ECC based multifactor authentication and key generation system for IoT Healthcare

Bharathi Malakreddy A[1], Vani G[2]

[1]Dept. of CSE BMS Institute of Technology, Bangalore, Karnataka, India
[2]Dept. of CSE BMS Institute of Technology Bangalore, Karnataka, India
Bharathi_m@bmsit.in, [2]vanigkathare@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: The Internet of Things is a collection of digital sensors linked to the Internet. The IoT Explosive Growth and the massive increase in wireless technology are unfolding novel opportunities for enlargement in numerous areas such as Transportation, coaching, farming and particular in medical. An introduction of Internet of Things over medical apps brings numerous advantages including cost savings over lower hospital visiting expenses, healthcare provider expenses, transport expenses, human resource expenses, and insurance expenses. However, greater use of IoT facilities in healthcare apps has resulted in increased data protection and privacy issues, particularly like in the medical area. In reality, medical applications are susceptible with information violation as well as expanding safety problems owing to expanding the amount of access points through electronic medical records to sensitive information. Although a number of researchers have performed safe authentication for lightweight multi-factor, it is a very important to develop and build a safe authentication model that provides a substantial level of safety against various assaults such as impersonation attacks, mid-attack man and unidentified important sharing attacks. In this paper, to cover this security gap (authentication &amp; authorization), the suggested model is a new Multifactor Authentication and Key generation system that is based on the Elliptical Curve Cryptography (ECC) that can overcome an existing security (authentication and authorization) challenges in IoT healthcare applications.

Keywords— Security challenges, Authentication, Authorization, ECC, Elliptic Curve Cryptography, IoT

1. Introduction

The Internet of Things has been making important progress in all possible fields over the last few years; ever ything is smart, locatable and internet-addressable. IoT has increased significance in healthcare area and monitoring of parameters related to health. It gives opportunity to continuously monitor the various health related parameters remotely and analyse the various factors in real time. It gives numerous of highpoints like consistent remote checking of information. Thus, the patients can observe day by day by utilizing sensors in Personal Digital Assistant (PDA) or wearable gadgets [1] Security is one of the main factors in the IoT environment. Securing the sensitive real time data over the air as well as at interface points plays important role in the development of IoT healthcare solutions [2]. Over the recent years, the number of cyber-attacks and cyber-crimes has evolved exponentially. The attackers use restricted devices mostly because they have low or no security at all [3]. The network security protocols are used for a traditional internet cannot be used to IoT due to device constraints and low network throughput. IoT needs fresh communication and security protocols with low computational complexity, lower performance, low power consumption, etc. To secure networks and devices, strong authentication protocols are required [4]. An authentication is the method of verifying the identity of the object. The greatest safety procedures condition that at least two distinct credentials should be included in the authentication protocol. IoT authentication is challenging since it is impossible for the details involved in IoT background cannot manage to provide cryptographic techniques of high computational density in a traditional internet. The computational density limit can improve via using the scheme that uses middle-ware like computing gateway. There are different types of security issues that should be a dealt with authentication and authorization to ensure restricted access (which is the point of our examination), data privacy using the various encryption methods, data integrity during the transactions etc. The fundamental objective is to make safety an essential part of IoT-based human services innovation for secured information exchange, use and trade. This paper proposes a model on ECC based Multifactor Authentication and Key Generation Scheme, which offers high level of security (authentication & authorization) against various attacks and prevalent verification with less expenses in medical services IoT based applications.

2. Related work and motivation

In order to secure sharing of healthcare record in IoT application and to retain the security of health information, the various types of cryptographic methods haves been proposed. Each proposed method has its specific advantages and drawbacks. The following table 1 gives an overview of the problem statement, the techniques applied and its benefits.

SUMMARY OF PROBLEMS TECHNIQUES ON SECURITY HEALTHCARE DATA

This paper outlines the background study regarding the existing approach & techniques and had analysed its computational efficiency. Research work shows that the level of security provided by various algorithm or approaches using ECC communication can take place via a secure channel, which can overcome key exchange make it susceptible to man-in-middle of an attack. Most of the algorithms party involved in the key exchange. To overcome man in middle of attack an ECC based Multifactor Authentication and Key generation scheme cab be used.

