Journal of Medical Systems (2019) 43: 260
https://doi.org/10.1007/s10916-019-1378-2

MOBILE & WIRELESS HEALTH

An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System

S. Kavitha[1] · P. J. A. Alphonse[1] · Y. Venkataramana Reddy[2]

Received: 2 April 2019 / Accepted: 5 June 2019 / Published online: 2 July 2019

Abstract
Due to tremendous development in the network technologies forms an Internet of Things (IoT) based Health Care System (HCS) is an essential application in day-today life. In HCS, constitute a group communication among doctors, patient, caretaker, ambulance, and hospital, which intern's devices transfer personal information from one to many group members. Providing security on the personal health information is the most critical issue, because malicious access on this information may leads to life threads. Concurrently, traditional cryptographic framework has unsuccessful to protection to the HCS over lightweight communications network. So, the proposed framework deals the security flaws through hyper elliptic curve based public key cryptosystem, which combines Digital Signature algorithm, Elgamal approaches that ensure the entity authentication and secure group communication. The performance of the proposed work analyzed using efficient security measures and compared with related schemes.

Keywords Hyper elliptic curve · DSA · IoT security · Genus 2 · Group key communication

Introduction

The massive improvement in communication technologies enables the possibility of inter connecting devices over the internet called IoT, which works collaboratively for providing human value added services. The smart objects are retrieve data in effectively, on demand IoT based services has been deployed in various applications like military, environment monitoring, health care system, transportation, and building automation [1, 2]. Among these services, IoT based Health Care System is prominent as its directly employing over human health issues. So, the development of IoT HCS is mostly focused by government and industries [3].

Everything in IoT connects to internet and avail identity and it has number of serious vulnerability if devices improperly protected. The primary responsibility of HCS is to accumulate health related personal information and transfer to the group members of IoT HCS through an access point(s). While transferring information on the network, HCS suffered from various attacks such as eavesdropping, reputation, and modification. The malware may intend to manipulate the transmitted data that leads to user's inconvenience and even medical crime. Hence, HCS must ensure data communication over at the right time and to the right person.

In HCS, group of devices are working together for gathering the health information, secure group communication has two primary security functions of identity authentication and group key management [4–7]. Available secure cryptographic schemes try to ensure the confidentiality of data and providing security to the IoT based HCS. Unfortunately, IoT consist of low power computational and communication devices and design of sentry component is much tricky, so most of the

This article is part of the Topical Collection on *Mobile & Wireless Health*

✉ S. Kavitha
kavi.parama@gmail.com

P. J. A. Alphonse
alphonse@nitt.edu

Y. Venkataramana Reddy
vaiviar@ieee.org

[1] Department of Computer Applications, National Institute of Technology, Tiruchirapalli, Tamilnadu, India

[2] CVR College of Engineering, Hyderabad, India

systems unable to guarantee the security. While designing the cryptographic system needs to ensure the security of the group communication and well-structured key management protocol.

In this paper mainly focused on providing efficient secure cryptosystem to IoT HCS, cryptosystem consist of hyper elliptic curve based DSA and Elgamal(Elg) algorithm. The security element endorses in the proposed authentication and encryption scheme to meet prerequisite of the IoT based devices. The correctness of the proposed cryptosystem as the primary protection component for the entry point of an IoT based HCS evaluated.

The rest of the paper is organized as follows. Second section, discuss about security issues based on algorithm in IoT health care system. Third and fourth section, represents the preliminaries and set up procedure for proposed cryptosystem description for IoT HCS. Fifth section, discuss the efficiency and performance of the Proposed work group communication in IOT Environment. Sixth section, concludes the proposed work.

Related work

In current decades, researchers dedicated to concentrate on the progress of IoT appliance security issues, which were handling by different methodology and protocols. In 2001 [8] Richard Duncan mention different authentication methods and protocols, description begins with password protection and end with digital signature that address the security issues like SSL, IPSEC, Kerberos. Every method had advantages and disadvantages when providing security. An authentication algorithm of Digital Signature Algorithm (DSA) used to communicate multiple groups by basic protocol and extended protocol that concludes two protocols were non-interactive [9].

