© Universiti Tun Hussein Onn Malaysia Publisher's Office

IJIE

Journal homepage: http://penerbit.uthm.edu.my/ojs/index.php/ijie
ISSN : 2229-838X e-ISSN : 2600-7916

The International Journal of Integrated Engineering

A Novel Authentication and Key Agreement Scheme for Countering MITM and Impersonation Attack in Medical Facilities

Steve Olsen Maikol[1], Adnan Shahid Khan[1*], Yasir Javed[1,2], Anderson Lau Anak Bunsu[1], Chelsten Petrus[1], Heindwick George[1], Simon Jau[1]

[1]Faculty of Computer Science and Information Technology,
Universiti Malaysia Sarawak, Sarawak, MALAYSIA

[2]Department of Computer Science,
Prince Sultan University, Riyadh, 11586, KSA

*Corresponding Author

DOI: https://doi.org/10.30880/ijie.2021.13.02.015
Received 27 May 2020; Accepted 2 December 2020; Available online 28 February 2021

Abstract: Authentication is used to enfold the privacy of the patient to implement security onto the communication between patients and service providers. Several types of research have proposed support for anonymity for contextual privacy in medical systems that are still vulnerable to impersonation attack and Man-in-the-middle attack. By using powerful technology that is used in medical facilities, it can help in building an advanced system. However, the same powerful tools can also be used by the attackers to gain personal profits and to cause chaos. The proposed countermeasure that is to be taken to prevent this kind of attacks is by implementing mutual authentication between users, their devices/mobile devices, and the system's cloud server, and also a key agreement scheme together with the help of Elliptic Curve Cryptography (ECC). A novel authentication scheme which consists of two phases, a signature generation, and authentication process. The ECC implementation is to ensure that the keys are thoroughly secured and is not copy- able, together with a Key generation scheme that shields the system against impersonation attacks. The usage of Elliptic Curve Digital Signature Algorithm (ECDSA), in a signature generation, on the other hand, provides users more secure way to hide the user private key and bring additional security layer before proceeding to authentication phase due to the existence of extra elements of domain parameters. Authentication is still considered as a crucial component in maintaining the security of any critical facilities that require the CIA tried and non- repudiation as a need to maintain their data. It does not only apply to medical centers, but any organizations that possess valuable data that is needed to be protected also requires strong authentication protocols. Thus, the trend for the need of novel authentication protocols will keep on rising as technology gets fancier and fancier.

Keywords: Authentication, security, ECC, ECDSA, Key Generation Scheme

1. Introduction

Technological advances in a different field, especially in medical, has brought significant improvement in peoples' daily life. The usage of wireless communication network opens various solution to solve an existing problem in the traditional healthcare system, and the rise of On-Demand healthcare enable a legitimate mobile user to enjoy wireless healthcare services or known as medical cloud computing service. Medical cloud computing offers an inexpensive,

*Corresponding author: skadnan@unimas.my

powerful, scalable, and easy to access solution [1] offering ubiquitous medical facilities access to everyone anywhere. [2]. Security issues such as man in the middle (MITM) or impersonation attack are always possible because of the adversary. Impersonation attack can be defined as an attack in which the identity of one of the trusted sides in the communication protocol is successfully assumed by an adversary while MITM is an interception on traffic attack. Kim et al. proposed an authentication scheme using smartcard [3], but this scheme has limitations as smartcard can be stolen, lost or duplicated and this scheme assumes the channel between user and server is an intranet. Therefore, it is not possible to fully utilize cloud computing, where users can access the service anywhere.

The research proposes a new authentication scheme that cloud computing for the mobile user. As the chance of an adversary attack is relatively high in the wireless channel, authentication and verification are one of the core aspects in ensuring secure channel between user and cloud. Therefore, the proposed solution implements two-layer security with key agreement scheme. Cryptography, which is one of the well-known technique in securing communication in the presence of adversary [4], is used as the based line of the proposed solution. Elliptic Curve Cryptography (ECC) is used together with Menezes-Qu-Vanstone (MQV) and ECDSA for the authentication and key agreement scheme. Current authentication scheme and the proposed scheme has been extensively analyzed, and the analysis shows that the impersonation attack and MITM can be minimized. The addition of the second layer in the key agreement scheme, which is generated keyword via ECC-MQV help in reducing the risk of impersonation attack as it provides mutual authentication between sender and receiver. The implementation of ECDSA ensures the message sent encrypted along with private key and digital signature [5]. Since the generation of the digital signature is pick from random domain parameter, it will minimize the chance of MITM.

