I.J. Wireless and Microwave Technologies, **2019, 1, 1-10**
Published Online January 2019 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2019.01.01

***Available online at** http://www.mecs-press.net/ijwmt*

A Hybrid Cryptosystem to Enhance Security in IoT Health Care System

Kavitha.S*, P.J.A.Alphonse

Department of Computer Applications, National Institute of Technology, Tiruchirapalli, TamilNadu, India

Received: 08 July 2018; Accepted: 16 October 2018; Published: 08 January 2019

Abstract

Internet of Things (IoT) based health care system provides an essential interface between tiny devices and customers, who require customary checking by remedial focus. The technological innovation is important to guarantee the data protection and security among customer and devices, though it is vulnerable by various security assaults. The cryptographic technique is a prominent method for data protection in a healthcare management system. Single cryptographic algorithm based solution suffered to provide efficient security as its high probability of attacks. So this paper proposes a hybrid cryptographic algorithm that secures the sensitive medicinal information in IoT health care system. The proposed hybrid algorithm is dealing with various security attacks in a proficient way, and also increases its performance when compared to other cryptographic algorithms.

Index Terms: Attacks, Hessain Curve, Diffie Hellman, AES, IoT security.

1. Introduction

IoT is involved in the growing occurrence of devices with distinctive identifiers and able to transfer data over the network automatically. IoT communication is established among devices to a device, vehicle to vehicle, smart energy grids, home automation, wearable computing devices, etc [1]. It is endeavoring anxiously in safeguarding devices and networks because each domain has its requirement and challenges. One among the beneficial technological revolution enables health care system in IoT framework.

Recent day's people are moving with high intensity of workout that leads to low/high blood pressure, heart

* Corresponding author. Tel.:
E-mail address: kavi.parama@gmail.com, alphonse@nitt.edu

attack, stroke, mental stress, etc. It is imperative to search out a solution for these diseases in place through an IoT health care system. When the patient connected with an IoT health monitoring system, they get immediate action from hospital/staff through suggesting drugs or an ambulance to take care of them. Data about health care system is more sensitive, that it should be secured, because there is a probability of data corruptions and mislead by attackers [2].

The consequence absent of security in the health care system leads to permanent health, loss of the patient, they are unable to get immediate health care attention [3, 4]. The existing cryptographic algorithms are focused on ensuring security in particular infrastructure and safeguard the available services. But the design and management of IoT framework are vulnerable due to the wide range of security threats and attacks [5, 6]. Those security issues and ever-changing attacks can't be managed by a single cryptographic algorithm [7] in spite of that, and the security system must empower and ensure that data will be traveling over trusted nodes. The better level of security achieved through the selection of cryptographic algorithm that depends on the devices connected in the IoT environment. Therefore, this paper introduces a hybrid cryptographic algorithm to enhance security system, combines symmetric and asymmetric hybrid cryptographic algorithms to handle security issues efficiently.

The rest of the paper organized as follows, Section II discusses various algorithms applied in IoT health care system to handle security issues. Section III represents the working procedure of end-to-end security system and also explains the structure of the proposed hybrid algorithm. Section IV discuss the superiority of the proposed algorithm performance analyses by experimental results. Section V explained the efficiency of the proposed hybrid algorithm against the various security attacks in IoT Environment. Section VI Concludes the proposed work.

2. Related Work

This section reviews the current IoT healthcare security issues at different levels. Besides, various techniques and cryptographic algorithms were used to improve the health data security in IoT.

The secure IoT gateway architecture tries to provide solution to the domain of electronic healthcare system concern. It addresses the communication interoperability issues of aggregated sensor data which was solved using Public Key Cryptography(PKC) algorithm[8]. An article [9] describes the optimized Elliptic Curve Cryptography(ECC) implementation over the IoT heterogeneous network. An optimization achieved in scalar multiplication by recovering x co-ordinate representation of the Edwards curve. Besides, the key negotiation protocol demonstrates the usability of Elliptic Curve Diffie Hellman(ECDH) implementation.

