Journal of Theoretical and Applied Information Technology
15th February 2023. Vol.101. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT GROUP KEY AGREEMENT PROTOCOL IN TELEMEDICINE

SRAVANI JAYANTI[1], K CHITTIBABU[2], PRAGATHI CHAGANTI[3], CHANDRA SEKHAR AKKAPEDDI[*]

[1,2]Research Scholar, Department of Mathematics, GITAM, Visakhapatnam, India

[3]Associate Professor, Department of Mathematics, GITAM, Visakhapatnam, India

[*]Professor, Department of Mathematics, GITAM, Visakhapatnam, India

E-mail: [1]sjayanti@gitam.in, [2]12196210201@gitam.in , [3]pchagant@gitam.edu , [*]cakkaped@gitam.edu

ABSTRACT

Telecommunication is an important trait in telemedicine. In an e-Health Care System of telemedicine, the medical information of a patient needs to be collected and safeguarded from the adversaries. This is attained by an efficient protocol which would provide access to the authorized persons to receive and update the medical information of a patient. In this paper, an efficient and secure Group Key Agreement protocol is designed which enables the authorized persons to agree on a Group key to access the private information and modify them. The designed protocol applies a Number-Theoretic function and an Affine operator to achieve robustness and security which is applicable for the smooth functioning of an e-Health Care System.

Keywords: *Cryptology, Group Key Agreement Protocol, Number-Theoretic Function, Affine Operator, e-Health Care System, Telemedicine*

1. INTRODUCTION

The health of an individual is treated with utmost care in any Health care System (HCS). For the smooth functioning of medical organizations and comfort of patients, e-Health care Systems of telemedicine are developed which monitor the health record of the patient by providing access to the patient's data to the authorized persons from remote locations over Internet. The e-HCS are designed to meet the security requirements in the patient's information by retaining privacy, confidentiality and integrity [1][2]. Different cyber threats to steal the medical information of a patient are led to gain access to the patient's health record. The attackers take undue advantage of the unauthorized access to manipulate patient's data to incur insurance basing on patient's identity, to cause personal distress to the patient, to falsify the medical information to claim extra insurance and to alter patient's health record to worsen the patient's health for personal grudges [3]. Thus the security of the developed e-HCS is vital which is procured by Cryptography [4]. Several key agreement and authentication schemes are developed for telemedicine [5][6][7].

Cryptosystems enable encrypting the information but the authorization is provided with the help of the key required to access and decrypt the information. Thus an efficient Group Key Agreement protocol would be a best fit to regulate the well-functioning of an e-HCS.

The prevention of unauthorized access of private and vital information over internet is achieved by secure cryptosystems developed applying mathematical concepts. The security of a cryptosystem is dependent on the secret keys which are used to interpret the cipher text. These keys need to be exchanged between the communicating parties such that an intruder fails to hack it. It is carried out by a strong and an efficient key exchange protocol. The methodological approach of the protocols changes based on the number of communicating parties.

An ancient and the most famous key exchange protocol is the Diffie-Hellman key exchange protocol where the hardness in solving the Discrete Logarithm problem makes the protocol secure [8]. The protocol was designed for a secure key exchange between two parties. It can be extended to a group of n-parties where n-parties mutually agree on a secret key but it would take $(n-1)$ iterations

to compute the shared key [9]. Thus there is an underlying need for generating an efficient Group Key Agreement Protocol (GKAP) which computes the key in less number of iterations. Many such protocols are designed, out of which, one of them is the protocol designed in [10][11]. This design takes $(n-1)$ iterations to generate a group key whose security relies on the difficulty in solving the Discrete Logarithm Problem. The protocol in [10] is resistant to passive attacks.