A network of the network can hold security by preceding methodology; here need to think about next level development in IoT based environment. IoT HCS network unable to gain a better level of protection by the single cryptographic algorithm, so author suggested and obtain security using hybrid algorithm of Advanced Encryption Standards (AES) and Elliptic Curve Cryptography (ECC). The most secure cryptographic algorithms of DSA and Diffe Hellman (DH) proved the strength of security through elliptic curve based DSA and DH, which continues the implement and discuss the generalization of ECDSA and ECDH [10]. Moreover sensitive medical care devices forms network of network where travel sensitive medical data. Increased various security issues mentioned in terms of design flaws, fails to inside attack, man in middle attack. These issues handled through different phases of the proposed model and evaluated through Automated Validation of Internet Security Protocol and Applications (AVISPA) tool.

Another variation of genus 2 Hyper Elliptic Curve based Cryptography (HECC) provides efficient scalar multiplication that applied in IoT HCS [11]. HECC compared with ECC by scalar multiplication and HECC offer a high level of security in variable based single scalar multiplication than ECC. ECC implementation through fixed variable based single scalar multiplication for key generation and multi scalar multiplication for signature verification [12]. Comparative study discusses and evaluates the binary field implementation of HECC and ECC.

There was a variant representation of hyper elliptic curve equations and scalar multiplication, discussion about how it has support and satisfies the security level [13, 14]. Hyper elliptic curve based DSA used for identity authentication, their performance also analyzed through previously used methodology. IoT environment may be handled by preceding ECC based cryptographic algorithms, but need to improve the efficiency of arithmetic operation, besides security issues and attacks are increased day by day [9, 11]. Thereby IoT based HCS environment needs more suitable protection, efficient algorithms and methodology.

From reviewed work, different methodology and protocols were provides security. Earlier day's traditional methods of algorithm are satisfied to obtain protection, but technological development unable to gain security. Therefore, this paper proposed to implement with hyper elliptic curve based DSA and Elgamal algorithms in the novel methodology.

Preliminaries

Previously, elliptic curves based security standards acknowledged. Their steadiness depends on the substantial computational complexity of discrete logarithm issue in the points on elliptic curve. At present, increasing technological power in network and development of cryptanalysis strategies, cryptographic transformations on elliptic curves rather satisfy required level of secrecy. It may result in reducing steadiness of security system, so hyper elliptic curve will take place of elliptic curve cryptography.

HECC was introduced by koblitz in 1995 [15] and implemented on discrete logarithm problem on the Jacobian. HECC defined over fields of any characteristic, considering finite field.

Let p be a prime order Hyper elliptic Curve Hc of genus >1 over finite field f_p representation is an equation of the form

$$\begin{aligned} &\mathrm{Hc}: \mathrm{y}^2 + \mathrm{h(x)y} = \mathrm{f(x)} \\ &h, f \in f_p[x] \\ &\deg(\mathrm{f}) = 2\mathrm{g} + 1 \\ &\deg(\mathrm{h}) \leq \mathrm{g},\ \mathrm{f}\ \text{monic polynomial} \end{aligned} \tag{1}$$

There is no point(x,y)$\in\overline{f_p}*\overline{f_p}$. To satisfies both equation $y^2 + h(x)y = f(x)$ and the partial derivative equation $2y+ h(x) = 0$ and $h'(x)y-f'(x) = 0$ So, all points on the curve are non-singular points and also denoted as set of K - rational points on Hc. The definition of the Jacobian group $J(f_p)$ considered as generalization of the group of points on elliptic curves.

The computation of hyper elliptic curves of genus 2 over genus 1 follows much smaller base field in Jacobian groups, which is set of curve and exchange $J(f_p)$ by operation of addition, doubly addition and scalar multiplication of divisors.

To gain quality computation, representation of the curve genus g is 2~6, finite field limit to $p >= 2^{160}$ and points derive from the curve Hc to a Jacobian group $J(f_p)$, an element divisor D is obtained from Hc. It is the computation of finite addition of $D = \sum K_i q_i$ of base point on Hc over f_p, where K_i is point coefficient, $\sum K_i$ is the sum of points, coefficient q_i is corresponding point on the curve Hc [16].

