Acta Biomed 2023; Vol. 94, N. 3: e2023718 DOI: 10.23750/abm.v94i3.13442

Mutually Authenticated Tripartite Key Agreement Protocol for Smart Hospital in IoT Environment

Dr. T. Isaiyarasi[1], V. Nagarani[2], Dr.S.Chitra[3]

[1]Assistant Professor, Department of Mathematics, SRM Valliammai Engineering College, Chengalpattu District, Tamil Nadu, isaiyarasit.maths@srmvalliammai.ac.in. [2]Assistant Professor, Department of Mathematics, SRM Valliammai Engineering College, Chengalpattu District, Tamil Nadu, Nagaraniv.maths@srmvalliammai.ac.in. [3]Assistant Professor, Department of Mathematics, SRM Valliammai Engineering College, Chengalpattu District, Tamil Nadu, chitras.maths@srmvalliammai.ac.in.

Abstract. Key agreement protocol is one of the fundamental cryptographic technique. This enables the communicating entities to exchange information securely through an insecure medium. The key agreement protocol involves all the communicating parties to arrive at a common key. In this paper an authenticated key agreement protocol is proposed which can be later used in the e-health care system. In the key agreement protocol proposed in this paper is based on the hardness of the triple decomposition search problem. This search problem is implemented in the five dimensional discrete Heisenberg group. The protocol is authenticated by digital signature algorithm, which also uses the triple decomposition search problem as the one way function. The proposed protocol is secure against all the attacks and the security analysis also discussed. The key agreement protocol devised is then applied in the digital (smart) hospital. The digital hospital set up consists of a gateway node, User (Physician) and IoT enabled device with the patient. The IoT enabled medical equipment like thermometer and Pacemaker are with the patient. The gateway node contains the information and medical history of the patient received through the IoT device. The physician access the gateway node for the information about the health condition of the patient. The digital hospital environment allows the physician the make clinical decisions that means the doctor can analyse patient's symptoms. The doctor takes the details of the patient from the gateway node. In order to ensure the privacy of the patient's information an authentication is required. To achieve this, the authenticated key agreement protocol is required. The Key agreement protocol enables the communication between the doctor, digital hospital and the patients IoT enabled devices. The protocol derives a mutually authenticated common key between the gateway node and the user (doctor) and a mutually authenticated common key between the gateway node and the patient. Using the common keys arrived by key agreement protocol presented in this paper, the communicating entities gateway node, doctor and the patient communicate securely

Keywords: Key agreement protocol, triple decomposition search problem five dimensional discrete Heisenberg group, Smart hospital.

Mathematical Subject Classification: 2010 Mathematics Subject Classification: 94A60

Introduction

Cryptography enables people to communicate securely over an insecure medium. Cryptography is concerned with the Confidentiality, Integrity, Non-repudiation, and Authentication. Cryptography can be classified as symmetric key (private key) and asymmetric key (public key) cryptography There is a necessity to have a common key among the communicating entities as Cryptography is applied in various fields, like military, e-commerce, banking sectors, Digital hospital etc. To arrive at a common key, a technique need to be devised. The technique is called Key exchange protocol. Key exchange protocol can be classified in to two major categories namely, Key transport protocol and Key agreement protocol (KAP). In Key transport protocol, one party creates a key and then transport it to other entities, where as in Key agreement protocol all the communicating entities involve in arriving at a common key.

In this paper a mutually authenticated tripartite key agreement protocol is proposed. The KAP proposed is based on the intractability of triple decomposition search problem in five dimensional discrete Heisenberg group. This protocol provides a common key between the communicating entities. The key thus arrived is then applied in the concept of smart hospital environment. The smart hospital concept consists of three communicating entities. They are the gateway node at the hospital which is the common entity, the user (doctor) and the patient with IoT enabled medical equipment.

The paper is organised as follows , In section2 the related works have been discussed, section 3 displays the

computational facts about the five dimensional discrete Heisenberg group. In section 4, a mutually authenticated key agreement protocol is proposed, section5 deals with the smart hospital concept and the KAP devised in section 4 is applied in smart hospital environment. Section 5 concludes the paper.

