], S. Ashicka[3] and S. SenthilKumar[4]

[1,2,3,4]Department of CSE, Kathir College of Engineering

Abstract: Internet of Things (IoT) has emerged as one of the most powerful communication paradigms of the 21st century. In the IoT environment, all objects in our daily life become part of the Internet because of their communication and computing capabilities (including microcontrollers, transceivers for digital communication, suitable protocol stacks) that allow them to communicate with other objects. In the healthcare area, IoT involves many kinds of cheap sensors (wearable, implanted, and environmental) that enable elderly people to enjoy medical healthcare anywhere, any time. Radio-frequency identification (RFID) is one of the most important technologies used in the IoT as it can store sensitive data, wireless communication with other objects, and identify/ track objects automatically. To satisfy the various security requirements of RFID technology in IoT, many RFID authentication schemes have been proposed in the past decade. Recently, ElGamal elliptic curve cryptography (EECC)-based RFID authentication schemes have attracted a lot of attention and have been used in the healthcare environment. In modified method, the number of doubling and adding operations in the encryption process has been reduced. The reduction of this number is a key point in the transformation of each character into an affine point on the EC.

Keywords*:*Elliptic curve cryptography (ECC),ElGamal encryption,Radio-frequency identification (RFID).

I. INTRODUCTION

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities.

Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. As well as the expansion of Internet-connected automation into a plethora of new application areas, IoT is also expected to generate large amounts of data from diverse locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. IoT is one of the platforms of today's Smart City, and Smart Energy Management Systems.

II. LITERATURE SURVEY

Wolkerstorfer introduced the concept of ECC-based RFID authentication scheme in 2005. However, he did not propose any specific authentication scheme. It shows the plausibility of meeting both security and efficiency requirements even in a passive RFID tag. Practical identification scheme which is proven to be as secure as the factoring problem and is almost as efficient as the Guillou-Quisquater identification scheme: the Guillou-Quisquater scheme is not provably secure. Later, Lv et al pointed out that Martinez et al.'s scheme is vulnerable to the tracking attack. To overcome weaknesses in their previous schemes, Lee et al proposed three improved ECC-based RFID schemes. Recently proposed RFID authentication protocols which rely exclusively on the use of Elliptic Curve Cryptography are not secure against the tracking attack. Unfortunately, Deursen and Radomirovic pointed out that Lee et al schemes were still vulnerable to the man-in-the-middle attack. Farah also pointed out that Chou's scheme was vulnerable to the impersonation attack and proposed an improved scheme to withstand such attacks. Chou proposed a RFID authentication protocol based on elliptic curve cryptography. However, it demonstrates that the Chou's protocol does not satisfy tag privacy, forward privacy and authentication, and server authentication. Based on these security and privacy problems, we also show that Chou's protocol is defenseless to impersonation attacks, tag cloning attacks and location tracking attacks. Therefore, propose a more secure and efficient scheme, which does not only cover all the security flaws and weaknesses of related previous protocols, but also provides more functionality. We prove the security of the proposed improved protocol in the random oracle model.

III. PROPOSED SYSTEM

With recent advances in modern cryptography, it is well-known that must be able to prove that a cryptographic scheme is provably secure using a security model. Elliptic Curve Cryptosystem (ECC) is one of the most efficient cryptosystems that is used to encrypt/decrypt data; it is secured against all kinds of attacks. The short key size of ECC gives it strengthened security compared to other cryptosystems like RSA with the same security level. This advantage leads to fast computations, less memory and power consumption, and saving bandwidth. These advantages make ECC efficient to be used in some applications like e-commerce, smart cards, chip cards, and portable devices. In EECC work, a new efficient method has been proposed to encrypt/decrypt any text using the hexadecimal ASCII value for each character. ECC offers the same security level like RSA and ElGamal algorithms with shorter key length which makes it works with a little amount of memory and low power [68-69]. In this work, a modified method that uses ElGamal ECC for encryption and decryption of the plaintext has been proposed. The modified method uses the hexadecimal ASCII value to represent each character. This representation reduces points doubling and addition which are required to transform the characters into points on the elliptic curve. As a result, further from speeding up the computations can be achieved.