Advantage of Hc over ECC has small base field size 2^{128}, produces size 2^{256}, and security level obtained 2^{128}. The exceptional procedure issue in Hc genus-2 curve has easily avoided by ladder for shared-secret computation. The hyper elliptic curve computation aid to hold current security issue properly.

Setup procedure

Due to enrichment of IoT might be used sensor-based devices, those are battery-powered devices, it needs to save energy. At the same time, group communication among group members ought to be secure, for the reason of malware or unauthorized members exploitation, vulnerability on the network. These points are remembering to propose the methodology for efficient computation and accuracy of the group communication.

The IoT HCS group communication forms number of subgroups sg_{im}, namely in $sg_{10\ldots}$, $sg_{20\ldots}$, …sg_{im}. Those are related to each other because of subgroup key generation from hierarchical order of group controller gc to the end of the sub group members. Everyone in the group member involves to generate partial key has transferred to next phase member. Finally, the last member of group generates group key with the combination of all the partial keys.

Every sg_i has sg_{im-2} number of phases, a combination of three members in every phase is involved in generating partial keys. The generated partial keys are transferred through neighborhood nodes to the last member of the subgroup, who is the initiator of the each subgroup receives the combination of partial key that is used to create its group key. Sg_i subgroup partial keys are represented as follows

$sg_i p_1 x_{1\ldots..} x_3$, $sg_i p_2 x_{1\ldots..} x_3$,…….. $sg_i p_i x_{1\ldots..} x_3$

$sg_1 p_1 x_{1\ldots}$ $sg_i p_i x_n$ is the combination of $hcds(m_j)$,t_i,$su_i m_{j.}$, where $hcds(m_i)$ is the hashing function of jth message, $su_i m_j$ represents ith user and jth message.

The subgroup members Sg_{im} have compute group key generation with Sg_{im-1} phases, sg_{im-1} phase send their partial key to $sg_{im+1.}$ The procedure of scalable decentralized group key agreement protocol used to implement the proposed hyper elliptic curve based algorithms, which has a minimum computation of arithmetic operation. An algorithm DSA used to authenticate sg_{im}, generate and distribute the group key in an IoT environment by Elg over Hc [16].

Notations in IoT HCS

Hc	Hyper elliptic curve
$J(f_p)$	Finite field Jacobian group
n	large prime order
G	reduced divisor large prime order n in $J(f_p)$
d_i	positive integer no longer than n-1
M_i	message
$[.]_E$	mapping from $J(f_p)$ to Z_p^{2g}
Sg_{im}	group members
$Hm(x_{1..n}, y_{1\ldots n})$	encoded curve points

Authentication algorithm

Authentication extract through hyper elliptic curve Hc and g which has reduced divisor of large prime order n in $J(f_p)$. kg refer to the divisor scalar multiplication of D, multiplied by the positive integer k and $[.]_E$ represent an mapping from $J(f_p)$ to Z_p^{2g}. The generalized equation of Hyper elliptic curve Digital Signature Algorithm (HcDSA) procedure has structured.

The user A wants to sign a message m

- Function f(x,y,z) is mapping with direct product group z_m x $J(f_p)$, Select o(x,y,z), t(x,y,z), q(x,y,z) are 3- variable one valued rational function in $z_{m.}$
- Generate the similar equation
-

$$F(r, m, kg) = 0 \quad (2)$$

- $ko(r,s,m) + dt(r,s,m) + q(x,y,z) = 0$
- Selects an random integer d_i as private key and compute the divisor scalar multiplication $q_i = d_i g$ as public key
- Select random integer k_i and computes divisor scalar multiplication $k_i g$
- Compute r_i using (2) equation $r_i = [k_i g]_E \bmod n$ where $r_i \neq 0$
- Compute s_i using (2) equation $s_i = k^{-1}(h(m_i) + d_i r_i) \bmod n$, where $s_i \neq 0$
- User A has HcDSA signature (r_i, s_i)

Message signature has generated by using first choosing function f(r,m,kg), then selection of random integer used to

solve r_i, s_i from the Eq. (2), solution of (r_i,s_i) satisfied with condition $s_i\ r_i \neq 0$. If it is not satisfied then need to change function f and precede the procedure up to satisfies the condition.