The proposed solution will encourage other researchers to look deeper into two-layer security using cryptography. The implementation of MQV and ECDSA are proven to be more secure [6] as compared to the conventional method due to its extra layer in the authentication. And the proposed solution can also be used as a baseline for any wireless communication as cloud computing are becoming more relevant each day. The rest of this paper is organized as follow: Section II briefly reviews the problem statement of this paper. Section III discuss the related work. Section IV presents the proposed solution. Section V presents the performance analysis and in Section VI presents the concluding remarks.

2. Problem Statement

Medical facilities contain critical data, such as patient personal information, medical history, and medicine usage. Data privacy and data security is a key security issue that must be addressed. Townsend [7] stated with the improvement of technology, the risk of attack also increases. Authentication is one of the key components in a secure medical system. Fig 1 illustrates the network model of common problem encounter in the today healthcare center. The patient and physician's privacy is an important aspect and can be protected through authentication. By using powerful technology that is used in medical facilities, it can help in building an advanced system but we cannot ignore the fact that the same powerful tools can also be used by the attackers to gain personal profits and to cause chaos, one component that is likely to be hacked as a target by these adversaries is the third-party devices that were used. The data integrity and security of hospitals is easily stolen by adversaries, resulting in a flawed system that is corrupted and manipulated by digital criminals, especially from third- party devices such as the patient's mobile phone. These third-party devices are not always secure, as some of them does not implement authentication protocols.

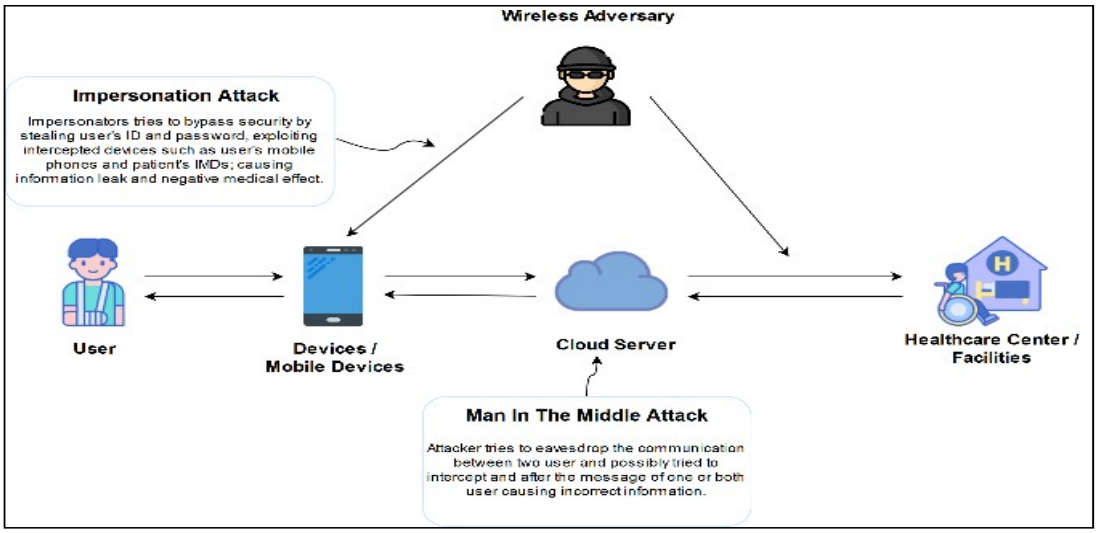

Fig. 1 -System model of the health care system

2.1 Impersonation Attack

One of the notable attacks would be an impersonation attack, which can be defined as an attack in which the identity of one of the trusted sides in the communication protocol is successfully assumed by an adversary. To achieve this, impersonator can generate current timestamp and a random nonce to generate a valid login request message. This will give the impersonator full control to the patient wearable device and allow the impersonator to exploit it, which can hurt the patient and its medical data. For example, the impersonator can exploit the insulin pump and can cause an excess of insulin to the diabetic patient, which cause hypoglycemia, which in worst cases, become a diabetic shock to the patient.