IV. ARCHITECTURAL DESIGN

4.1 RFID Tag

A tag is composed of a microchip, an antenna, and a dedicated hardware for cryptographic operations. It can store secret data for authentication and it communicates with the RFID reader. Usually, the RFID tag's computing capacity and memory storage are very limited. RFID tags could be divided into three types: passive tag, semi active tag, and active tag [65]. The passive tag gets power through wireless signals from the reader. The semi active tag is equipped with a small battery and gets power from it. The passive and the semi active tags use backscatter modulation to send messages. The active tag is equipped with a small battery and a radio transceiver. It can communicate directly with the reader.

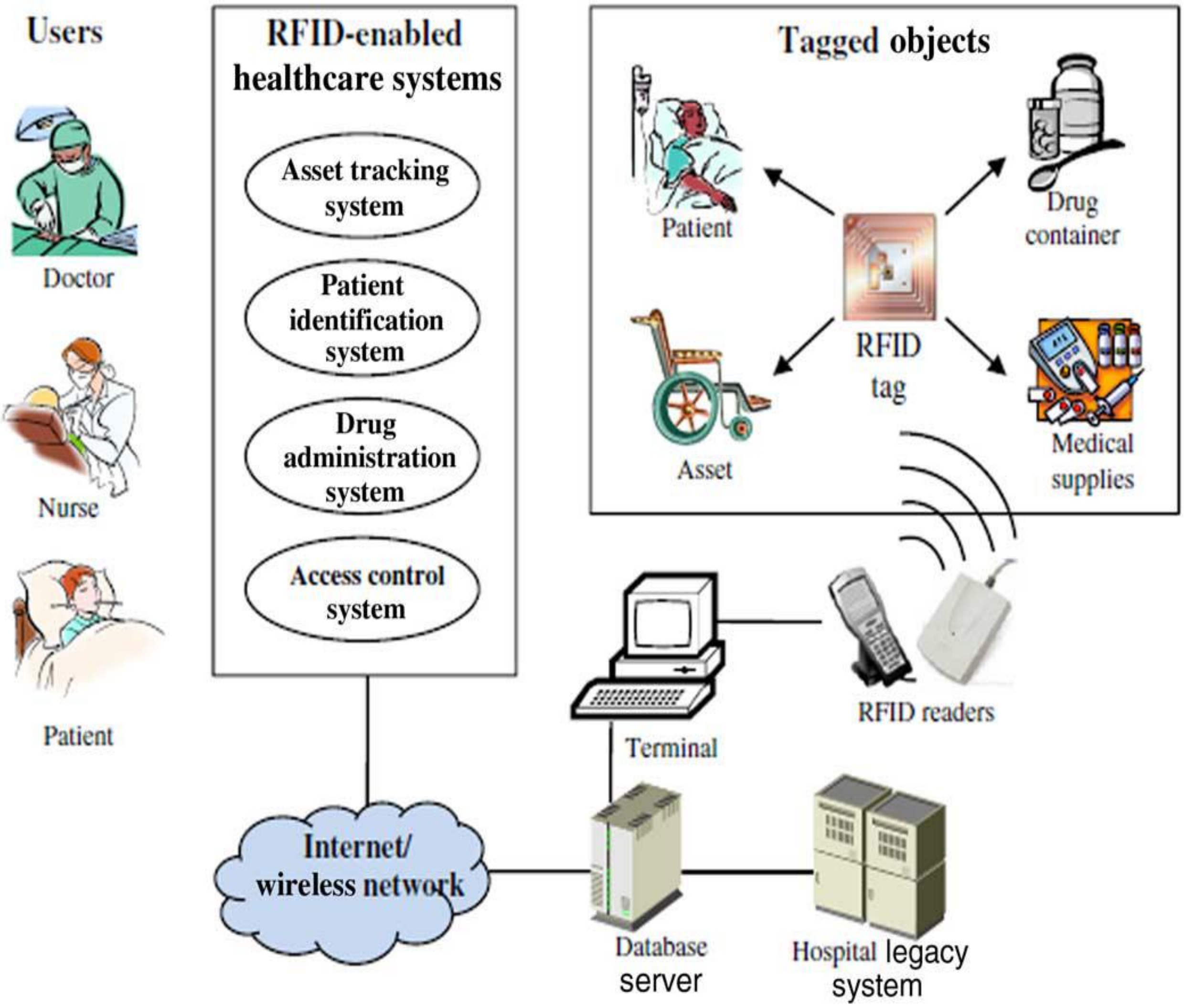

Fig 1: Architecture Diagram

4.2 RFID Reader

An RFID reader is composed of a radio transmitter, a radio receiver, a control unit, and a memory unit. The main function of an RFID reader is to enable the RFID tag and the server to exchange messages between each other and achieve mutual authentication. Usually, the RFID reader's computing capacity is higher compared to that of the RFID tag.