The analysis of different arithmetic formulas applied in binary representation of generalized hessian curve. To measurement of time taken to compute arithmetic operations on the curve with small parameters, and it was concluding hessian curve requires less time computation, than other curves. As a result, the generalization of the scalar multiplication improved performance in IoT security [10]. There is need to design light weight algorithm in securing data management in the IoT health care system. So the proposed bilinear Diffie Hellman algorithm computes light weight data encryption, key word trapdoor generation and data recovery with efficient computation and less communication cost [2].

Distinctive way management strategies were introduced in the paper [1, 11] for Tiny ECC implementation and analyzed framework based on a non-optimized ECDH. The proposed lightweight encryption algorithm for Secure IoT handles 64-bit block cipher key to encrypt the data. In this algorithm, substantial security was obtained in the fifth round of the encryption process. It was implemented in hardware level low-cost 8-bit micro-controller compared with benchmark algorithms [12].

In 2016, implementation of RSA (Rivest- Shamir- Adleman) and ECDH algorithms in low power devices in IoT environment, and it concludes that ECDH is superior to the RSA regarding bandwidth required to transfer the data [6]. However, these single encryption procedures were failing to perform well for IOT network. In hybrid key technology was introduced for secure IOT which includes AES and ECC. It claimed that the hybrid

cipher algorithm has easy calculation and achieves faster key distribution and provide a high level of security. Hence, ECC takes more time to compute scalar multiplication than the hessian curve cryptography [13].

Since various cryptographic algorithms were proposed to provide security in IoT there is an issue need to address. From the review analysis, providing the high level of protection with low computational complexity is a key challenging issue in IoT environment. Therefore an efficient hybrid algorithm is proposed to provide more reliable security with less computational cost than a single cryptographic algorithm.

3. Proposed Work

Due to communication limitations of IOT device security issues is motivated to provide high level of security by proposed algorithm and also essential to reduce the computational complexity of security system. The efficient security protection achieves through the twisted Hessian Curve (HC) cryptography, Diffie Hellman (DH) algorithm and Advanced Encryption Standard 128 bit (AES) algorithms. These algorithms are combined to form an efficient hybrid cryptographic system named as (AES_DH)HC. The two phases of the proposed hybrid algorithm working procedure of AES_HC and DH_HC explained in Fig 1.

In the Proposed work, an (AES_DH)HC hybrid algorithm implemented as symmetric and asymmetric cryptographic mechanism, and key generation process through by combining DH and HC follow by encryption of AES with HC. The selection of HC has efficient and less computation than ECC. Since known plaintext attack is one of the issues in AES, proposed work converts the plain text into (x,y) coordinates using HC and feed these coordinates as input to AES.

Thus the key generation process of the prominent DH algorithm is powerful, computational complexity of the algorithm is exponential. Therefore, computational complexity of the DH key generation algorithm is reduced by DH combined with HC and named as DH_HC. The DH_HC algorithm generates the key at once, instead of processing at every round as in AES so, comparing the key generation of AES significantly reduced.

The implementation of AES algorithm initialized as a round key process which accomplished with a private and public key obtained from DH_HC. Up to 9 rounds of AES, private key is used to process the cipher text, at the 10th round the public key is used to prepare the cipher text. Public and private key produced by combing DH_HC replaces the AES key process. The issue noted in the symmetric AES, key encrypted by one of the asymmetric algorithms like RSA, DSA, then encrypted key to send to the concerned party. From this, viewed a symmetric key security hold by an asymmetric algorithm so, overcome this problem by introducing the asymmetric DH_HC algorithm, which manipulates its private key (pr) and public key (pu) on-demand basis. The DH_HC are structured as an AES rectangular array with four rows and number of columns for encryption and decryption process.

The security measures of confidentiality and integrity are obtained by an AES_HC algorithm, and key exchange process is accomplished by DH_HC between Router and sensors, which is overcome the disadvantage of HMAC based Key Derivation Function (HKDF) [14].