When concerned about the group key agreement protocols, two types of designs are available. One is the Centralized GKAP and the other is the Contributory GKAP. In case of a Centralized GKAP, the major communications are carried out by a central authority due to which the sole responsibility of the key generation is controlled by a single contributor. In short, it is a two-party key exchange process carried out with n-entities. In case of a Contributory GKAP, each of the group members participate in the protocol and hence the entry and exit of a group member after initiation of the protocol effects the key generation process depending upon whether the protocol is partially contributory or fully contributory. The protocol proposed in [10] is partially contributory and the one proposed in [12] is fully contributory.

In [10], a partially contributory key exchange method, Cliques is developed where the security of the method is dependent on the Discrete Logarithm problem. In [12], a fully contributory key exchange method based on the units of a groupring is developed. In [13], a centralized group key distribution method is proposed based on the key star structure. In [14], a key exchange protocol between two communicating parties is proposed whose security relies on the hardness in solving the Diophantine equations which is secure for the Diophantine equations of degree greater than 2. The security aspects of the protocol in [14] are discussed in [15]. In [16], a key exchange protocol for two communicating parties based on the insolvability of Diophantine equations is proposed which is secure for the Diophantine equations of degree greater than 1.

In view of [9-12], PCGKAP is developed applying mathematical concepts which takes less number of iterations in sharing the key. Application of a classical cipher (Affine) and a number-theoretic function is witnessed in an e-HCS. Telemedicine requires a secure and an efficient GKAP to share and update the patients' health record among a trusted n-number of parties. Thus, the mathematical model is established to meet the requirements of Telemedicine in an e-HCS. In this paper, a partially contributory GKAP is designed applying the following mathematical concepts:

1.1 Number theoretic function [17]:

A function $f: N^n \to N$ is a number theoretic function i.e, a function whose arguments and values belong to the set of natural numbers.

1.2 Affine Cipher [18][19]:

An affine cipher is a combination of a multiplicative cipher and an additive cipher.

In an Affine Cipher, over a congruence modulo n, for the values of $a, b \ni \gcd(a, n) = 1$, $a, b < n$, plaintext (P) is encrypted as Cipher text, $C = (a * P + b) \bmod n$ and the Cipher text (C) is decrypted to Plain text, $P = (C - b) * a^{-1} \bmod n$ where $a.a^{-1} \equiv 1 (\bmod n)$.

Here, for different choices of a, b, different cipher texts are obtained for the same plain text character. The maximum number of possible combinations for a, b is $n.\varphi(n)$ [20]. This cipher is vulnerable to the Known plaintext attack and attacks by frequency analysis.

The proposed group key exchange protocol is inspired from [8] which is applicable in telemedicine. Here, the operations are performed over a special type of number theoretic functions and the operator used is an Affine operator.

2. PROPOSED GROUP KEY AGREEMENT PROTOCOL

The methodological approach to agree on a key by a group of n-multiple parties $A_1, A_2, \dots, A_n$ is:

The number theoretic function applied in the method is:

$$f: \mathbb{N}^n \to \mathbb{N}$$

defined by

$$f(x_1, x_2, \dots, x_n) = t. \prod_{i=1}^{n} a_i^{x_i}$$

where

$$a_i \in \mathbb{N}. \qquad (1)$$

The transformation used in the method is Affine transformation. For a function 'f',

Journal of Theoretical and Applied Information Technology
15th February 2023. Vol.101. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$T_{\{m,n\}}(f) = (m.f + n) \bmod k$$

where $(m, k) = 1, n < k$ and

$$T_{\{m,n\}}^{-1}(f) = \left((f - n).m^{-1}\right) \bmod k$$

where $m.m^{-1} \equiv 1 \pmod k$ (2)

Initially a random number 'k' is made public to all.

Each A_i, for $i = 1,2,\dots,n-1$ individually selects two pairs of positive integers $\{(m_i, n_i), (p_i, q_i)\}$ such that $\gcd(m_i, k) = 1, \gcd(p_i, k) = 1$ and $n_i, q_i < k$ and A_n selects a random n-tuple $(\alpha_1, \alpha_2, \dots, \alpha_n) = \alpha$.