4.3Server

A server is a trusted entity. To achieve the goal of mutual authentication, it stores all the RFID tag's identification information in its database when the system is set up. Using the stored identification information, the server could determine the validity of the tag. Usually, the server's computing capability and memory capacity are high.

The Modification of ElGamal Elliptic Curve Cryptosystem (MEGECC) has been presented in this section. This modification depends on the speeding up of the computation on EGECC using hexadecimal ASCII values by reducing the number of doubling and addition operations needed. The domain parameters (that is $\{A, B, p, G\}$) are public for all entities.

Suppose A and B are two users wishing to communicate and exchange the information using MEGECC over insecure channel.

Let us choose the user A as the sender who wants to encrypt and send a message m to the user B (the receiver). Every entity, namely A and B, need to choose a private key. The private keys, $n_A$and $n_B$are positive integers chosen randomly from the interval $[1, p - 1]$. The public keys for the users A and B can be generated respectively as follows:

$$P_A = n_A . G$$
$$P_B = n_B . G$$

The basic idea of the contribution in this work depends on using the hexadecimal ASCII value to reduce the number of doubling and addition operations. Suppose user A wants to send a message m to user B. Firstly, he converts each character in the message m into hexadecimal ASCII value of two digits $(h_1h_2)_{16}$ then separates the value into two values $(h_1, h_2)_{16}$ and converts each value of h_1 and h_2 to decimal values d_1 and d_2 respectively. The scalar multiplication of the base point G on E by each value of d_1 and d_2 can be computed to transform the values to points on E by the following formulas:

$$P_{h_1} = d_1 . G$$
$$P_{h_2} = d_2 . G$$

where $(h_1h_2)_{16}$and are two points lie on E . User A computes the secret key K by multiplying his private key $n_A$by B's public key P_B

$$K = n_A . P_B$$

and adds the result to the points $P_{h_1h_2}$and to compute the ciphertext message as follows

$$C_1 = P_{h_1} + K$$
$$C_2 = P_{h_2} + K$$

where C_1 and C_2 are two points lie on E. The set of points $\{C_1,C_2\}$ is sent to the user B. Upon receiving the ciphertext $\{C_1,C_2\}$ by user B, the decryption process will be started. User B first needs to multiply his private key $n_B$by A's public key $P_A$to get the secret key K

$$\boldsymbol{C_1 - k = C_1 - n_B . P_A = P_{h_1} + n_A . P_B - n_B . n_A . G = P_{h_1} + n_A . n_B . G - n_A . n_B . G}$$
$$\boldsymbol{= P_{h_1} \text{ and in similar way for } C_2}$$
$$\boldsymbol{C_2 - k = C_2 - n_B . P_A = P_{h_2} + n_A . P_B - n_B . n_A . G = P_{h_2} + n_A . n_B . G - n_A . n_B . G}$$

Next step is to solve the following equations for d_1 and d_2 by using Elliptic Curve Discrete Logarithm **Problem (ECDLP) where P_{h_1} , P_{h_2}, and G are known**

$$\boldsymbol{P_{h_1} = d_1 . G}$$
$$\boldsymbol{P_{h_2} = d_2 . G}$$

The last step is to convert d_1 and d_2 to hexadecimal h_1 and h_2 respectively, and write them as, $(h_1h_2)_{16}$ then find the match character from the hexadecimal ASCII table. Repeat the previous procedure for each character in the message m. One of the advantages of the modified cryptosystem is that the solution of $P_{h_1} = d_1.G$. and $P_{h_2} = d_2.G$. is not difficult for the receiver and will not take a long time because he largest value for $d1$ and $d2$ in decimal is 15 (the maximum digit in hexadecimal is F = 15) but it is very difficult for the adversary because he can't know the private key nB and the prime number p will be chosen as a large number.