2.2 Man in the Middle Attack

Another notable attack is the man-in-the-middle attack which is an attack where attacker privately transmit and possibly intercept the communication between two sides who think they are communicating with each other without an intermediary as described by DuPaul (2019) [8]. As the precision of information is very important in the medical field, any form of changes will greatly affect patient health. Therefore, it is a concern for every medical system. An attacker can easily change the patient health information, and this can lead to incorrect prescription by the physician to the patients. Another example is when a patient is arranging an appointment with their physician. If the attacker can intercept the communication between the physician and patient, a fake appointment can be set, and it will affect both the physician and patient time table as the appointment is very important especially to the very-ill patient because they required strict scheduling and planning. Although many have proposed for the anonymity support for context privacy in the medical system, some of them are still vulnerable to known attack. Thus, a generalized yet strong authentication protocol is needed to be implemented for the whole medical system.

3. Literature Review

Medical facilities contain critical data, such as patient personal information, medical history, and medicine usage. Data privacy over the past few years, many researchers have proposed and developed many types of authentication protocols to eliminate the lack of security in systems as well as to avoid security attacks from happening, especially for medical systems. There are a few related works that are being reviewed as guidance in designing the proposed authentication scheme to utilize cloud computing for the mobile user. [9] Proposed an anonymous authentication scheme for WBAN. The scheme proposed three algorithms, which are initialization, registration, and authentication. The chance of impersonation attack is higher because it is reasonable to assume that there exists an adversary with privileged access to the system. The addition of a network manager in the system increase the secureness of the system but with higher communication cost. The performances of the system are determined by evaluating storage overhead, communication cost, and computation cost. [10] proposed an authentication scheme to preserve privacy based on identity-based cryptography. Compared to another existing scheme, this proposed scheme omits the needs of Electric Health Record (EHR) to distribute different security value with the user. The implementation of two-factor security brings more in security aspect by converting user secret information to other value. The proposed scheme evaluates five different perspectives which are confidentiality, integrity, authentication, contextual privacy, and insider privacy and is evaluated with the help of quadratic residue assumption to overcome the weaknesses from the existing scheme. [11] Proposed an anonymous authentication scheme that uses a revolving group signature pattern based on ECC to deliver privacy to patients. The perspective of the proposed scheme is measured by the intractable problems, the anonymity it provides, forward unlink-ability, traceability, integrity and resistance to attack, resistance over denial of service (DOS) attacks and traffic analysis attacks. [13] Proposed a novel approved available security show (AAPM) to solve the security of patient data and their identity privacy. The patient/client can give authority to physicians by setting up an entrance tree supporting flexible limit predicates. The strength of the proposed solution is it outperforms the previous system in term of computational, correspondence, and capacity overhead. The weakness is the impersonation attack. The types of attack are eavesdropping and tampering [14]. The method to measure the proposed solution is formal security evidence and simulation results (efficiency evaluations). The evaluation metrics for the proposed solution are numerical analysis and implementation. [15] Proposed an authentication protocol that uses minimal energy for medical cloud architecture. The protocol mitigates impersonation attack by having a secret key which only shared between healthcare center and cloud, which the adversary cannot find out the valid authentication message signatures to pass the authentication [16]. A novel authentication for the deployment of implantable medical devices (IMD) was proposed by [17] in which it consists of key agreement scheme; they applied elliptic curve cryptography (ECC) into a three-factor remote user authentication protocol [18], [19]. An adversary could hack its way to a hospital's weak-authenticated private networks through IP or ARP spoofing, thus, crashing the whole system and may lead to a DOS attack [20], [21].