Signature verification has the computation of divisor scalar multiplication over Hc. After that need to check whether signature is accept or reject. The signature can verify by checking the equation.

$$R = \left(s_i^{-1}\, h(m_i)\right)G + \left(s_i^{-1} r_i\right)n \tag{3}$$

$$F\left(r, m, o^{-1}(r,s,m)(-t(r,s,m)n - q(r,s,m)G)\right) = 0 \tag{4}$$

Using this (4) equation, signature can be verified.

Points to be noted in Eq. (2) to obtain the efficient and secure signature. The chosen function f(.) helps to solve signature parameter of r easily when $r_i = s_i = 0$, repeat the process of finding k from {1,2,…..n-1}.The guarantee of the validity is obtained, When signature (r_i,s_i) on message m has appear in Eq. (2). Finally if there is no solution in Eq. (2) then need to change the functions f(.), o(.), t(.), q(.).

The advantage of HcDSA has selected the small parameters, which incorporate speed and small keys size. It is especially vital role in the IoT environment where the processing power, memory and transmission capacity are obliged.

Group key construction

The proposed group key generation method depends on decentralized group key management scheme; it does not have a centralized key-management control system. Each group member participates to generating group key, and equal privilege assigned to group members while communicating within the group as well as between subgroups. As a result, proposed method eliminates a single point of failure in a group key agreement. The generalized scalable group key agreement [17] protocol helps to provide secure group communication by Hc_Elgamal (HcElg) algorithm.

Group key generation by algorithm HcElg gets as parameter of Hc, divisors D, prime n are apply in the generalized scalable and efficient group key agreement for sg_{im} member's methodology [17], which helps to generates group key with the combination of partial keys and also broadcast to all subgroup [8, 18].

Every three members in a group is consider as one phase, transfer partial key to next phase member up to sg_{im} members of sub group which forms $sg_{im\text{-}2}$ phases. The significance of this method eliminates the rekeying process in-group key agreement protocol. When a member joins or leaves in the group, forward and backward secrecy can maintained by methodology [19, 20].

$sg_{(1..i)(1...m)}pa_{(1..i)}x_{(1..i)}$ number of partial key generated in a group. Every phase has transferred partial key along with message in the form of M_i, r_i, pa_ix_i mod p. After generation of group key, message 'M_i' embed on the curve Hc which returns as a series of curve points represented as P(x,y). The encoded message is referred as $Hm(x_{1..n},y_{1..n})$.

Encryption Algorithm

Let n be prime number, and g be a generator of Z_n. The random integer as private key k between 1 and n-2. Compute y = gk mod n. The group key for ElGamal encryption is (pa_ix_i, g, y). While releasing y = gk mod n unable to reveal the k value due to discrete logarithms is as hard as it is extensively believed.

To encrypt a plaintext M_i, using group key gk

Select an random integer r_i

Compute $c_1 = r_i$*g mod n Compute $c_2 = r_i$*y*m_i mod n

The encrypted cipher text C consists of the pair (c_1, c_2) computed above.

Decryption Algorithm

The decryption of the cipher text C = (c_1, c_2) in the Elgamal scheme, to retrieve the plaintext M

M < —c_2/c_1 r_i mod n

In the above expression, the "division" by c_1r_i should be interpreted in the context of modular arithmetic, M is multiplied by the inverse of c_1r_i in Zp. The correctness of the ElGamal encryption scheme is easy to verify.

c_2 / c_1r_i mod n = M_i yk(c_1r_i) 1 mod n

$M_igk_i(gkr_i)$ 1 mod n

M

The evergreen strengthen Elgamal algorithm is very hard to break added to the implementation through Hc points, which proves efficiency of the algorithm.