TABLE: I

Author name and year of publication	**Problems**	**Techniques Applied**	**Advantages**	**Limitations**
Serial Zeadally et.al in 2019	Achive RFID authentication between FID tags, RFID reader and server	RFID authentication systems based on ECC are utilized in cryptographic techniques like hash function and public key operation	Proposed an enhanced system to solve key challenges for the public	RFID authentication schemes based on ECC can't satisfy particular mutual authentication as vulnerable to various types of malicious attacks
Mourad Talbi1et.al in 2019	Quantized speech image for secure Io which provides substantial security	Secure IoT, image histogram and light weight encryption algorithms are used	Sending confidential data to multiple devices with high level of security	Light weight algorithms do not always use security efficiency trade-offs
Jose Costa et al in 2018	Overcome user credibility in user application that reduce the risk of malicious user filtering their systems	Light weight Two Factor Authentication (TFA) protocols with web services	Services can be used as a single sign on frame work which allows multiple services to switch to different services via TMA work	Biometrics has a high implementation cost and hence for many organization, it would not be a possible option to use

Haiping Huang et.al in 2018	An Information security and privacy preservation	Context of the health scheme, Send Receive proto groups and Homo morphic encryption modules are used	Evaluate the scrambled health data and immediately feedback the results & improved the effectiveness of healthcare systems with low cost compared with the current system	The systems accuracy in diagnosis is not optimal& health care system can't analyse the sudden diseases
Kumar S. A et.al in 2017	The malevolent code attacks, Software defencelessness and phishing attacks	Keep In Touch (KIT) and Near Field Communication (NFC) and RFID are used	An application system code which activates the program to break-down in the major security challenges in the application layer	The production of most dominant operating system for IoT is still a great challenge for developers to maximize the trust of people on IoT network
MoonBae et.al in 2016	To address the security issue of the patient data considering their health data	Secure user reporting framework with a dual Hash function and single time encryption key are used	A encrypted communication mechanism with a hash function and a single time encryption between a client and hospital to fix the safety issues and an OTP input value generated	Care is crucial because of social involvement in IoT healthcare tenders with strong and effective secure communication network between healthcare sensors, actuators and patient
Vijayaraghavan in 2016	Vulnerability detected and various kinds of DOS attacks	Infrastructure for data security and IoT privacy	Suitable security by making the appropriate solutions accessible as soon as system identifies any vulnerability	Different kinds of risks correlated with a SQL injection attack

Zhang. Y. et.al in 2015	To observe patient health status more effectively	Mobile healthcare monitoring system with mobile device and web service	Facilitate remote diagnosis to provide timely support for real time notification, alert services through an emergency like heart attack and paralysis attack, etc.	In order to drain data security leakage, the dangers of any communication with networks and other end users need to be constantly identified
Sawand A et.al in 2015	Security threats targeting E-healthcare monitoring system	Architecture framework and essential service components	To achieve the robust, data efficiency and secure health care monitoring	To achieve high-quality and potential solutions, existing solutions can be analysed and identified
Guo et.al in 2014	Authenticity of Privacy preserving attributes for personal health records.	Privacy preserving attribute-based authentication system in M-health care network. The attribute-based authentication schemes designed are used	Better care and better quality of life to enable to Patient –To-Physician and Patient-To-Patient communication using components E-health system, M-health using mobile devices	The possible leakage of privacy from mobile devices is the major concern for patients. The evaluation criteria used might not have been appropriate
Ning et.al in 2014	Authentication schema	User authentication and aggregated	Secure protection among ubiquitous things	User attributes-based access control policy which needs to be further studies

3. Methodology

The proposed IoT healthcare application solution consists of interaction between three different systems. Each system interfaces are protected by authentication at its entry point. In the lightweight encryption system, the implementation process includes in the architecture design of ECC encryption model. Since, for the better secure data transmission process the ECC model can be enhanced generation of random keys. In that enhancement wok, we propose a hybrid model of data encryption architecture by the combination of ECC model with Truncated Quantum Hashed Signature (TQHS) based architecture design to develop a lightweight encryption system. This architecture mainly focused on the random key generation system to reduce the time complexity than from the traditional model of ECC encryption system.

Here, the proposed Truncated Quantum Hashed Signature (TQHS) method integrates the Hashed signature technique for random key generation model for the better security complexity. The Hashing models are designed by the Quantum model of architecture that truncates the looping design with appropriate components that can achieve reduced amount of components and device utilizations. This results in lightweight architecture of encryption system in the IoT application.