4. Proposed Solution

Based on the above analysis of related work, the authentication scheme has been proposed to overcome the attack that is discussed in section II. A basic wireless healthcare system consists of 2 phase: the login phase and the data storing phase. As discussed in section II, it is assumed that the impersonation attack usually happens during user login phase and man in the middle attack usually happen during data storing phase. For impersonation attack, we proposed two phase to mitigate the attack: Asymmetric key generation based on ECC approach phase and Key agreement phase. As for the man in the middle attack, the phases are Signature generation phase and authentication process phase. Therefore, this paper focuses on these two attacks that happen during its respective phase. Fig 2 illustrates the network model of the proposed solution. One of the factors that contribute to the occurrences of Impersonation Attack in the Medical Centre was because of the lack of authentication between senders and receivers. Impersonation Attack is an attack in which external adversaries succeeded in stealing the identity of one of the system's authorized user or in a protocol for communications. When a user's account was hacked or stolen, an impersonation attack is bound to happen. Usually, these attacks occur in the form of emails that attempt to impersonate a trusted individual or company in an attempt to gain access to corporate finances or data. A popular example of an impersonation attack is Business Email Compromise (BECs), or also known as CEO fraud. When missed, the impersonator may use this advantage to gain access to the company's system and steals information or data. Thus, the company may suffer a loss or eventually closed down due to the insecurity of the system's protection. From problem statement, this often occurs to the user after they tried to log in into the healthcare center's system. Impersonator generates the current timestamp during the login of a user and a random nonce to generate a valid login request message. The proposed countermeasure that is to be taken to prevent this kind of attack was by implementing mutual authentication between users, their devices/mobile devices, and the system's cloud server, and also a key agreement scheme together with the help of Elliptic Curve Cryptography (ECC).

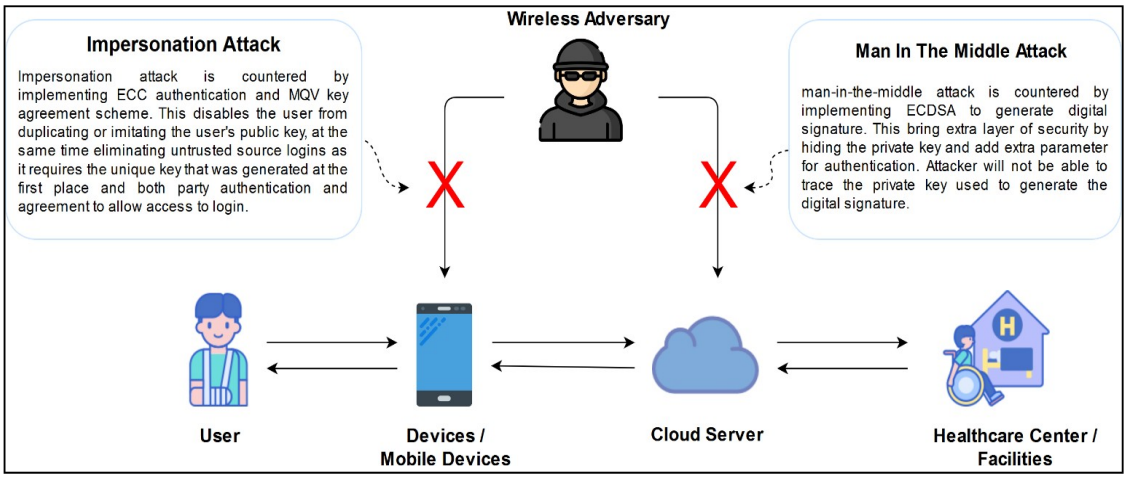

Fig. 2 - Network model of the proposed system

Algorithm 1 : Asymmetric key generation

User Asymmetric keys = (A, a), A user's public key, a user's private key

Cloud server Asymmetric keys $=(B, b)$, cloud server's public key, b cloud server's private key, where R $=(X, y)$, a point on an elliptic curve and $\bar{R} = (x \bmod 2^L) + 2^L$ where $L = \frac{\lceil \log_2 n \rceil + 1}{2}$ and is the order of the used generator point P. So $\bar{R}$ are the first bits of the first coordinate of R.

Step 1

User key pair (X, x), $X = xP$, x is randomly-generated values, P is a point on an elliptic curve.

Cloud server's key pair (Y, y), $Y = yP$, y is randomly-generated values, P is a point on an elliptic curve.

Step 2:

User calculates $S_a = x + \bar{X}a \bmod n$, X sent to Cloud while

Cloud server calculates $S_b = y + \bar{Y}b \bmod n$, and Y sent to Cloud.