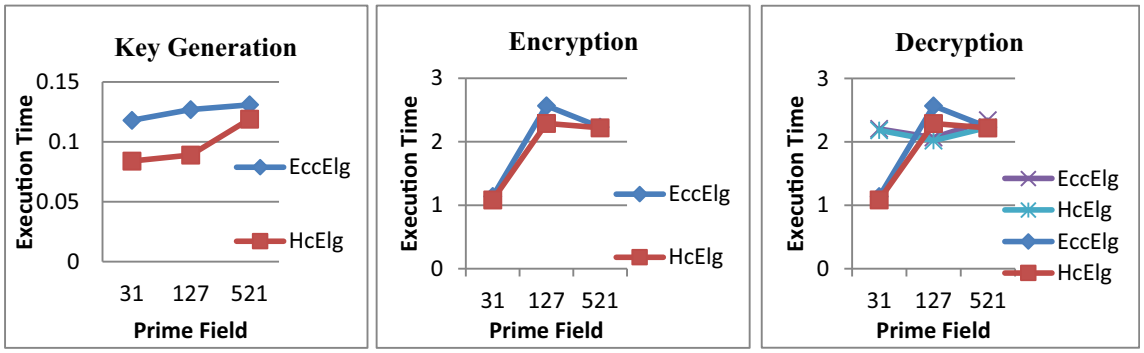
Security analysis

The IoT HCS security system has enhanced authentication and provide better level of security. Well organizing and stronger authentication prevent the security attacks like eavesdropping, data and identity theft, privacy loss, organized crime, psychological suffering, and the probability of put in danger human lives. Moreover, IoT device based authentication mechanisms must be fast and efficient without compromising level of security.

To ensure identity authentication and security proved by HcDSA, Here to consider, HcDSA known possible attacks

Table 1 Comparison of Ecdsa and HcDSA computation of scalar multiplication

Curves	Prime field	Group order	Addition/ doubling
ECDSA	521	2^{521}	I + 2 M + 3S
HcDSA	521	2^{521}	I + 22 M + 3S



Figs. 1–3 Comparison of EcElg and HcElg algorithm execution

could be classified through as hash function attacks, per message secret attack and solve Hc_Discrete Logarithm Problem.

- As though the selected function employed through a secured hash function, then the hash function attacks should avoided.
- An attacker try to compute per message secret key k by the user's generated signature (r_i,s_i) on selected message m then attacker regain private key d as inverse function of F^{-1}, S^{-1}, ϕ^{-1}. However, each distinct message signed by the distinct per message secret. Thus per message secret attack proved efficiently.
- Hyper elliptic curve discrete logarithm problem on the jacobian group has defined as $G \in J(f_p)$, $p \in G$, find an integer k such that $p = kG$ Solving the Hyper elliptic curve Discrete Logarithmic Problem (HcDLP) in valuable.

HcDSA facilitate, non membership detection and identification can carried out through each member sg_{im} in every phase generated partial key (Mi, r_i, sg_{im-1}) which has been authenticated and communicated securely, otherwise non-members communicate with the group.

Nonmember ship identification has pointed out after the detection of non-member, each member sg_i used pa_i where $i = 1 \ldots n$, computation of partial key used to identify the non members in the group communication. Group key $gk = pai_i x_i \bmod n$ generation involves all the members in the group to compute sg_{im} members in the group.

Performance analysis

To prove that an efficiency of the proposed method by calculation of HcDSA and ECDSA. The Table 1 shows comparison of HcDSA and ECDSA in terms of addition and doubling operation. HcDSA security is much stronger than DSA's 160 bit. HcDSA has same level of security as 1024 bit. The generalized HcDSA signature scheme extracts efficiency and secure cryptographic application for IoT health care system.

Figures 1, 2 and 3 shows that graphical representation of HcElg and EcElg algorithm execution time. These algorithms are compared to the different prime field with key generation, encryption and decryption. From this, conclude HcElg takes less time for execution. In the generalized group key generation methodology used to store their partial key, which takes less memory for computation of gk.

Since in a field, complexity of one inverse operation is more times than one multiplication operation, as fewer inversion operations as possible in the HcDSA signature and verification. The HcElg complexity significantly impedes its wide application on resource-constrained devices in IoT health care system.