Related works

The first public key cryptosystem [10] was proposed in 1976, which is a key agreement protocol in which one of the keys were made public. In this, the discrete logarithm problem was used as the one-way function. A new directions in cryptography by Diffe-Hellman is a key exchange protocol, in which the session keys are computed by the communicating parties with the help of public information shared in advance. This paper opened up new directions in the field of Cryptography. Anshel-Anshel-Goldfeld [3] scheme proposed a key agreement protocol, based on the hardness of multiple search problem which is implemented in the Braid group. [19]M.R. Magyarik, N.R. Wagner proposed a Public Key Cryptosystem based on the word problem in non-abelain platform [23] E.Stickel proposed a Diffie Hellman type key agreement protocol using the discrete logarithm problem. . A.Joux [17] proposed a One Round Protocol for tripartite Diffie-Hellman key agreement. RSA [22] digital signature scheme was based on the hardness of integer factorization problem. ECDSA is based on the hardness of discrete logarithm problem in the elliptic curve group.

G.S.G.N.Anjaneyulu, Dr. P. Vasudeva Reddy, Prof. Dr.U.M.Reddy [7] proposed a Secured Digital Signature Scheme using Polynomials over Non-Commutative Division Semi rings. Hai-Duong Le [18] proposed A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hocWireless Sensor Networks. Muhamed Turkanovic et al [20] proposed a novel user authentication and key agreement scheme for heterogeneous adhoc wireless sensor networks. Hamizdreza Yazdanpanah et al [11] proposed a secure user authentication of key agreement scheme for HWSN tailored for the IoT environment. [9] Dae-Hwi Lee,Im-Yeong Lee, "A Lightweight Authentication and Key Agreement Schemes for IoT Environments".

The five-dimensional Discrete Heisenberg group

$\mathcal{H} = Z_p^5$ be the set of all elements of the form $(x_1, x_2, x_3, x_4, x_5)$ and the binary operation in this set is defined as follows.

$(x_1, x_2, x_3, x_4, x_5) \cdot (y_1, y_2, y_3, y, y_5) = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4, x_5 + y_5 + x_1 y_3 + x_2 y_4)$

SAGE Code:

$x = (x1, x2, x3, x4, x5)$

$y = (y1, y2, y3, y4, y5)$

$show("x.y = ")$

$[(x1 + y1)\%p)(x2 + y2)\%p, (x3 + y3)\%p, (x4 + y4)\%p), (x5 + y5 + x1 * y3 + x2 * y4)\%p]$

$Show("(x\,.y)" = ")$

Output:

$(\,(x1 + y1), (x2 + y2,), (x3 + y3), (x4 + y4), (x5 + y5 + x1 * y3 + x2 * y4))$

This operation satisfies the closure, associative properties and under this operation an identity element exists and each element possesses an inverse. But this operation is not commutative, thus this set constitutes a non-abelian group which is infinite.

This group is made finite as follows:

$(x_1, x_2, x_3, x_4, x_5) \cdot (y_1, y_2, y_3, y, y_5) = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4, x_5 + y_5 + x_1 y_3 + x_2 y_4) mod\ p$

where p is a prime number.

Computational Facts:

(i)Order of $\mathcal{H} = Z_p^5$ is p^5

To generate the elements of the group the following code will be used

SAGE Code

$[(x, y, z, w, t)\ for\ x\ in\ range(p)\ for\ y\ in\ range(p)\ for\ z\ in\ range(p)\ for\ w\ in\ range(p)\ for\ t\ in\ range(p)]$

(ii)Identity element is $e = (0,0,0,0,0)$

(iii)Inverse: $(x_1, x_2, x_3, x_4, x_5)^{-1} = (-x_1, -x_2, -x_3, -x_4, -x_5 + x_1 x_3 + x_2 x_4)\%p$

SAGE Code:

$show('inverse\ x = ')$

$(-x1\%p, -x2\%p, -x3\%p, -x4\%p, (-x5 + x1 * x3 + x2 * x4)\%p)$

$(iv)\ (x_1, x_2, x_3, x_4, x_5)^n = \left(nx_1, nx_2, nx_3, nx_4, nx_5 + n^{(2)}(x_1 x_3 + x_2 x_4)\right) mod p$

SAGE Code:

$show('x\hat{}n = ')$

$n * x1\%p, n * x2\%p, n * x3\%p, n * x4\%p, ((n * x5) + (n * (n-1)/2 * x1 * x3 + x2 * x4)\%p)$

(v)Generators of $\mathcal{H}$ are:

$(1,0,0,0,0), (0,1,0,0,0), (0,0,1,0,0), (0,0,0,1,0)$

$(vi)[a, b] = a \cdot b \cdot a^{-1} \cdot b^{-1} = (0,0,0,0, x_1 y_3 + x_2 y_4 - x_3 y_1 - x_4 y_2) mod\ p$

Thus, any element of $\mathcal{H}$ is expressed as follows:

$(x_1, x_2, x_3, x_4, x_5) = (1,0,0,0,0)^{x_1} \cdot (0,1,0,0,0)^{x_2} \cdot (0,0,1,0,0)^{x_3} \cdot (0,0,0,1,0)^{x_4} \cdot [(1,0,0,0,0), (0,0,1,0,0)]^{x_5}$

$(viii)$Order of any element is p, which is for any $a, a^p = e(identity)$

(ix)Subgroups of DHG:

The cyclic subgroup $G_1 =< e, a >$is of order P,

The elements of G_1 are $\{a, a^2, a^3, a^4, a^5 \cdots, a^{p-1}, a^p = e\}$

The cyclic subgroup $G_2 =< e, a, b >$is of order P^2 where $a \cdot b = b \cdot a$,

The cyclic subgroup $G_3 =< e, a, b, c >$ where a, b, c commute with each other is of order P^3,

Proceeding in similar way, we get

The cyclic subgroup $H_{p-1} =< e, a_1, a_2, \dots, a_{p-1} >$ where the generators commute with each other is of order P^{P-1}

Let $A =< e, a, b >$ with $a \cdot b = b \cdot a$and $B =< e, c, d >$ with $c \cdot d = d \cdot c$, but the generators of A do not commute with those of B.

The generators of the cyclic subgroup A are:

$< e, a, a^2, \dots, a^6, b, b^2, \dots, b^6, ab, \dots,$

$ab^6, a^2b, \dots, a^2b^6, a^3b, \dots, a^3b^6, a^4b, \dots, a^5b, \dots, a^5b^6,$

$a^6b, \dots, a^6b^6 >$

Subgroup generation code:

$x = (x1, x2, x3, x4, x5)$

$y = (y1, y2, y3, y4, y5)$

$p = 7$

$show("subgroup")$

$for\ n\ in\ range(p)$:

$for\ m\ in\ range(p)$:

$print(((n * x1 + m * y1)\%p, (n * x2 + m * y2)\%p, (n * x3 + m * y3)\%p, (n * x4 + m * y4)\%p, (n * x5 + m * y5 + n * x1 * m * y3 + n * x2 * m * y4 + n * (n-1)/2 * (x1 * x3 + x2 * x4) + m * (m-1)/2 * (y1 * y3 + y2 * y4))\%p))$

Triple Decomposition Search problem:

The communicating parties, generally Alice and Bob agree on Discrete Heisenberg group $\mathcal{H} = Z_p^5$. Also the subgroups $G_1 =< e, g_1, g_2, g_3 >, G_2 = < e, h_1, h_2, h_3 >$

$G_3 =< e, l_1, l_2, l_3 >$ where $g_i g_j = g_j g_i,\ i, j =$ 1,2,3.where

$g_i g_j = g_j g_i, h_i h_j = h_j h_i,\ l_i l_j = l_j l_i\ for\ i, j =$ 1,2,3 and $g_i h_j \neq h_j g_i,\ g_i l_j \neq l_j g_i,\ h_i l_j \neq l_j h_i$, $g_i, h_i, l_i \in \mathcal{H}$