Consider $T_i(f) = T_{\{m_i,n_i\}} \circ T_{\{p_i,q_i\}}(f)$ and $T_i^{-1}(f) = T_{\{p_i,q_i\}}^{-1} \circ T_{\{m_i,n_i\}}^{-1}(f)$ where $T_{\{m_i,n_i\}}, T_{\{m_i,n_i\}}^{-1}$ are operators as defined in (2).

2.1 Methodological Approach for GKAP

Step 1: A_1 selects a function 'f' of the type (1) and sends $T_1(f)$ to A_2.

Step 2: $\forall\, i = 2,3,\dots,n-2$, A_i sends $T_i \circ T_{i-1} \circ \dots \circ T_1(f)$ to A_{i+1}.

Figure 1. Transmission of signals by A_i to $A_{i+1}, i = 1,2,\dots,n-1$

Step 3: A_{n-1} sends $T_{n-1} \circ T_{n-2} \circ \dots \circ T_1(f) = T(f)$ to A_i for $i = 1,2,\dots,n-2,n$.

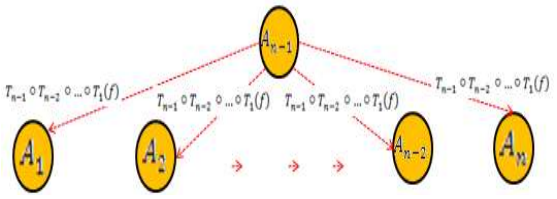


Figure 2. Transmission of signals by A_{n-1} to other users

Step 4: A_n calculates the key $K = T(f(\alpha_1, \alpha_2, \dots, \alpha_n))$.

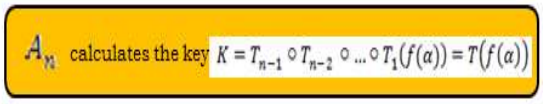


Figure 3. Calculation of Key by A_n

Step 5: $\forall\, i = 1,2,\dots,n-1$, A_i sends $T_i^{-1} \circ T(f(x_1, x_2, \dots, x_n))$ to A_n.

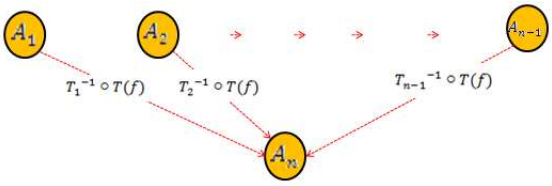


Figure 4. Transmission of signals for key sharing by A_i's to A_n

Step 6: A_n distributes $T_i^{-1} \circ T(f(\alpha_1, \alpha_2, \dots, \alpha_n))$ to A_is $\forall\, i = 1,2,\dots,n-1$.

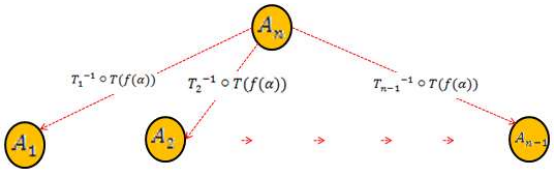


Figure 5. Transmission of signals from A_n to the other users for key retrieving

Step 7: $\forall\, i = 1,2,\dots,n-1$, each A_i retrieves the key by computing $K = T_i \circ T_i^{-1} \circ T(f(\alpha_1, \alpha_2, \dots, \alpha_n))$.

Figure 6. Key Retrieval by each A_i

3. EXAMPLE

Implementation of the proposed key exchange protocol for 4-parties (A_1, A_2, A_3 and A_4):

For the chosen values of $k = 61$, (public to A_1, A_2, A_3 and A_4),
$\{m_1, n_1\} = \{2,5\}, \{p_1, q_1\} = \{3,6\}$ (private to A_1),
$\{m_2, n_2\} = \{5,11\}, \{p_2, q_2\} = \{9,15\}$ (private to A_2),
$\{m_3, n_3\} = \{7,13\}, \{p_2, q_2\} = \{16,5\}$ (private to A_3),