4. Experimental Results and Discussion

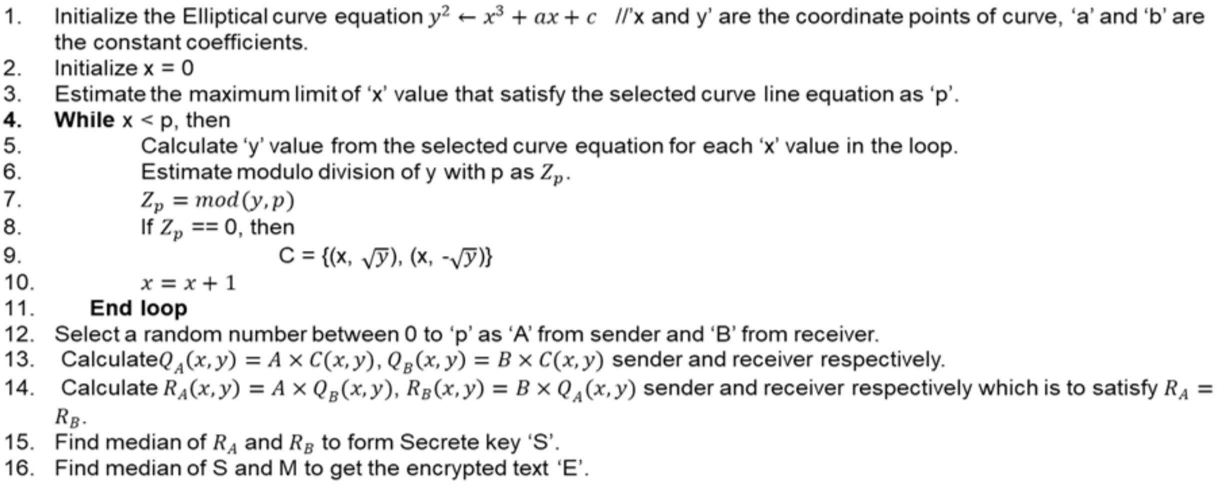
A. Encryption Process

To develop a novel hybrid encrypt algorithm for data exchange:

The present encryption shows the average encryption where the x-axis shows the timestamp for encryption in regards to the parameter sets on hybrid Encrypt. A representation of the average can evaluated, relative to the server timestamp. The fastest parameters of the key generation are in addition the fastest when it comes to encryption. Interestingly, 112 bits parameter is the slowest when encrypting but it was second fastest when generating keys. The parameter was the second fastest when generating keys out of the parameters with 128 bit but is the slowest when it comes to encryption.

Input: Plain text 'A novel light weighted ECC'
Encrypted

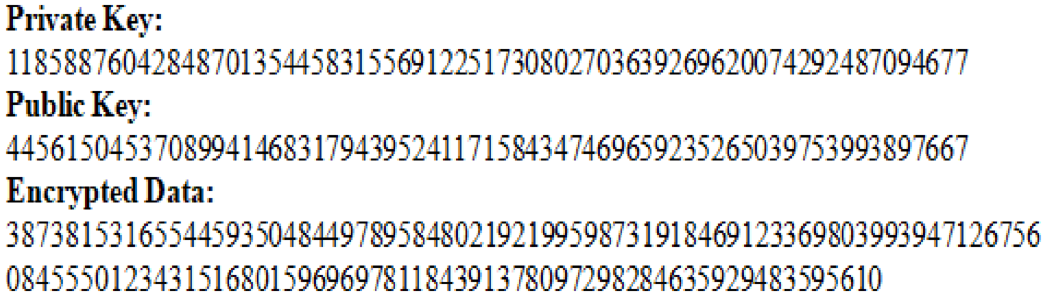
Output:
51436339934267800086770953836507484702679748686639568627977265427712842971477297091474437361039838343012357318592081059691552386367855'



```
1.  Initialize the Elliptical curve equation $y^2 \leftarrow x^3 + ax + c$   //'x and y' are the coordinate points of curve, 'a' and 'b' are
    the constant coefficients.
2.  Initialize x = 0
3.  Estimate the maximum limit of 'x' value that satisfy the selected curve line equation as 'p'.
4.  While x < p, then
5.          Calculate 'y' value from the selected curve equation for each 'x' value in the loop.
6.          Estimate modulo division of y with p as $Z_p$.
7.          $Z_p = mod(y,p)$
8.          If $Z_p$ == 0, then
9.                  C = {(x, $\sqrt{y}$), (x, -$\sqrt{y}$)}
10.         $x = x + 1$
11.     End loop
12. Select a random number between 0 to 'p' as 'A' from sender and 'B' from receiver.
13. Calculate$Q_A(x,y) = A \times C(x,y)$, $Q_B(x,y) = B \times C(x,y)$ sender and receiver respectively.
14. Calculate $R_A(x,y) = A \times Q_B(x,y)$, $R_B(x,y) = B \times Q_A(x,y)$ sender and receiver respectively which is to satisfy $R_A =$
    $R_B$.
15. Find median of $R_A$ and $R_B$ to form Secrete key 'S'.
16. Find median of S and M to get the encrypted text 'E'.
```