The twisted Hessian Curve in field K represented as an affine coordinate system:

$$H_E : ax^3 + y^3 + 1 = dxy \tag{1}$$

Where a=1, d is in K. the equation (1) derives the additive and doubling formula to compute the scalr multiplication of HC.

Let $p=(x_1,y_1)$ and $q=(x_2, y_2)$ then compute $r=p+q=(x_3,y_3)$ is given by the following equations.

$$x_3 = \frac{x_1 - y_1^2 * x_2 * y}{a * x_1 * y_1 * x_2^2 - y_2} \tag{2}$$

$$y_3 = \frac{y_1 * y_2^2 - a * x_1^2 * x_2}{a * x_1 * y_1 * x_2^2 - y_2} \tag{3}$$

Let p=(x,y), then 2p=(x_1, y_1) is given by the following equations.

$$x_1 = \frac{x - y^3 * x}{a * y * x^3 - y} \tag{4}$$

$$y_1 = \frac{y^3 - a * x^3}{a * y * x^3 - y} \tag{5}$$

The above mentioned additive and doubling formulas used to find points on the curve. Due to Discrete Logarithmic Problem(DLP) in HCC which is very hard to break by the attacks.

The proposed hybrid algorithm (AES_DH)HC working procedure accomplished through DH_HC algorithm , Embed message on the curve algorithm, and (AES_DH)HC algorithm.

Algorithm 1: DH_HC

Input: Equ(1), Ri, Si, G, p, a and d
Output: private key Pr and public key Pu

- Random prime selection of kr & ks used to calculate the public key
- Router R generates its Public key (PuR) and distribute to sensors S: PuR=kr*G
- Sensor generates its Public key (PuS) and send to Router R: PuS=ks*G
- Router calculates its Private Key, PrR=kr*PuS
- Sensors calculate their Private key, PrS=kr*PuR

Algorithm 2: Embed message on the curve

Input : Equ(1), p, a, d and message M
Output : (x,y) point representation of hessian curve

- Derive the points from hessian curve by prime p
- Convert the plaintext message into ASCII value of m1,m2,m3….mn
- Plot message on the curve by Computing hessian equation f(xm)
- check Whether f(xm) is a quadratic residue by Legendre symbol
- If so, yn=sqrt(f(xm) mod p
- Then m1,m2,m3….mn of xm and yn are embed message points

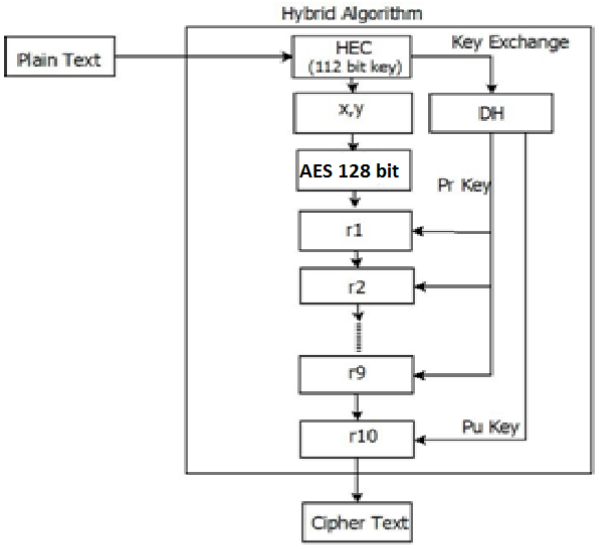

Fig.1. Structrure of Hybrid Algorithm (AES_DH)HC

Algorithm 3: Process of the hybrid algorithm of (AES_DH)HC

Input: (x,y) coordinates of the points
Output: Encrypted cipher text of the message

- Phase I - data are considered in X, Y coordinates
- Phase II – Generation of Private and Public Keys from the DH_HC algorithm
- Phase III -AES_HC include the initial round public key to starting state array
  - Calculation of sub-byte, shift rows, mix columns up to ninth round using Private key: Pr
  - Performance of the tenth round accomplished by public key :Pu
  - Considers the final state array out as cipher text End to End security establishment by hybrid algorithm (AES_DH)HC

The following statements are used to establish end to end security in IOT health care system by hybrid algorithm.