Journal of Theoretical and Applied Information Technology
15th February 2023. Vol.101. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\alpha = (1,2,3,4)$(private to A_4) and
the function $f(x_1, x_2, x_3, x_4) = 5.2^{x_1}.3^{x_2}.5^{x_3}.2^{x_4}$
(chosen by A_1), the protocol works as:

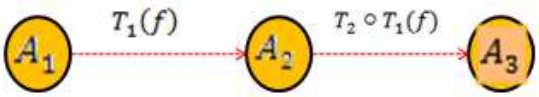


Figure 7. Transmission of signals by $A_1$to A_2 and $A_2$to A_3

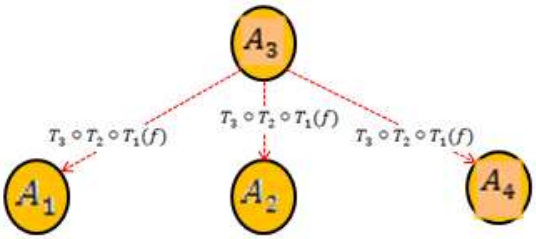


Figure 8. Transmission of signals by $A_3$to other users

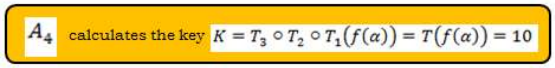


Figure 9. Calculation of Key by A_4

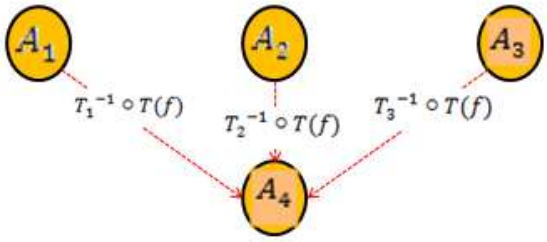


Figure 10. Transmission of signals for key sharing by A_1, A_2 and $A_3$to A_n

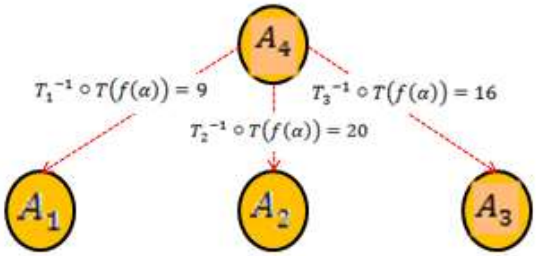


Figure 11. Transmission of signals from A_4 to the other users for key retrieving

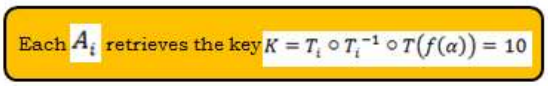


Figure 12. Key Retrieval by A_1, A_2 and A_3

4. ANALYSIS OF THE PROTOCOL

The protocol uses a number theoretic function $f: N^n \to N$ defined by $f(x_1, x_2, \dots, x_n) = t.\prod_{i=1}^{n} a_i^{x_i}$ where $a_i \in N$.

The transformation used to carry out the communications in the protocol is an Affine transformation which is invertible. The composition of Affine transformations is non-commutative,i.e., for a function $'f'$ and an operator $'T'$ (as in (1)), with different choices of $\{m_1, n_1\}$ and $\{m_2, n_2\}$ where $\gcd(m_1, k) = 1, \gcd(m_2, k) = 1$ and $n_1, n_2 < k$, $T_{\{m_1,n_1\}} \circ T_{\{m_2,n_2\}}(f) \neq T_{\{m_2,n_2\}} \circ T_{\{m_1,n_1\}}(f)$.

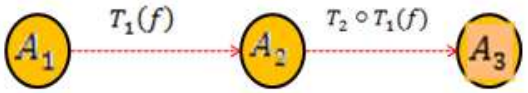
Due to the non-commutative nature of the compositions of Affine transformations, the order in which the operators are being operated plays a major role in the process of exchanging signals.