B. Key generation

The above proposed algorithm provides the secret key sharing mechanism involving two different parties (sender and receiver exchanging a secret key). They are exchanging some confidential data. They have to agree on certain specific parameters to encode and decode the data. The arrangement of Public and Private Key is used to regenerate the confidential information obtained on the receiver side along with encryption decryption logic. They both have Private Key and public key at the end. The information to be transmitted is multiplied by the side secret key of the transmitter. At the receiver end, the freshly created multiple data are obtained and its data are regenerated using the various steps given in the decryption algorithm. Secure authentication and authorization algorithm are used to build a shared secret key which can be used for secret interaction while sharing information over a public network using the Elliptical curve cryptography (ECC) to generate points and use the variables to get the secret key.



Private Key:
1185887604284870135445831556912251730802703639269620074292487094677

Public Key:
4456150453708994146831794395241171584347469659235265039753993897667

Encrypted Data:
387381531655445935048449789584802192199598731918469123369803993947126756
0845550123431516801596969781184391378097298284635929483595610

C. Decryption Process

The present encryption shows the average decryption time. The x-axis shows the timestamp for the decryption in regards to the parameter sets on hybrid Encrypt and the relative to the server timestamp. This shows how long it takes to decrypt in regards to different strength settings (bits), where the parameter had the shortest time and the longest time. When comparing decryption samples based on security bits in implemented for practical approaches, it is possible to observe the similarities between encryption and decryption times. However, the times are overall slower for decryption compared to encryption.

D. Possible Outcome

Based on the analysis of the literature and the findings of the Hospital case study, this work proposes an IoT Security Risk Management methodology for Medicare with includes three categories. Such as are Human Privacy, Reliable Process and Data. The new proposed model focuses on ensuring the state of the art and upgraded IoT technology infrastructures are in place. The future authentication and authorization will been mathematically compared with elliptic curve cryptosystem. To achieve the required level of secure authentication and bypass authorization, the comparing the three parts: key generation, encryption and decryption combined, there is a clear best performer for 112 bit for each level of security, the best performer is the fastest in all three parts. The conclusion from the test is that the hybrid Encrypt performed well with high speed overall under the key generation, encryption and decryption phases.

5. Conclusion

This paper provides an overview and analysis of an authentication & authorization in the IoT healthcare sector. Authentication and authorization are two significant security challenges in the IoT based healthcare system. Multi-factor authentication methods have several benefits in the healthcare sector where security challenges exist. Few solutions are discussed in order to resolve the issues and reduce the risk. The implementation paper also details the authentication issues, various kinds of security bouts, risks and security holes in healthcare organizations and how multi-factor authentication helps to improve the security when sensitive data is transmitted over the air. All the possibilities are taken care to make sure that the patient data is secure, and its integrity is ensured. There are numerous opportunities are there to make the authentication algorithms even more secure and strong by ECC based mutual authentication or using cryptographic hash functions for data encryption or by using authenticated encryption along with a digital signature or a combination any of the above two methods to create an authentication and authorization algorithm and encryption method to the overall benefit of healthcare applications.

Acknowledgements

I would like to convey my appreciation to Sonata Software Ltd., for providing me a pleasant environment and support at my workplace and would like to thank Dr. Bharathi Malakreddy A, Professor and HOD, most sincerely for her precious advice, encouragement and recommendations.