Step 3:

User calculates $K = h * S_a(Y + \bar{Y}B)$,

Cloud server calculates $K = h * S_b(X + \bar{X}A)$, where h is the cofactor.

The secret key K generation for communication was successful, K is a symmetric-key algorithm that can be derived.

When a user tries to login into the medical center's system, as well as sending and retrieving data, there should be a validation process in which in this case, an authentication, to confirm that the data that is going to be transferred is truly from a trusted source. We proposed a mutual authentication method to be implemented in between the process from a user and the system's cloud server through their devices. The moment when data from a user is requested to be transferred to the healthcare system, Asymmetric key Cryptography; private key and public key generation, will be implemented through the approach of ECC. Implementing this to the proposed system means, senders will be allowed to encrypt a message using the receiver's public key, albeit, the encrypted message is only decrypt-able using the receiver's very own private key. To implement it in terms of mutuality, both sender and receiver will have their public and private keys. The ECC implementation is to ensure that the keys are thoroughly secured and is not copy-able. Algorithm 1 shows the Asymmetric key generation model.

4.1 Key Agreement Scheme

Key Agreement scheme is also to be conducted in the transfers of data between the users and the cloud server. Key Agreement is a key generation procedure where the generated secret keying material is produced as a result of the information entered by two participants so that no one other individuals can provide the exact value of the secret keying material. Only if the user enters the right keyword that was sent, will he/she be able to access the account. It is the same concept that we proposed to be implemented in the hospital account login systems, perhaps a keyword will be sent to the user's registered mobile device number, and it is to be keyed in into the account login interface. Thus shields the system against impersonation attacks as it requires both party access agreement to be able to access any account and a secret key to allow the movements of data in the system. Algorithm 2 shows the detailed explained scheme.

Algorithm 2 : Key Agreement Scheme

Step 1

Cloud Server calculates: $K = h * S_b(X + \underline{X}\ A) = h * S_b(xP + \underline{X}a)P = h * S_b S_a P$

Step 2:

User calculates:

$K = h * S_a(Y + \bar{Y}B) = h * S_a(yP + \bar{Y}bP) = h * S_a(y + \bar{Y}b)P = h * S_b S_a P$

Thus, when the shared secrets K are indeed the same, both parties are authenticated, with $K = h * S_b S_a P$

4.2 Attacks

As for the man-in-the-middle attack, it always occurs during communication between 2 users. Data transmission are one of the important operations in the medical system. In the proposed system, all message will be directed to the cloud-first before sent to the actual receiver. Therefore, secure data transmission is needed to ensure data integrity of the hospital each time a user asks to retrieve data from its cloud storage and to block man-in-the-middle attack. One of the concepts of man-in-the-middle attack is the attacker intercept the communication between two entities that are communicating with each other without an intermediary. To address this problem, we have proposed a new solution for authentication, which consists of two-phase, which is the signature generation and authentication process. Signature generation takes place before the message reaches the cloud. Once arrived, the authentication phase will be triggered.

4.3 Signature Generation Scheme

In the signature generation phase, it implements the Elliptic Curve Digital Signature Algorithm (ECDSA) to hide the private key and generate the digital signature. ECDSA need private/public key pair to be used to generate digital signature together concerning a particular group of domain parameters; it is also used for verification [5]. When a user sends a message to another user, such as patient to the physician and before the message is sent to the cloud, the digital signature will be generated for the message based on choosing the Elliptic curve field, which is the group of domain parameters, randomly paired with the private key of the patient. Signature generation then uses the patient private key, selected curve fields, and patient private key to hide their private key. The generated digital signature is then needed to be verified by sending it to the authentication phase for verification along with the message. Algorithm 3 shows the mathematical model for this phase.

Algorithm 3 : Signature Generation Scheme

Choose unique constant and random integer k within the interval $[1, r-1]$.

Compute 1 and 2. If $R = 0$ then back to the previous step.

1. $kG = (x1, y1)$
2. $R = x1 \bmod r$

Step 2:

let r = the order of prime number (Decimal), R and G = elliptic curve parameter

3. Compute $k^{-1}\ mod\ r$
4. Compute 4-a. If $S = 0$ then go to the first step.

   let S = signature, h = secure hash function, m = message

Message signature is generated which is $s = (R, S)$.