In order to retrieve a function $'f'$ from $T_{\{m_1,n_1\}} \circ T_{\{m_2,n_2\}}(f)$, the order in which the composition of their inverses shall be operated should be in reverse order of the initial composition,
i.e., $T^{-1}_{\{m_2,n_2\}} \circ T^{-1}_{\{m_1,n_1\}} \left(T_{\{m_1,n_1\}} \circ T_{\{m_2,n_2\}}(f)\right) = f$.

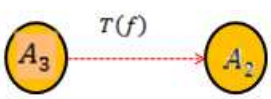
This property is used in restoring the key by (n-1) parties from the nth party.

The protocol is resistant to passive attacks. In the example discussed above, let us consider that all the communications are public. Then there are two ways to trace the key by an intruder. One is by gaining access to $\{m_i, n_i\}, \{p_i, q_i\}$ of A_ith party and the second is by gaining access to the values of $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

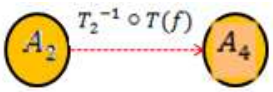
Suppose that $\{m_2, n_2\}, \{p_2, q_2\}$ are to be traced. Then the signals communicated to and by A_2 are to be considered which are:



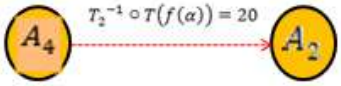
$T_1(f) = (30.2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4} + 17) \bmod 61$ (3)
$T_2 \circ T_1(f) = (8.2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4} + 58) \bmod 61$(4)



$$T(f) = (42.2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4} + 17) \bmod 61 \quad (5)$$



$$T_2^{-1} \circ T(f) = (5.2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4} + 31) \bmod 61 \quad (6)$$



$$T_2^{-1} \circ T(f(\alpha)) = (5.2^1.3^2.5^3.2^4 + 31) \bmod 61 = 20 \quad (7)$$

The number of operators composition performed in obtaining $T_2 \circ T_1$ is unknown to the intruder. Since the composition of Affine transformations is affine therefore, the intruder assumes two values (k_1, k_2) where $\gcd(k_1, k) = 1, k_2 < n$ such that $T_2 = T_{\{k_1,k_2\}}$.

In this method, the operator is operated on a function of the form

$$f(x) = ax + b, \text{where } x = 2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4}.$$

Therefore,

$$T_{\{k_1,k_2\}}(ax + b) = [(k_1 a)x + (k_1 b + k_2)] \bmod k \quad (8)$$

and

$$T^{-1}_{\{k_1,k_2\}}(ax + b) = [(ak_1^{-1})x + (bk_1^{-1} - k_1^{-1}k_2)] \bmod k \quad (9)$$

where $k_1 k_1^{-1} \equiv 1 (\bmod k)$.

From the set of equations above (3) and (4) we have,

$$30k_1 = 8 (\bmod 61)\ ;\ 17k_1 + k_2 = 58 (\bmod 61) \quad (10)$$

On solving the above set of equations, we get $k_1 = 19, k_2 = 40$.

From the equation (7), $T_{\{19,40\}}(20) = 54$,this is not equal to the key value 10.

Despite having the knowledge of all the communicated signals to and from A_2, the intruder is unable to retrieve the key.

Hence, the proposed protocol is safe. In fact, the security can be increased to a greater level by selecting more than two transformations by an individual party.

On the other hand, the set of equations that are helpful to determine the values of $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ are:

$$7.2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4} \bmod 61 = 9 \quad (11)$$

$$5.2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4} \bmod 61 = 20 \quad (12)$$

$$(8.2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.2^{\alpha_4} + 58) \bmod 61 = 16 \quad (13)$$

As the number of unknowns (4) is greater than the number of equations (3), therefore it is infeasible to solve them for $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Also, the equations involve exponents modulo a positive integer making the computations complex. Hence, tracing the values of $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is infeasible.