Alice randomly chooses $a_1, x_1 \in G_1, a_2, x_2 \in G_2, a_3 \in G_3$ and computes

$u = a_1 \cdot x_1$,$v = x_1^{-1} \cdot a_2 \cdot x_2$,$w = x_2^{-1} a_3$, (u, v, w) is her public key and the 5-tuple

$(a_1, x_1, a_2, x_2, a_3)$ is her private key

Bob randomly chooses $b_1 \in G_1,\ b_2, y_1 \in G_2, b_3, y_2 \in G_3$ and computes

$p = b_1 \cdot y_1, q = y_1^{-1} \cdot b_2 \cdot y_2$,$r = y_2^{-1}.b_3$, (p, q, r) is his public key and 5- tuple $(b_1, y_1, b_2, y_2, b_3)$ is his private key.

From the public keys of Alice or Bob getting their corresponding private keys is called triple decomposition search problem. That is from$u$, the adversary needs to get $a_1\ and\ x_1$, from v the adversary needs to get x_1^{-1}, a_2, x_2 and from w the adversary needs to get $x_2^{-1}\ and\ a_3$. Thus getting the private keys from the public keys is known triple decomposition problem.

Intractability of triple decomposition search problem:

If an adversary Eve tries to get the private keys of the communicating parties from the public keys, he must solve the following system of equations:

(i) Extracting $a_1$andx_1 from u

Let $a_1 = (a_{11}, a_{12}, a_{13}, a_{14}, a_{15}), x_1 = (x_{11}, x_{12}, x_{13}, x_{14}, x_{15})$and $u = (u_{11}, u_{12}, u_{13}, u_{14}, u_{15})$

$$u = a_1 \cdot x_1 = (a_{11} + x_{11}, a_{12} + x_{12}, a_{13} + x_{13}, a_{14} + x_{14}, a_{15} + x_{15} + a_{11}x_{13} + a_{12}x_{14})modp \quad \dots (1)$$

But $u = (u_{11}, u_{12}, u_{13}, u_{14}, u_{15})$ $\dots (2)$

Comparing (1) and (2)

$u_{11} = (a_{11} + x_{11})modp, u_{12} = (a_{12} + x_{12})modp, u_{13} = (a_{13} + x_{13})modp$

$u_{14} = (a_{14} + x_{14})modp \qquad u_{15} = a_{15} + x_{15} + a_{11}x_{13} + a_{12}x_{14})modp$

Now u may assumes the integers between 0and $p-1$

Case1: $u_{11}=0$, then $a_{11}$and x_{11} may assumes the following p possible values

a_{11}	0	1	$p-1$	2	$p-2$	…	$\frac{p+1}{2}$	$\frac{p-1}{2}$
x_{11}	0	$p-1$	1	$p-2$	2	…	$\frac{p-1}{2}$	$\frac{p+1}{2}$

Case2: $u_{11}=1$ then $a_{11}$and x_{11} may assumes the following 2 possible integers

a_{11}	0	1
x_{11}	1	0

Case3: $u_{11}=2$ then $a_{11}$and x_{11} may assumes the following three possible integers

a_{11}	0	1	2
x_{11}	2	1	0

Proceeding in similar way

Case $p-2$: $u_{11}=p-2$ then $a_{11}$and x_{11} may assumes the following $p-1$ possible integers

a_{11}	$p-2$	0	$p-3$	1	$p-4$	2	…	$\frac{p-2}{2}$
$x1_1$	0	$p-2$	1	$p-3$	2	$p-4$	…	$\frac{p-2}{2}$

Case $p-1$: $u_{11}=p-1$ then $a_{11}$and x_{11} may assumes the following$p-1$ possible integers

a_1	$p-1$	0	$p-2$	1	$p-3$	2	…	$\frac{p-1}{2}$
x_1	0	$p-1$	1	$p-2$	2	$p-3$	…	$\frac{p-1}{2}$

Similar cases will arise when the adversary tries to get the values of $a_{12}$and x_{12} from u_{12}, $a_{12}$and x_{13} from $u_{13}$and $a_{14}$and x_{14} from u_{14}.But when he tries in the case of u_{15} he needs to solve $u_{15}=a_{15}+x_{15}+a_{11}x_{13}+a_{12}x_{14}$ he needs to solve much more complicated equations than the above cases. The same argument may be repeated while the adversary tries to extract x_2^{-1} and a_3 from w.