5. Security Analysis

Confidentiality, Integrity, and Availability (CIA), as well as non-repudiation, has always been the main concern and the standard for computer security as it covers a wide range of safety levels in a computer system. When we want to store data, especially in the medical centers, indeed it must have strong security and shields against attackers or data-theft. It is perceived that the security of this information should only be emphasized for inside facilities itself, but also on the user's devices or any other external devices that try to access the systems cloud servers. The sole purpose of the creation of the CIA triad was to act as a benchmark standard for information security evaluation and implementation, regardless of the system and organization structure.

5.1 Impersonation Attack Mitigation

Evaluating the mitigation on an impersonation attack on the hospital systems, suppose an adversary has successfully stolen a patient's public key, A. In the event when a hospital's system only implements the asymmetric key cryptography for its system access authentication, an attack from an adversary; for example, he/she send a valid login request with the intention to upload fake data into the hospital's health-tracking record in its cloud server using the hacked patient's public key, it would have been a successful attack as there is only a single layer of security exists that is needed to be breached by the adversary. However, in the event when a proposed solution is implemented, after successfully gaining a patient's public key, the adversary will be forced to face a second layer of authentication which is a key-agreement scheme as mentioned in the discussion of the proposed solution. The key generated in this scheme was produced through the implementation of a mathematical algorithm based on the Menezes-Qu-Vanstone concept or also known as Elliptic Curve Menezes-Qu-Vanstone (ECMQV). The key is generated real-time and will be valid only for seconds, similar to TAC and also QR codes that are being implemented in the modern systems nowadays. Based on Fig 3, from step 1, the phase where the key is being generated real-time is based on x, randomly-generated values. The value would change over time. Thus, this fails the attacker from being able to bypass the security as the key-generated is valid only for a certain time and is only available and sent to the real patient's mobile device. Also, to get the exact value of the generated key, the adversary would need to calculate x, the patient's private key, and h, its cofactor, based on the formula in step 2 and 3. The adversary could never compute this as he/she does not know the value of x; thus, will also not know the value of h. The adversary would never know what the correct key is unless the patients give it themselves. It also helps to notify the patient that an anonymous source is trying to use his/her account to send unauthorized data into the hospital's cloud storage. It proves that a proposed solution is secure enough to be implemented as an authentication protocol.

Curve bit length	Private key generation (ms)	Public key generation (ms)	Sign generation (ms)	Sign verification (ms)
P-521	126	17	642	4454
P-384	16	17	251	2123
P-256	19	18	110	876
P-P224	1	16	79	689
P-192	1	16	47	516

Fig. 3 - Time analysis of different curves

5.2 Man in the Middle Attack

Evaluating the mitigation on an impersonation attack on the hospital Suppose A intercepts the message m and attempt to modify the m to create a valid message. The generation of the public key using ECC involves computing the

elliptic curve, P, where X=xP. To crack the elliptic curve, *A* need to discover the private key, x, since, during signature generation, x is concealed. Based on Fig 4, to compute x given xP and P will roughly take 2^(n/2) operations. For example, a key length of 192 bits (the e size that was recommended by NIST for a defined over prime finite field curve, as it is considered to be the smallest), about 2^96 operations will then be required for A to compute. If a supercomputer is owned by and that its capabilities are to perform a billion operations per second, which would cost around trillion years to find the key. Therefore, propose a digital signature algorithm which implement ECDSA can mitigate man-in-the-middle attack. If decides to inject multiple message request, authentication algorithm will validate the signature by computing the value of validation using $U_1G + U_2Q = (x0, y0)$ and $v = x0 \bmod r$. If $v = R$, then m is valid. Otherwise, invalid.