Therefore, the protocol is resistant to attacks whenever all the communications are public.

The maximum number of possibilities for the key is 'k'. Thus a brute force attack can be carried out to trace the key. Therefore by increasing the value of 'k' to a sufficiently large prime, the security of the protocol can be increased. Also, selection of a large prime number leaves maximum choices for the values of m_is, n_is, p_is and q_is.

The designed protocol helps in exchanging the keys among n-parties in less than $(n - 1)$ number of iterations which are easily computable.

5. APPLICATION

Cryptography witnesses diverse applications to secure information by retaining availability, confidentiality and privacy. One of the vital applications of Cryptography is in a telemedicine where a patient's information needs protection from undue usage.

A practical model in an e-HCS constituting the proposed Group Key agreement protocol is proposed. The model is well suited in an instance

Journal of Theoretical and Applied Information Technology
15th February 2023. Vol.101. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where a patient's information needs to be available to the major persons accountable for the treatment of the patient who are:

Insurance Provider: who provides insurance to the patient.
Bill Processor: who keeps record of all the necessary transactions and processes the bill.
Health Care Provider: who keeps track of the Health Care kits and medicines used to treat the patient.
Assigned Doctor: who treats the patient
Hospital's Official Authority: who is responsible for the admission and discharge of the patient
Patient: who is diagnosed with health illness.

The communication of signals among the contributing parties for agreeing on a shared secret key occurs as pictured:

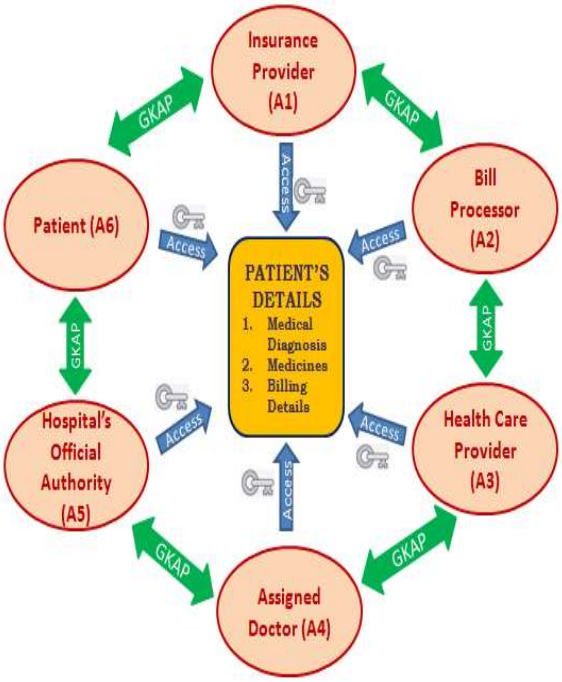
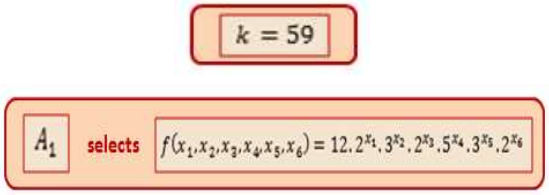


Figure 13. Proposed Model of e-HCS of Telemedicine

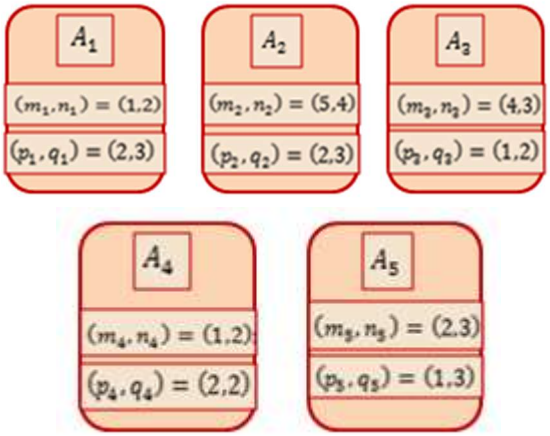
The working of the protocol when six parties in the proposed e-HCS model agree on a group key is explained below using a mathematical example:

Table 1. Implementation of GKAP in e-HCS model

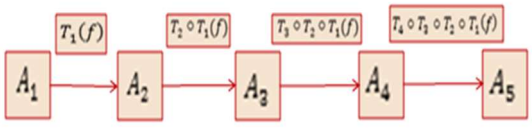
Step 1: A prime k is made public.A_1 selects a number theoretic function f.