References

1. Vani G, Bharathi Malakredd A, “Survey on Security challenges in IoT in Healthcare domain”, in the ICNTET, 2018, ISBN- CFP18P34-PRT/978-1-5386-5629-7.
2. Vani G, Bharathi Malakreddy A, “A review on identification & analysis of security issues & challenges of IoT based Healthcare”, International journal of innovative technology & exploring engineering (IJITEE) ISSN - 2278-3075, Vol. 8 Issue:4, February 2019, pp. 546-549.
3. Vani G, Bharathi Malakreddy A, ‘Security challenges in IoT in the Healthcare Domain”, September 2016, DOI No. IAECS IRAJ DOI 5592, pp.141-144.
4. Debiao He et.al, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography”, in ‘IEEE INTERNET OF THINGS JOURNA’, Vol. 2, No. 1, February 2015.
5. Mourad Talbi1et.al, Application of the Lightweight Encryption Algorithm to the Quantized Speech Image for Secure IoT, 2018, DOI: 10.20944/preprints 201802.0096. v2.
6. Jose Costa et al, “Middle Man: An Efficient Two-Factor Authentication Framework”, third IEEE International Conference on Communication, Computing, Control and Automation, Pune, India 17th to 18 Aug 2017”, IEEE.
7. Dylan Sey et al, “A survey on authentication methods for the IoT‟, Vol.2, 2018, pp. 537-567
8. Hafizah Che Hasan et.al, “Comparison of authentication methods in IoT technology”, Vol. 12, No. 3, 2018
9. Lee T, ‘Verifier Based three party authentication schemes’, Vol. 38, No. 5, in 2014, pp. 464 – 472.

10. H. Zhou, X Lin et.al, “Patient Self controllable and Multi-level Privacy preserving cooperative authentication in Distributed Healthcare Cloud CS”, in 2014, pp.1693-1703
11. Rehiman K Aet.al, ‘A Secure Authentication Infrastructure for IoT Enabled Smart Mobile Devices’, in 2016, in Vol. 9, DOI: '10.17485/ijst/2016/v9i9/86791.
12. LellaA, Martin B et al, ‘The Mobile App Report. available at– www.comscore.com/Insights/Presentations and-Whitepapers’, in 2015.
13. Anurag Shukla et.al, “A Survey on Next generation Computing IoT Issues & Challenges”, in International Journal of Pure and Applied Mathematics, Vol. 118, No.9 2018, pp. 45-64.
14. Shantha Mary, Joshitta R et.al “Authentication in Internet of Things Environment: A Survey”, Vol. 6, Issue 10, October 2016, ISSN:2277 128X.
15. Isra Ahmed Zriqat, 'Security and Privacy Issues in E-healthcare systems - Towards trusted services', Vol. 7, pp. 9, 2016.
16. Z. Shelby, “The Constrained Application Protocol (CoAP)”, Internet Engineering Task Force (IETF), 2014.
17. Alok Kulkar et al, “Healthcare applications of the internet of things– A Review”, Vol. 5, 2014, pp. 6229-6232.
18. Hafizah Che Hasan et.al, “Comparison of authentication methods in IoT technology”, Vol. 12, No: 3, 2018.
19. Rafidha Rehiman K Aet.al, “A Secure Authentication Infrastructure for Internet of Things Enabled Smart Mobile Devices”, in 2016, in Vol. 9, DOI-10.17485/ijst/2016/v9i9/86791.
20. Anjali Yeoleet.al, A Robust Scheme for “Secure communication” in IoT, in Vol 3, no.11, 2015, pp 10401- 10406.
21. Gajanayake R, Sharma et.al, ‘Privacy oriented access control for Health records’, in ‘Electronic health information journal’, 2014, pp 5
22. Liu Wet.al, ‘Cryptography’, in 3rd IEEE International Conference, Pune, India August 2017, IEEE. Available online at “ieeexplore.ieee.org/Xplore/home.jsp”.
23. Jose Costa, ‘A Two Factor Authentication scheme’, DOI: 10.13140/RG.2.2.16228.99207, Jun 14, 2017
24. Kennedy and Millard C, ‘Data security & Multifactor authentication' in Vol: 32, No. 1, 2016, pp. 91 – 110.
25. Bruce Ndibanje; Hoon-Jae Lee et.al ,’Security Analysis & Improvements of Authentication & Access Control in the IoT’, in Vol. 14, 2014, pp 14786 -14805
26. Sanaz Rahimi Moosavi et.al, ‘A Secure & Efficient authentication & authorization architecture for IoT based Healthcare using Smart gateways’, in CS Journal, published in Elsevier in 2015, Vol.52, pp. 452-459.
27. First Author and Second Author. 2002. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. (Nov 2002), ISSN NO: XXXX-XXXX DOI:10.251XXXXX.