V. ALGORITHM

5.1Elliptic Curve Cryptosystem (ECC) based RFID schema

With recent advances in modern cryptography, it is well-known that must be able to prove that a cryptographic scheme is provably secure using a security model. Elliptic Curve Cryptosystem (ECC) is one of the most efficient cryptosystems that is used to encrypt/decrypt data; it is secured against all kinds of attacks. The short key size of ECC gives it strengthened security compared to other cryptosystems like RSA with the same security level. This advantage leads to fast computations, less memory and power consumption, and saving bandwidth. These advantages make ECC efficient to be used in some applications like e-commerce, smart cards, chip cards, and portable devices. If the number of tags in Wang *et al.*'s scheme is N, the back-end server has to check about $N/2$ equations to verify the validity of the tags on average. Therefore, the computational workload of the searching algorithm increases significantly with an increase in the number of tags making this scheme not scalable and not suitable for practical applications. Besides, the tag in Wang *et al.*'s scheme cannot authenticate the backend server because it receives only a random number sent by the back-end server. Therefore, Zhang *et al.*'s schemes cannot provide mutual authentication.

Liu *et al.*also proposed an ECC-based RFID authentication by using ElGamal scheme. Compared to Godor and Imre's scheme, Liu *et al.*'s scheme has better performance because the ECDSA is not used in it. In the initialization phase, the server generates the system parameters params = $\{F(q), E(F(q)), n, P\}$, stores (id, X_1) and (id, x_1, X_1) in its database and the tag's memory separately, where id is the tag's unique identity.

Step 1) $Tag \rightarrow Server$: The tag sends its identity id to the server.

Step 2) $Server \rightarrow Tag$: After receiving the tag's identityid, the server looks up its database for the tuple (id,X_1). If there is no such tuple, the server aborts the session; otherwise, the server generates three random numbers$n_1, n_2, n_3$and $computes$ $(c_1, c_2) = n_3X_1, \gamma_1 = c_1n_1, \gamma_2 = c_2n_2, \gamma_3 = n_3P$, and $A = (id + n_1 + n_2) \oplus X_1$Then, the server sends the message $\{\gamma_1, \gamma_2, \gamma_3, A\}$ to the tag.

Step 3) Tag → Server: Upon receiving the message $\{\gamma 1, \gamma 2, \gamma 3, A\}$, the tag computes $(c_1, c_2) = x_1\gamma_3, n_1 = c_1^{-1}\gamma_1$, and$n_2 = c_2^{-1}\gamma_2$ and checks whether the equation $A = (id + n_1 + n_2) \oplus X_1$holds. If it does not hold, the tag rejects the session; otherwise, the tag computes $B = (n_1 \oplus n_2) + id$ and sends the message $\{B\}$ to the back-end server.

Step 4) Server: Upon receiving $\{B\}$, the back-end server checks whether the equation $B = (n_1 \oplus n_2) + id$holds. If it does not hold, the back-end server rejects the session; otherwise, the tag is authenticated.

5.1ElGamal elliptic Curve Cryptosystem based RFID schema

In EECC work, a new efficient method has been proposed to encrypt/decrypt any text using the hexadecimal ASCII value for each character. The main contribution is to reduce the number of doubling and addition operations. The modified method uses the hexadecimal ASCII value to represent each character. This representation reduces points doubling and addition which are required to transform the characters into points on the elliptic curve. As a result, further from speeding up the computations can be achieved. This modification depends on the speeding up of the computation on EGECC using hexadecimal ASCII values by reducing the number of doubling and addition operations needed. The domain parameters (that is $\{A, B, p, G\}$) are public for all entities. Suppose A and B are two users wishing to communicate and exchange the information using MEGECC over insecure channel. Let us choose the user A as the sender who wants to encrypt and send a message m to the user B (the receiver). Every entity, namely A and B, need to choose a private key. The private keys, $n_A$and $n_B$are positive integers chosen randomly from the interval $[1, p - 1]$.