5.3 Comparing the Key Size

RSA keys usually used in SSL certificates and the size of RSA keys continue to enlarge to maintain adequate cryptography strength. For this reason, ECC becomes a substitution to RSA. ECC and RSA key types receive the same crucial property of being asymmetric algorithms. However, ECC presents the same level of cryptography strength in a much smaller key size. In addition, ECC will help to improve security by cut down the computational requirement. From Fig 5, we can see that ECC key size is much smaller than RSA yet ECC is able to provide identical cryptographic strength as RSA. Smaller key size in ECC is important as devices with limited storage can store the key and would not take too much space. Besides that, smaller key sizes can result in a speedier SSL handshake and stronger security.

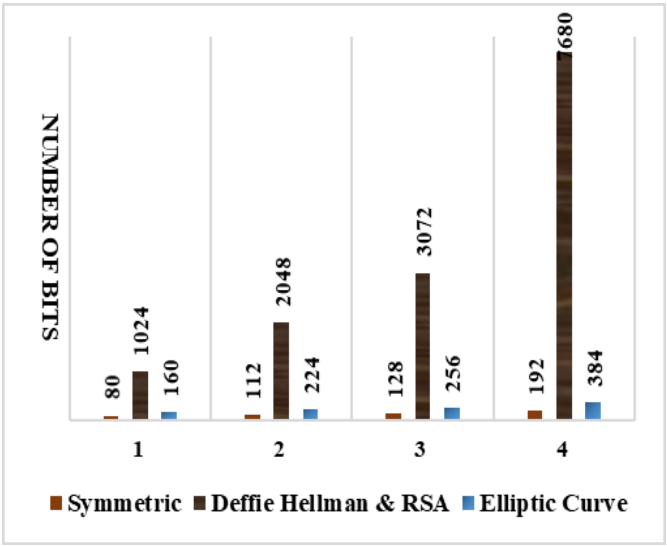

Fig. 4 - Key strength comparison

5.4 Comparing RSA Keys to ECC Keys

ECDSA is way better than RSA in term of security while having shorter key lengths. ECC uses 106 bits' key size equates the security strength of RSA which uses 512 bits' key size. ECC that uses 106 bits takes 104 years to break, the same time RSA that uses 512 bits. However, with the advancement of technology, it eases us in the process of factoring values, including large numbers, all the while it keeps on upgrading itself. An ECDSA key decryption, on the other hand, forces us to crack the Elliptic Curve Discrete Logarithm Problem (ECDLP). Since ECDSA was independently introduced by Koblitz and Miller in 1985, no major progress was made by the mathematical community in improving algorithms to solve problems that are related to it.

Suppose during the communication between a doctor and his patients in an attempt to make a medical appointment through a channel, Man in the Middle attack may happen. This is where an attacker intercepts the message for his own usage. To evaluate the traceability and anonymity of solution, a scenario is described as such, In the proposed solution, we tackle the problem using the implementation of ECC authentication. In the proposed solution, we tackle the problem using the implementation of ECC authentication. The solution uses a random nonce, $ri\ rj$ and current timestamp, Ti.Referring to Algorithm 1 to 3, the presence of $ri\ rj$ and TI, the value of ai, bi, cj and kij as shown above, becomes dynamic and becoming "unique" in all the messages for every session. The value of ai and bi of each message is calculated by CNj when timelines match. Value of cj is calculated when verification matches and CNj chooses the current timestamp of $T2$ and 160-bit random nonce, rj. Value of Kij is the session key which will be shared to the user

and the next message (for future secure communication). There is no direct indication of ID, therefore greatly add the anonymity and un-traceability of the messages sent.

6. Conclusion

In conclusion, an efficient scheme has been proposed to design a generalized yet strong authentication protocol that is to be implemented in medical systems. It fulfills the scope which is within the medical infrastructure, both the cloud storage and the hardware, as well as third-party devices, was covered within the authentication protocols. The proposed solution was to incorporate ECC encryption, specifically MQV – ECC, with Key Agreement Scheme and also using ECDSA, a variant of ECC to exhibit signature generation features for the authentication of the medical centers. The analysis shows that these methods would strengthen the security of the medical system's data protection to be much better and much stronger.

Acknowledgement

The authors would like to thanks Faculty of Computer Science and Information Technology (FCSIT), Universiti Malaysia Sarawak and Department of computer Science, Prince Sultan University, Riyadh, 11586, KSA for their support.