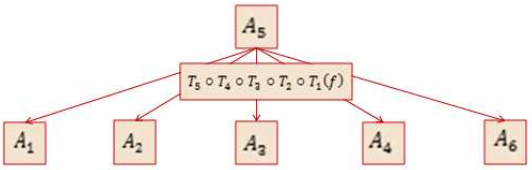
Step 2: The contributing parties A_1, A_1, A_1, A_1,A_1 randomly choose respective m_is, n_is, p_is and q_is.



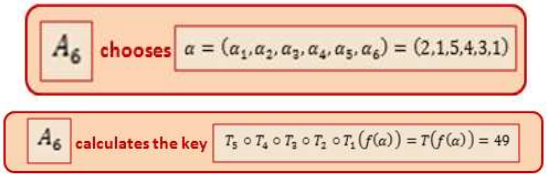
Step 3: Each $A_i, i = 1,2,3,4$ transmits $T_i \circ T_{i-1} \circ \ldots \circ T_1(f)$ to A_{i+1}.



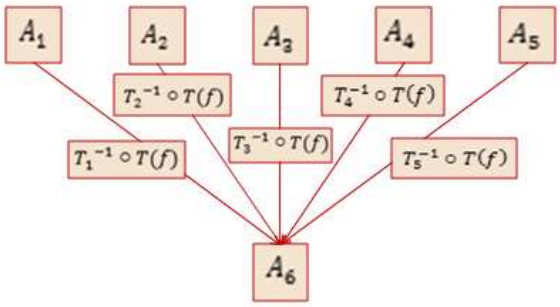
Step 4:A_5 transmits $T_5 \circ T_4 \circ T_3 \circ T_2 \circ T_1(f) = T(f)$ to A_i for $i = 1,2,3,4,6$.



Step 5: A_5 randomly selects α and calculates the key value.



Step 6: A_1, A_2, A_3, A_4 and A_5 transmits signals to A_6 for key sharing.



Step 7: The key is retrieved by each contributing party.

An efficient algorithm which would intake identification codes of individual party to generate the polynomial 'f' and the m_is, n_is, p_is, q_is and α can be developed to avoid manual inputs from the contributing parties.

The designed protocol allows the authorized persons to agree on a group key which is used to access and update the patient's record. The health record of the patient is only accessible to the authorized six major persons. This prevents the data from false modifications in the patient's data, false insurance claim by using the patient's identity, unnecessary public display of the patient's health record and false manipulation of patient's record to claim extra insurance.

6. CONCLUSIONS

A partially contributory Group Key Agreement protocol is designed applying mathematical tools which is applicable in telemedicine. The scenario of an e-Health Care System where the developed model is helpful to secure patient's health record is explored in the paper. The security aspects of the developed mathematical GKAP are examined which concludes that the protocol is resistant to passive attacks. The developed method has no restriction on the number of contributing parties to share the key. The defined number-theoretic function adds to the resistance of the protocol to passive attacks. Simple classical cipher and Number Theoretic function led to the development of a GKAP which helps in maintaining the health record of patient in an e-HCS securely. The developed mathematical model is less complex as it shares key in less number of iterations but is prone to active attacks.

FUTURE SCOPE

The future aspect of the model constitutes of developing an efficient mathematical algorithm to provide authentication and authorization to the contributing parties in the GKAP which would eliminate the issue of possible Man-In-The-Middle Attack. This could be achieved by applying the concept of Galois Field and Group codes.