VI. PERFORMANCE EVALUATION

Compare the performance and security aspects of the ECC-based RFID authentication schemes discussed earlier. By evaluating them in terms of the security requirements list and comparing their communication and computation costs, could determine whether an ECC-based RFID authentication scheme is suitable for practical applications. It is well known that the tag's computing capability and memory are very limited. Therefore, the computation cost, communication cost, and the storage requirements are important characteristics for practical applications. To achieve the same security level as the RSA algorithm with 1024 bits' key size, an elliptic curve defined over the finite field F (2163) is used in many implementations. Also uses a such an elliptic curve to discuss the computation cost, communication cost, and security requirements of the various schemes.

6.1 Analysis of Computation Cost

Let T_{mul}, T_{inv}, T_{eca}, T_{ecm}, and $T_h$denote the running time of a modular multiplication operation, a modular inversion operation, an elliptic curve point addition operation, an elliptic curve point multiplication operation, and a hash function operation respectively. For fair comparisons of the computational cost, the running time of different operations are measured according to that of a modular multiplication operation. According to have $T_{\text{inv}} \approx 3T_{\text{mul}}$, $T_{\text{eca}} \approx 5T\text{mul}$, $T_{\text{ecm}} \approx 1200T_{\text{mul}}$, and $T_h \approx 0.36T_{\text{mul}}$

6.2 Analysis of Communication Cost

Use an elliptic curve defined over the finite field F (2163) in comparisons. Need 42 bytes and 21 bytes to store a point on the elliptic curve and an element of the field, respectively. In addition, assume that the output of the hash function and the length of identifier are 20 bytes and 4 bytes, respectively.

6.3 Analysis of Security Requirements of ECC-Based Authentication Schemes

Security is the most important aspect of an RFID authentication scheme. The security requirements of related ECC-based RFID authentication schemes are discussed in this section. Let SR1, SR2, SR3, SR4, SR5, SR6, an SR7 denote mutual authentication, confidentiality, anonymity, availability, forward security, scalability, and attack resistance, respectively.

VII. ADVANTAGE OF EECC

Analysis of recently proposed EECC based RFID authentication schemes particularly suited for the healthcare environment. Although satisfy all security requirements and have satisfactory performance for the healthcare environment in terms of their performance and security.

VIII. CONCLUSION

RFID authentication is one of the most critical security services for IoT implementations in the healthcare environment. In this work presented an in-depth survey of recently proposed ECC-based RFID authentication schemes. With recent advances in modern cryptography, it is well-known that must be able to prove that a cryptographic scheme is provably secure using a security model. Elliptic Curve Cryptosystem (ECC) is one of the most efficient cryptosystems that is used to encrypt/decrypt data; it is secured against all kinds of attacks. The short key size of ECC gives it strengthened security compared to other cryptosystems like RSA with the same security level. This advantage leads to fast computations, less memory and power consumption, and saving bandwidth. These advantages make ECC efficient to be used in some applications like e-commerce, smart cards, chip cards, and portable devices.

IX. FUTURE WORK

In the future work detailed communication cost of various EECC-based RFID authentication schemes is validated and experimented under real time applications.

REFERENCES

1. Dave Evans (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (PDF). Cisco. Retrieved 15 February 2016.
2. Wood, Alex. "The internet of things is revolutionizing our lives, but standards are a must". theguardian.com. The Guardian. Retrieved 31 March 2015.
3. J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, D. Boyle: From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Elsevier, 2014, ISBN 978-0-12-407684-6.
4. Erlich, Yaniv (2015). "A vision for ubiquitous sequencing". Genome Research 25 (10): 1411–1416.

I. Wigmore: "Internet of Things (IoT)". TechTarget, June 2014.

5. Noto La Diega, Guido and Walden, Ian, contracting for the ‘Internet of Things’: Looking into the Nest (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016.
6. Farooq, M.U.; Waseem, Muhammad; Khairi, Anjum; Mazhar, Sadia (2015). "A Critical Analysis on the Security Concerns of Internet of Things (IoT)". International Journal of Computer Applications (IJCA) 11: 1–6.
7. Hendricks, Drew. "The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.
8. Fickas, S.; Kortuem, G.; Segall, Z. (13–14 Oct 1997). "Software organization for dynamic and adaptable wearable systems". International Symposium on Wearable Computers: 56–63.
9. Kushalnagar, N; Montenegro, G; Schumacher, C (August 2007). "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals". IETF RFC 4919.