End to End security establishment by hybrid algorithm (AES_DH)HC

- Base Station (BS) initiates the on-demand routing for data collection
- Router R generates public key pu using DH_HC and send to every sensors
- Each sensor encrypts its message using AES _HC with pu, send it to its Cluster Head (CH)
- CH aggregates the collected encrypted messages and send it to the Router R
- Router R decrypts the message of CH and encrypts the clustered message before forwarded to BS
- BS forward the encrypted message from R to sender
- Finally PC decrypts the message by AES_HC

The hybrid algorithm is categorized into three phases, and every phase implemented in Matlab. The prominent structure of AES algorithm implementation includes the process of the message as curve points, round key function, key generation, encryption and decryption. In AES_HC, 10th round key process accomplished with the help of shared and public key of DH_HC algorithm, shared key is used to complete 1 to 9 regular processes and 10th round completed by public key value follow by generating cipher text. In the proposed hybrid algorithm key is hard to break due to DLP in DH_HC, which intern increases its performance significantly.

4. Experimental Analysis

The strength of the proposed security algorithm evaluated through the effect of a cipher on the entropy, computational complexity, and resource utilization. Also, memory utilization, Average Data Rate, throughput and computational time can be observed by process of key generation, encryption, and decryption.

A. Execution time

The hybrid algorithm evaluated by the necessary parameters such as time taken to encrypt and decrypt the message as in given Table 1.which shows the minimum time to execute the hybrid algorithm(AES_DH)HC so, it is proved that IOT environment requires a minimum amount of time to execute the proposed algorithm to offer noteworthy security.

B. Memory usage

The deployment of IoT takes a significant role in memory utilization. Therefore a crucial DH_HC generation algorithm is designed to generate an efficient key with the high level of security. Hence the memory utilization of proposed algorithm is evaluated using block size and key size, which is tabulated in Table 1. shows that comparison analysis Time taken to execute algorithms

Table 1. Comparison analysis Time Taken to execute algorithms

Algorithm	Block size (KB)	Key size	Time (ms)	Ref paper
AES	550	128	140	[15] [16,17]
DH	2048	1024	682.6	[16,15]
ECDH	512	160	63	[16,17]
AES_HC	550	120	138	[13,17, 15,16]
DH_HC	1024	160	58	[16,13, 17]

The algorithm execution based on blocksize, keysize and time is represented in fig2. The hybrid algorithm shows that less time than other individual algorithm execution time.

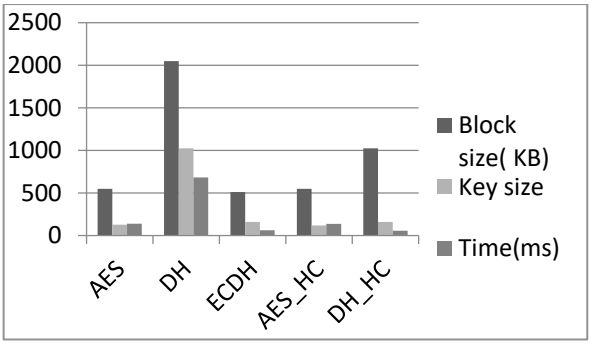

Fig.2. Algorithms in different data size.

The execution of (AES_DH)HC algorithm is used to measure the Average Data Rate (AVD_R) by different data sizes for encryption and decryption of the patient data value. Calculation of AVD_R is mentioned message and time for execution in KB / seconds in time

$$AVG_R = \frac{1}{tb}\sum_{i=1}^{tb}\frac{m_i}{t_i} \tag{6}$$

Where tb is represents the total number of plain text, m_i message in KB and t_i time in seconds.

The performance of encryption algorithm measured through throughput, which measure speed of algorithm how much time of execution in time.

$$T_P = \frac{N_b}{T} \tag{7}$$

Where N_b represents total plain text in KB measured, T is time to execute the encryption and decryption in seconds. The hybrid algorithm time taken for encryption and decryption is compared with [15]. The hybrid algorithm shows better performance through execution of different data size encryption and decryption.