ACKNOWLEDGEMNTS

We extend sincere thanks to GITAM for supporting the work by providing Dr. M.V.V.S. Murthi Research Fellowship.

REFERENCES:

[1] Mousavi HA, Seyyed Keyvan, Ali Ghaffari, and SinaBesharat, "Security of internet of things based on cryptographic algorithms: a survey", Wireless Networks, Vol. 27, No. 2, 2021, pp. 1515-1555.

[2] Mutinda Jackson, "Cryptosystem in Healthcare", Munich, GRIN Verlag, 2017. https://www.grin.com/document/430929

[3] Xavier Francis Oduor and Dr. Zachary BosireOmariba, "Application of cryptography in enhancing privacy of personal data in medical services", *International Journal of Communication and Information Technology* Vol. 3, No. 1, 2021, pp. 16-21.

[4] Rasha Thabit, "Review of Cryptography Applications in eHealth Security Systems", *International Journal of Science and Engineering Investigations*, Vol. 8, issue 89, 2019, pp. 110-116.

[5] Guo, D., Wen, Q., Li, W., Zhang, H., &Jin, Z, "An improved biometrics-based authentication scheme for telecare medical information systems", *Journal of Medical Systems*, Vol. 39, No. 3, 2015, pp. 1–10.

[6] Arshad, H., &Nikooghadam, M., "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems", *Journal of Medical Systems*, 2014. doi:10.1007/s10916- 014-0136-8.

[7] Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., and He, L., "A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems", *Journal of Medical Systems*, 2014. doi:10. 1007/s10916-013-9994-8.

[8] W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol. IT 22, No. 6, 1976, pp. 644-654.

[9] Key Exchange, Available online at: https://www.nku.edu/~christensen/092mat483%20DH%20key%20exchange.pdf

[10] M. Steiner, G. Tsudik and M. Waidner, "CLIQUES:A new approach to Group key agreement", *Proceedings of the 18th International Conference on Disturbed Computing Systems(ICDCS'98)*, 1998, pp.380-387.

[11] R. Schnyder, J. A. López-Ramos, J. Rosenthal, D. Schipani, "An active attack on a multiparty key exchange protocol", *Journal of Algebra Combinatorics Discrete Structures and Applications*, Vol.3, No.1, 2016.

[12] T. Hanoymak and O. Kusmus, "A New Multi-Party Key Exchange Protocol andSymmetric Key Encryption Scheme overNon-commutative Group Rings", *International Journal of Information Security Science*, Vol.8, No.1, 2019, pp.11-16.

[13] V. Kumar, R. Kumar and S.K. Pandey, "A computationally efficient centralized group key distribution protocol for secure multicast communications based upon RSA public keycryptosystem",*Journal of King Saud University – Computer and Information Sciences*, Vol. 32, 2020, pp. 1081–1094.

[14] Harry Yosh, "The key exchange cryptosystem used with higher order Diophantine equations", *International Journal of Network Security & Its Applications*, Vol. 3, No. 2, 2011, pp.43–50.

[15] Noriko Hirata-Kohno, Attila Peth″, "On a key exchange protocol based on Diophantine equations".

[16] P. A. Kameswari1, S.S. Sriniasarao, and A. Belay, "An Application of Linear Diophantine Equations to Cryptography", *Advances in Mathematics: Scientific Journal*, Vol.10, No. 6, 2021, pp. 2799–2806.

[17] J. P. Tremblay and R. Manohar, "Discrete Mathematical Structures with Applications to Computer Science", Tata McGraw-Hill Edition.

[18] D. R. Stinson and M.B. Paterson, "Cryptography: Theory and Practice", Fourth Edition, CRC Press, Taylor and Francis Group.

[19] B.A. Forouzan, D. Mukhopadhyay, "Cryptography and Network Security", Third Edition, McGraw Hill Education.

[20] H. Om and R. Patwa, "Affine transformation in cryptography", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 11, No.1, 2008, pp. 59-65.