The process of extractingx_1^{-1}, a_2 and x_2 from v is described as follows:

$v=x_1^{-1}\cdot a_2\cdot x_2$, Let $v=(v_{11},v_{12},v_{13},v_{14},v_{15})$,

$x_1^{-1}=(-x_{11},-x_{12},-x_{13},-x_{14},-x_{15}+x_{11}x_{13}+x_{12}x_{14})$

$a_2=(a_{21},a_{22},a_{23},a_{24},a_{25})$

$x_2=(x_{21},x_{22},x_{23},x_{24},x_{25})$

$$(v_{11},v_{12},v_{13},v_{14},v_{15}) = (-x_{11}+a_{21}+x_{21},-x_{12}+a_{22} + x_{22},-x_{13}+a_{23}+x_{23},-x_{14}+a_{24} + x_{24},-x_{15}+a_{25}+x_{25}+a_{12}x_{23} + a_{22}x_{24}$$

To extract the private keys the adversary needs to solve the following equations:

$v_{11}=(-x_{11}+a_{21}+x_{21})\ modp$

$v_{12}=(-x_{12}+a_{22}+x_{22})\ modp$

$v_{13}=(-x_{13}+a_{23}+x_{23})\ modp$

$v_{14}=(-x_{14}+a_{24}+x_{24})modp$

$v_{15}=(-x_{15}+a_{25}+x_{25}+a_{21}x_{23}+a_{22}x_{24})modp$

Thus the triple decomposition search problem is cryptographically hard. Thus it may be considered to be serve as a one way function. In this paper this problem is used to devise the digital signature

Authenticated Key Agreement Protocol for Smart Hospital

In the registration phase the user (doctor) and the sensor node in the IoT device generate their own public key and share them with the gateway node. A common shared key between the user and gateway node and a common shared key between the sensor node in IoT device and the gateway node are arrived in this phase.

Login phase enables the user and IoT device to communicate with the gateway node and through which the user and patients IoT device communicate and the doctor gives his medical advice to the patient. The architecture of this system is depicted as follows

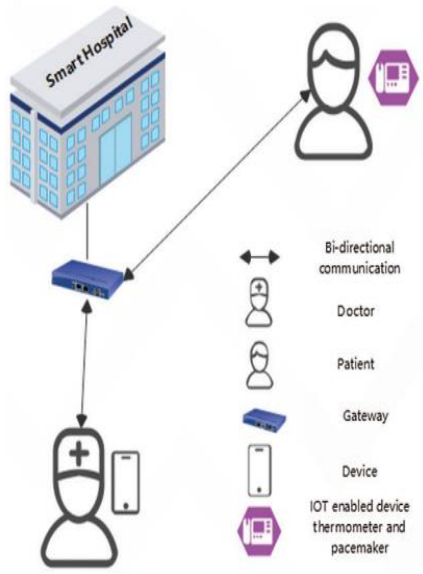

Figure 1: System model

The security at all the ends are achieved by the proposed key agreement protocol (KAP). It consists of three phases, The Pre deployment phase, the registration phase and the login phase. In the pre deployment phase the gateway node generate public keys for the user (doctor) and the sensor in the IoT enabled device

In the registration phase the user (doctor) and the sensor node in the IoT device generate their own public key and share them with the gateway node. A common shared key between the user and gate way node and a common shared key between the sensor node in IoT device and the gateway node are arrived in this phase.