Conclusion

In this paper, demonstrated IoT based healthcare security system with authentication processes and its major security requirements. Well-organized two approaches of DSA and Elg are expressed as hyper elliptic curve based cryptography. Novel group key methodology with HcDSA and HcElg algorithm is much stronger than DSA and Elg at better level of security. Deep look into the protection of the proposed authentication scheme and formal analysis has proved through known possible attack, hash function attacks, per message secret attack and solved HcDLP Problem. The proposed work has proved according to the security analysis and implementation results confirmed that the proposed methodology is appropriate security to the sensitive IoT based health care system.

Compliance with ethical standards

Conflict of interest Kavitha.S declares that she has no conflict of interest. P.J.A. Alphonse declares that he has no conflict of interest. Y.Venkatramana Reddy declares that he has no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Yeh, K.-H., A secure IoT-based healthcare system with body sensor networks. IEEE Access 4:10288–10299, 2016.
2. Harn, L., and Lin, C., Authenticated group key transfer protocol based on secret sharing. IEEE transactions on computers 59:842–846, 2010.
3. Alphonse, P. J. A., and Reddy, Y. V., A method for obtaining authenticated scalable and efficient group key agreement for wireless ad-hoc networks. Cluster Computing.:17, 2018.
4. Hou, J.-L., and Yeh, K.-H., Novel authentication schemes for IoT based healthcare systems. International Journal of Distributed Sensor Networks 59:842–846, 2015.
5. Li, C.-T., Wu, T.-Y., Chen, C.-L., Lee, C.-C., and Chen, C.- M., An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. Sensors 17:1482, 2017.
6. Veltri, L., Cirani, S., Busanelli, S., and Ferrari, G., A novel batch-based group key management protocol applied to the internet of things. Ad Hoc Networks 11:2724–2737, 2013.
7. Rafaeli, S., and Hutchison, D., A survey of key management for secure group communication. ACM Computing Surveys (CSUR) 35:309–329, 2003.
8. Ye, C., and Reznik, A., Group secret key generation algorithms, information theory. ISIT 2007. IEEE International Symposium: 2596–2600, 2007.
9. Porambage, P., Braeken, A., Schmitt, C., Gurtov, A. V., Yliant-tila, M., and Stiller, B., Authenticated group key transfer protocol based on secretsharing. IEEE transactions on computers 3:842–846, 2010.
10. Jaiswal, P., and Tripathi, S., An authenticated group key transfer protocol using elliptic curve cryptography. Peer-to-Peer Networking and Applications. 10:857–864, 2017.
11. Kim, Yongdae and Perrig, Adrian and Tsudik, gene, group key agreement efficient in communication. IEEE transactions on computers 53:905–921, 2004.
12. Amir, Y., Kim, Y., Nita-Rotaru, C., and Tsudik, G., On the performance of group key agreement protocols. ACM Transactions on Information and System Security (TISSEC) 7:457–488, 2004.
13. Lake, D., Milito, R., Morrow, M., and Vargheese, R., Internet of things: Architectural framework for ehealth security. J. ICT Stand. 1:301–328, 2014.
14. Duncan, R., An overview of different authentication methods and protocols, report submitted to SANS institute, 2001, 10.
15. Xin, Mingyuan, A mixed encryption algorithm used in internet of things security transmission system, Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), International Conference on. pp 62:65,.2015
16. Das, A. K., and Goswami, A., A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. ACM Transactions on Information and System Security (TISSEC) 7:9948, 2013.
17. Bernstein, D. J., and Lange, T., Hyper-and-elliptic-curve cryptography. LMS Journal of computation and Mathematics 17:181–202, 2014.
18. Wankhede Barsgade, M. T., and Meshram, S. A., Comparative study of elliptic and hyper-elliptic curve cryptography in discrete logarithmic problem. IOSR J. Math. 10:61–63, 2014.
19. Wei, L.-f., Design of hyperelliptic curve system digital signature in identity authentication. Fifth International Conference on Digital Image Processing (ICDIP 2013)IEEE transactions on computers 7:457–488, 2013.
20. Lin, YOU and Sang, Yong-Xuan, Effective generalized equations of secure hyper elliptic curve digital signature algorithms, The Journal of China Universities