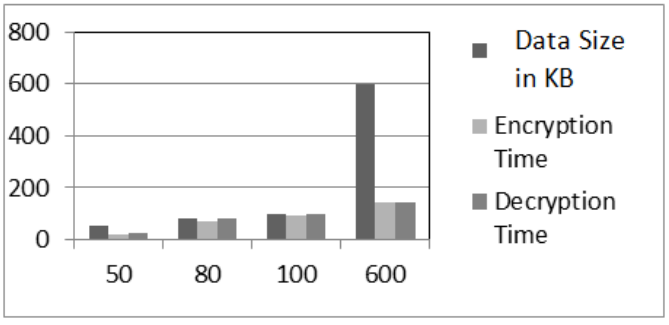

Fig.3. Encryption and decryption with different data size

Table 2. Tabulation of average data rate and throughput based different data size.

Data size in KB	**(AES_DH) HC**	
	Encryption	**Decryption**
50	19.478	22.695
80	70.932	79.84
100	93.21	100.02
600	139.672	1425.023
Average data rate	1342.672	1453.0231
Throughput	1.000842	2.05125

The performance of the proposed hybrid algorithm is compared with current algorithms, concerning block size, key size and time taken to execute. From Table 1, it can be concluded that the time taken to execute AES_HC and DH_HC are minimum compared to AES and DH. Table 2 shows that AVG_R and T_p calculations are minimized than individual algorithms. Hence, it is proved that the proposed hybrid algorithm achieves the better level of security.

C. Security attacks

Every algorithm is robust to the specific attack and security strength of these algorithms can be observed by the way to handle the attacks. The proficiency of the proposed hybrid algorithm is proved over attacks mentioned (AES_DH)HC in Table 3.

Table 3. Algorithms handled attacks

Attack / Algorithm	Known plain text attack	Related key	ECC security attack	DLP
AES	✓	✓	X	X
DH	X	X	X	✓
ECDH	X	X	✓	✓
DH_HC	X	✓	✓	✓
AES_HC	✓	✓	✓	✓
(AES_DH)HC	✓	✓	✓	✓

1. Known plaintext attack

The attack model of cryptanalysis can access the plain text and cipher text to reveal information about the secret key. Since, the message considered as (x, y) coordinates in an AES_HC algorithm, the known plaintext attack can't access plain text and cipher text easily.

2. Related Keys

An attack can perform a cipher operation using a related key or partially known keys by either symmetry key or slow diffusion with related keys. The design of the proposed hybrid algorithm is away from related key attacks and non-linear diffusion of cipher key due to DLP based key generation process.

3. Interpolation Attacks

Let n be the polynomial coefficient and m be the block cipher. If n<= 2m, then an interpolation attack can exist. In the hessian curve, coordinates point (x, y) on the cipher text attack, fail to obtain the polynomial, which is irreversible. Therefore, 100% failure to the success of interpolation attack.

Efficient arithmetic operation of DLP implements the hybrid algorithm on the hessian curve instead of elliptic curves, hence the ECC security attack is away from the IoT security [18].

5. Conclusions

IoT health care system holds sensitive medical data that need to be secured efficiently. It can be achieved by the proposed hybrid algorithm(AES_DH)HC that include the combination of AES_HC and DH_HC. To prove that superiority of the proposed hybrid algorithm (AES_DH)HC, it compared with various security measures. The performance analysis shows that the proposed key generation algorithm reduced computation time which provides faster execution significantly. The execution measures through average data rate and throughput effective way. It also proved that, the (AES_DH)HC away from known plaintext attack, related key attack, and DLP attacks. Hence, it claimed that the proposed hybrid algorithm is most suitable for the IOT health care system.

References

[1] L. Eschenauer,V. D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM, 2002, pp. 41-47.

[2] Y. Yang, X. Zheng, C. Tang, Lightweight distributed secure data management system for health internet of things, Journal of Network and Computer Applications 89 (2017) 26-37.