Login phase enables the user and IoT device to communicate with the gateway node and through which the user and patients IoT device communicate and the doctor gives his medical advice to the patient, Login phase enables the user and IoT device to communicate with the gateway node and through which the user and patients IoT device communicate and the doctor gives his medical advice to the patient.

Initial set up

The communicating entities are Hospital's device with Gateway node (GWN), the user (doctor) and the IoT device with patient.

The communicating entities GWN, User and The sensor node with patient's IoT device agree on the five dimensional Discrete Heisenberg group as the platform group described in section3 along with the subgroups.

Pre deployment phase:

GWN chooses $a_{11}, x_{11} \in G_1, a_{12}, x_{12} \in G_2, a_{13} \in G_3$

GWN computes $u_1 = a_{11}x_{11}, v_1 = x_{11}^{-1}a_{12}x_{12}, w_1 = x_{12}^{-1}a_{13}$

$a_{11}, x_{11}, a_{12}, x_{12}\ a_{13}$ are GWN's private keys and $(u_1 v_1, w_1,)$ is the public key

GWN transmits $(u_1 v_1, w_1,)$ to User and Sensor node

User registration phase:

User chooses $b_{11}, \in G_1, y_{11}, b_{12} \in G_2, y_{12}, b_{13} \in G_3$

User computes $p_1 = b_{11}y_{11}, q_1 = y_{11}^{-1}b_{12}y_{12}, r_1 = y_{12}^{-1}b_{13}$

$b_{11}, y_{11}, b_{12}, y_{12}, b_{13}$ are the private keys of the User and (p_1, q_1, r_1) is the public key

User transmits(p_1, q_1, r_1) to GWN

On receiving $(u_1 v_1, w_1,)$ from GWN, user computes $U_r = u_1 b_1 v_1 b_2 w_1 b_3$ and U_r is stored in user's memory

On receiving (p_1, q_1, r_1) from user, GWN computes $G_u = a_{11}p_1 a_2 q_1 a_3 r_1$ and G_u is stored in GWN's memory as User's identity

Sensor node registration phase:

Sensor node chooses $c_{11}, \in G_1, z_{11}, c_{12} \in G_2, c_{13}, z_{12} \in G_3$

Sensor node computes $l_1 = c_1 z_1, m_1 = z_{11}^{-1}c_{12}z_2, n_1 = z_{12}^{-1}c_{13}$

$c_{11}, z_{11}, c_{12}, z_{12}, c_{13}$ are the private keys of the Sensor node and (l_1, m_1, n_1) is the public key

Sensor node transmits (l_1, m_1, n_1) GWN

On receiving $(u_1 v_1, w_1,)$ from GWN, Sensor node computes $S_r = u_1 c_1 v_1 c_2 w_1 c_3$ and S_r is stored in sensor node's memory

On receiving (l_1, m_1, n_1) from sensor node, GWN computes $G_s = a_{11} l_1 a_{12} m_1 a_{13} n_1$ and $G_s$is stored in GWN as sensor node's identity

Login Phase:

Key Agreement Protocol between GWN and User:

Before logging in, user enters U_r as his identity. The GWN then checks that whether $U_r = G_u$, if so GWN accepts and confirms the identity of the User and permits for further communications.

GWN chooses $a_{21}, x_{21} \in G_1, a_{22}, x_{22} \in G_2, a_{23} \in G_3$

GWN computes $u_2 = a_{21}x_{21}, v_2 = x_{21}^{-1}a_{22}x_{22}, w_2 = x_{22}^{-1}a_{23}$

GWN transmits (u_2, v_2, w_2) to User

User chooses $b_{21} \in G_1, b_{22}, y_{21} \in G_2, b_{23}, y_{23} \in G_3$

User computes $p_2 = b_{21}y_{21}, q_2 = y_{21}^{-1}b_{22}y_{22}, r_2 = y_{22}^{-1}b_{23}$

User transmits (p_2, q_2, r_2) to GWN

On receiving (p_2, q_2, r_2) from User, GWN computes $K_U = a_{21}p_2 a_{22} q_2 a_{23} r_2$

On receiving (u_2, v_2, w_2) from GWN , User computes $K_{UG} = u_2 b_{21} v_2 b_{22} w_2 b_{23}$

$K_U = K_{UG} = a_{21}\ b_{21} a_{22} b_{22} a_{23} b_{23}$ is the common key between GWN and User.