References

[1] Xiong, H., Tao, J., & Yuan, C. (2017). Enabling telecare medical information systems with strong authentication and anonymity. IEEE Access, 5, 5648-5661

[2] Liu, X., & Ma, W. (2018). ETAP: Energy-efficient and traceable authentication protocol in mobile medical cloud architecture. IEEE Access, 6, 33513-33528

[3] Quaum, M. A.; Haider, S. U.; Haque, M. M. (2018). An Improved Asymmetric Key Based Security Architecture for WSN. IEEE 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2), 1-5

[4] Das, A. K..; Wazid, M.; Kumar, N., Khan, M. K., Choo, K. K. R., & Park, Y. (2017). Design of secure and lightweight authentication protocol for wearable devices environment. IEEE Journal of biomedical and health informatics, 22, 1310-1322

[5] Balan, K., Khan, A. S., Julaihi, A. A., Tarmizi, S., Pillay, K. S., Abdulrazak, L. F., & Sallehudin, H. (2018). RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks. International Journal of Advanced Computer Science, 9, 298-304

[6] Manickam, S., & Kesavaraja, D. (2016). Secure multi server authentication system using elliptic curve digital signature. IEEE 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), 1-4

[7] Malik, K. M., Krishnamurthy, M., Alobaidi, M., Hussain, M., Alam, F., & Malik, G. (2020). Automated domain-specific healthcare knowledge graph curation framework: Subarachnoid hemorrhage as phenotype. Expert Systems with Applications, 145, 113-120

[8] Ogudo, K. A. (2019). Analyzing Generic Routing Encapsulation (GRE) and IP Security (IPSec) Tunneling Protocols for Secured Communication over Public Networks. IEEE 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (ICABCD), 1-9

[9] Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors, 19, 4954

[10] Gismalla, M. S. M., & Abdullah, M. F. L. (2017). Device to Device Communication for Internet of Things Ecosystem: An overview. International Journal of Integrated Engineering, 9, 118-123

[11] Mehmood, A., Natgunanathan, I., Xiang, Y., Poston, H., & Zhang, Y. (2018). Anonymous authentication scheme for smart cloud based healthcare applications. IEEE Access, 6, 33552-33567

[12] Javed, Y., Khan, A. S., Qahar, A., & Abdullah, J. (2017). EEoP: A lightweight security scheme over PKI in D2D cellular networks. Journal of Telecommunication, Electronic and Computer Engineering, 9, 99-105

[13] Zhou, J., Lin, X., Dong, X., & Cao, Z. (2014). PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system. IEEE Transactions on Parallel and Distributed Systems, 26, 1693-1703

[14] Khan, A. S., Javed, Y., Abdullah, J., Nazim, J. M., & Khan, N. (2017). Security issues in 5G device to device communication. International Journal of Computer Science and Network Security, 17, 366-373

[15] Liu, X., & Ma, W. (2018). ETAP: Energy-efficient and traceable authentication protocol in mobile medical cloud architecture. IEEE Access, 6, 33513-33528

[16] Khan, A. S., Abdullah, J., Zen, K., & Tarmizi, S. (2017). Secure and Scalable Group Rekeying for Mobile Multihop Relay Network. Advanced Science Letters, 23, 5242-5245

[17] Wazid, M., Das, A. K., Kumar, N., Conti, M., & Vasilakos, A. V. (2017). A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE journal of biomedical and health informatics. 22, 1299-1309
[18] Jevremovic, A., Veinovic, M., & Shimic, G. (2017). An overview of current security and privacy issues in modern telecommunications. IEEE 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), 119-123
[19] Sah, B., & Jha, V. K. (2019). Reversible Data Hiding Technique using Novel Interpolation Technique and Discrete Cosine Transform. International Journal of Integrated Engineering, 11, 1-9
[20] Abidin, M. H. Z., Suchaad, S., Mashiko, K., & Ismail, N. (2019). Ethereum Blockchain Network Implementation for IoT Platform. International Journal of Integrated Engineering, 11, 1-6
[21] Khan, A. S., Halikul, H., Jambli, M. N., & Thangaveloo, R. (2017). Mitigation of Non-Transparent Rouge Relay Stations in Mobile Multihop Relay Networks. Advanced Science Letters, 23, 5246-5250