[3] M. Bhatia, S. K. Sood, A comprehensive health assessment framework to facilitate iot-assisted smart workouts: A predictive healthcare perspective,Computers in Industry 92 (2017) 50-66.

[4] V. Sermakani, Transforming healthcare through internet of things, in: of Project Management Practitioners' Conference, 2014.

[5] F. Zubaydi, A. Saleh, F. Aloul, A. Sagahyroon, Security of mobile health (mhealth) systems, in: Bioinformatics and Bioengineering (BIBE), 2015 IEEE 15th International Conference on, IEEE, 2015, pp. 1-5.

[6] T. K. Goyal, V. Sahula, Lightweight security algorithm for low power iot devices, in: Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on, IEEE, 2016, pp. 1725-1729.

[7] M. T. Gebrie, H. Abie, Risk-based adaptive authentication for internet of things in smart home ehealth, in: Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, ACM, 2017, pp. 102-108.11

[8] C. Doukas, I. Maglogiannis, V. Kou_, F. Malamateniou, G. Vassilacopoulos, Enabling data protection through pki encryption in iot m-health devices, in: Bioinformatics & Bio engineering (BIBE), 2012 IEEE 12th International Conference on, IEEE, 2012, pp. 25-29.

[9] L. Marin, M. P. Pawlowski, A. Jara, Optimized ecc implementation for secure communication between heterogeneous iot devices, Sensors 15 (9) (2015) 21478-21499.

[10] R. R. Farashahi, M. Joye, E_cient arithmetic on hessian curves, in: International Workshop on Public Key Cryptography, Springer, 2010, pp. 243-260.

[11] A. Liu, P. Ning, Tinyecc: A con_gurable library for elliptic curve cryptography in wireless sensor networks, in: Proceedings of the 7th international conference on Information processing in sensor networks,IEEE Computer Society, 2008, pp. 245-256.

[12] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, U. A. Shah, Sit: A lightweight encryption algorithm for secure internet of things, arXiv preprint Xiv:1704.08688.
[13] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, T. Lange, Twisted hessian curves, in: International Conference on Cryptology and Information Security in Latin America, Springer, 2015, pp. 269-294.
[14] A. Mathur, T. Newe, W. Elgenaidi, M. Rao, G. Dooly, D. Toal, A secure end-to-end IoT solution, Sensors and Actuators A: Physical 263 (2017)291-299.
[15] K. B. Adedeji, J. O. Famoriji, Investigating the effects of varying the key size on the performance of aes algorithm for encryption of data over a communication channel.12
[16] S. Thangavelu, V. Vijaykumar, Efficiient modified elliptic curve diffie-hellman algorithm for voip networks.,International Arab Journal of Information Technology (IAJIT) 13 (5).
[17] M. Xin, A mixed encryption algorithm used in internet of things security transmission system, in: Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2015 International Conference on, IEEE,2015, pp. 62-65.
[18] B. Pieper, An overview of the hipaa security rule, part ii: Standards and specifications., Optometry (St. Louis, Mo.) 75 (11) (2004) 728.

Authors' Profiles

P. J. A. Alphonse received the M.Tech degree from Indian Institute of Technology Delhi, India and Ph.D. degree from National Institute of Technology, Tiruchirappalli, Tamilnadu, India. He joined the Department of Computer Applications, National Institute of Technology, Tiruchirappalli, with a focus on Graph Theory and Cryptography. He is currently working as a Professor in Computer Applications.

Kavitha.S received the M.Tech degree from SASTRA University, Tanjur, Tamilnadu, India. She is currently Pursuing Ph.D. degree in National Institute of Technology, Tiruchirappalli, Tamilnadu, India. Her research interests include Information security, Cryptography.

How to cite this paper: Kavitha.S, P.J.A.Alphonse, "A Hybrid Cryptosystem to Enhance Security in IoT Health Care System", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.9, No.1, pp. 1-10, 2019.DOI: 10.5815/ijwmt.2019.01.01