Key Agreement Protocol between GWN and Sensor node:

Before logging in, sensor node enters S_r as his identity. The GWN then checks that whether
$S_r = G_s$, if so GWN accepts and confirms the identity of the sensor node and permits for further communications
GWN transmits (u_2, v_2, w_2) to sensor node
Sensor node chooses $c_{21} \in G_1, c_{22}, z_{21} \in G_2, c_{23}, z_{22} \in G_3$
Sensor node computes $l_2 = c_{21} z_{21}, m_2 = z_{21}^{-1} c_{22} z_{22}, n_2 = z_{21}^{-1} c_{23}$
Sensor node transmits (l_2, m_2, n_2) to GWN
On receiving (l_2, m_2, n_2) from sensor node, GWN computes $K_S = a_{21} l_2 a_{22} m_2 a_{23} n_2$
On receiving (u_2, v_2, w_2) from GWN, sensor node computes $K_{SG} = u_2 c_{21} v_2 c_{22} w_2 c_{23}$
$K_S = K_{SG} = a_{21} c_{21} a_{22} c_{22} a_{23} c_{23}$ is the common key between Sensor node and GWN

Smart hospital environment

The digital hospital environment allows the physician the make clinical decisions that means the doctor can analyse patient's symptoms. The doctor takes the details of the patient from the gateway node. In order to ensure the privacy of the patient's information an authentication is required. To achieve this the proposed an authenticated key agreement protocol. The Key agreement protocol enables the communication between the doctor, digital hospital and the patients IoT enabled devices.

As the first step, the smart hospital provides IoT enabled medical equipment to the registered patient. The sensor node with the IoT equipment allows the user doctor to dialogize and give medical advice to the patient. The doctor access the sensor node through GWN. In this process the doctor communicates with GWN using the common key K_U , after GWN verifies the identity of the doctor (user). GWN sends the request to the patient's sensor node through the common key K_S between Sensor node and GWN. Sensor node verifies the common key from GWN and permits the user to access the sensor node and gets the medical advice from the doctor.

Conclusion

In this paper, a mutually authenticated key agreement protocol is proposed. This protocol is based on the intractability of the triple decomposition search problem in the five dimensional discrete Heisenberg group. Using the key agreement protocol proposed in this paper, the smart hospital environment works. The patient can get benefitted by the smart hospital concept as it enables the patient to get medical advice from the doctor without contacting directly. Thus, the smart hospital enables patient to get the treatment even in remote mode.

Reference

1. Alexei Myasnikov,Vladimir Shpilrain, Alexander Ushakov, 'Group Based Cryptography',
2. CRM ,Birkhäuser Verlag, Basel, Boston, Berlin, 2008
3. Alfred Menezes, Paul Van Oorschot, Scott Vanstone, 'A Handbook of Applied Cryptography',
4. CRC Press , Taylor &Francis Group, 1997
5. I.Anshel, M. Anshel, and D. Goldfeld, 'An algebraic method for public-key cryptography', Math.
6. Res. Lett., 6 (1999), 287–291
7. G.S.G.N.Anjaneyulu , Dr. P. Vasudeva Reddy, Prof. Dr.U.M.Reddy, 'Secured Digital Signature
8. Scheme using Polynomials over Non Commutative Division Semirings', International Journal of
9. Computer Science and Network Security, VOL.8 No.8, August 2008
10. G. S. G. N. Anjaneyulu, V. Madhu Viswantham , A. Vijayabarathi,'Secured Directed Digital
11. Signature Scheme Using Polynomial over Non-Commutative Groups' International J. of Math.
12. Sci. &Engg. Appls. (IJMSEA) ISSN 0973-9424, Vol. 7 No. II (March 2013), pp. 371- 383
13. Alfred Menezes and Don Johnson and Scott Vaanstone, 'The Elliptic Curve Digital Signature
14. Algorithm (ECDSA)', http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pd , August 23,1999 Updated
15. February24, 2000
16. Dr.G.S.G.N.Anjaneyulu, Dr.D.U.M.Reddy,' Secured Directed Digital Signature over Non-
17. Commutative Division Semi rings and Allocation of Experimental Registration Number' IJCSI
18. International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012 ISSN
19. (Online): 1694-0814, www.IJCSI.org
20. Chin-Chen Chang Fellow, IEEE, and Hai-Duong Le ' A Provably Secure, Efficient, and Flexible
21. Authentication Scheme for Ad hocWireless Sensor Networks' IEEE transactions on wireless
22. Communications, Vol. 15, No. 1, January 2016 357
23. Dae-Hwi Lee , Im-Yeong Lee, "A Lightweight Authentication and Key Agreement Schemes for
24. IoT Environments", 2020 Sep; 20(18): 5350
25. Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on
26. Information Theory, 22(6), 644–654. Doi: 10.1109/TIT.1976. 1055638.
27. Hamizdreza Yazdanpanah et al., 'A secure user authentication of key agreement scheme for
28. HWSN tailored for the IoT environment' Cryptology ePrint archive 2017
29. T.Isaiyarasi, K.Sankarasubramanian, A New Multiparty Key Agreement Protocol using triple
30. decomposition search problem in Discrete Heisenberg Group, International Journal of Computer
31. Engineering and Information Technology, ISSN Online: 0976-6375, Vol.4, Issue 6, 2013.

32. T.Isaiyarasi, K.Sankarasubramanian, Tripartite Key Agreement Protocol using Triple
33. Decomposition Search Problem, International Journal on Cryptography and Information Security,
34. ISSN: 1839-8626, Vol.2, No.1, 49-55, Sept 2012.
35. T.Isaiyarasi, K.Sankarasubramanian, A New Key Agreement Protocol using two layers of
36. Security, Journal of Discrete Mathematical Sciences and Cryptography, Vol.15, No.2 & 3,April
37. & June 2012.
38. T.Isaiyarasi , K.Sankarasubramanian, A New Multiparty Key Agreement Protocol using search
39. Problems in Discrete Heisenberg Group, Indian Journal of Computer Science and Engineering,
40. ISSN 2231-3850, Vol.3, Issue 1, 154-161. March 2012.
41. JeffreyHoffstein, Jill Pipher, Joseph H. Silverman, 'An introduction to Mathematical
42. Cryptography', Springer
43. A.Joux, 'A One Round Protocol for tripartite Diffe-Hellman',InW.Bosma, editor proceedings
44. Of Algorithmic Number Theory, Symposium, ANTSIV, Lecture Notes in Computer Science,
45. 1838 (2000), 385−394, Springer Verlag
46. Ki Hyoung Ko, Doo Ho Choi, Mi Sung Cho, and Jang Won Lee, New Signature Scheme Using
47. Conjugacy Problem, Cryptology e print Archive: Report 2002/168, 2002.
48. M.R. Khan Magyarik, N.R. Wagner, 'A Public Key Cryptosystem Based on the Word Problem',
49. Advances in Cryptology (CRYPTO 1984), Lecture Notes in Computer Science, 196 (1985),19–36,
50. Springer, Berlin
51. Muhamed Turkanovic et al, 'A novel user authentication and key agreement scheme for
52. heterogeneous adhoc wireless sensor networks' Ad Hoc Networks, vol. 20, 201
53. PeterJ., 'Automorphisms of the Discrete Heisenberg Group', arXiv: math /0405109VI [math SG]6
54. (May2004).
55. R.L. Rivest, A. Shamir, L. Adleman,, A method for obtaining digital signatures and public key
56. cryptosystems ', Communications of the ACM, 27 (1978), 120-126
57. E. Stickel, A New Method for Exchanging Secret Keys ', Proceedings of the Third International
58. Conference on Information Technology and Applications (ICITA05), Contemporary Mathematic

.