International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 24 (2015) pp 44554-44563

Healthcare IOT-A Multilayer Security Mechanism using Linear Programmable Pre-coded Matrix Decomposition Method

B. Nagajayanthi
Assistant Professor (SR), SENSE, V. I. T University, Chennai njeya2014@gmail. com

Dr. R. Radhakrishnan
Principal, Electronics and Communication, Vidhya Mandhir Institute of Technology, Erode rlgs14466@rediffmail. com

Dr. V. Vijayakumari
Professor, Electronics and Communication, Sri Krishna College of Technology, Coimbatore ebinviji@rediffmail. com

Abstract
Network security is the key challenge in IoT. Possible source for security issues and vulnerabilities in IoT networks are caused due to its dynamic network topology, mobility and weak physical security of low power devices. Authentication, Authorization and Access control are important and critical functionalities in the context of IoT to enable secure communication between devices. It is infeasible to use conventional cryptography in IoT networks since security and privacy of critical data are crucial. In this paper, a secure and efficient authentication mechanism in IoT based healthcare system is proposed. Security and privacy of patients' medical data are crucial for the acceptance and ubiquitous use of IoT in healthcare. Primary focus of this work is to provide a Multilayer Security using Linear Programmable Pre-coded Matrix Decomposition (MS_LPMD) method for secure authentication and authorization of remote in or out patients. The proposed architecture uses an efficient and secure key management scheme between IoT node and IoT s_gateway. In this approach during the pre-authentication phase, connection between IoT node and IoT secure gateway is established. The Secure Gateway being the primary authentication server validates unique pattern coefficients generated using LPMD process against the coefficients received from IoT Node for authentication. Authenticated IoT Node employs a simple light-weight computational process for cipher key generation used for subsequent encrypted data communication through a secure communication channel. Proposed MS_LPMD scheme is built to protect the confidentiality, integrity and availability of network data by making the system reliable and protecting the system from malicious attacks which can lead to information disclosure. The proposed MS_LPMD approach has outperformed other existing approaches such as AES, EDCH etc, in terms of higher security level and trust worthiness factor. The performance analysis revealed that our proposed MS_LPMD approach has less communication overhead and latency between the IoT Node and secure gateway. Using software-hardware co-designed IoT test bed, the computed results on standard simulation setup shows an average reduced overhead of 29% and latency of 21% when compared to existing EDCH scheme.

Keywords: Internet of Things, Security, Authentication, non-orthogonal, unique pattern, coefficients, Encryption, Decryption, MS_LPMD

Introduction

Recent advances in information and communication technologies have given rise to a new application centric requirements viz., Internet of Things (IoT). Due to rapid development in Radio Frequency Identification (RFID) [1], Wireless Sensor Networks (WSN), actuators and mobile communication, it is possible to realize the IoT to perform ubiquitous interactions between things and devices in an "anytime, anywhere and anything" form. IoT enables people and objects in physical world as well as data and virtual environments to interact with each other, hence realizing smart environments such as: smart transport systems, smart cities and smart healthcare etc as part of a prosperous digital society. eHealth is the most important application of IoT, where sensors, actuators, RFID tags, etc., are applied in the health sector to facilitate ease of life service across geographic and time barriers. Ubiquitous access to services and monitoring the vital data in eHealth is granted only to identities which fulfill the access control rules. The Access rules serves to heterogeneous device interaction, authorization, mutual authentication, secure delegation within IoT devices and servers. Securing user interactions with IoT is essential if the notion of "things everywhere" is to succeed. Maintaining security and privacy are key challenges in IoT based applications since data collected from IoT-based healthcare sensor is vulnerable to top privacy concerns [2], as it involves direct human interventions.

Among 10 IoT devices tested by Hewlett Packard, it has been reported that, 6 out of 10 popular IoT devices did not use encryption when downloading software updates, 90% of the devices collected atleast one piece of personal information via the device, cloud or its mobile application, 70% of the devices uses unencrypted network services and transmitted credentials in plain text. It has been predicted that nearly half of the IT leaders will invest more in: access control, intrusion prevention, identity management, virus and malware protection because most of the security issues are caused due to: insecure web interface, insufficient authentications, insecure network services, lack of transport encryption, privacy concern, insecure cloud interface, insecure mobile interface, insufficient security configurability, insecure software and poor physical security. All the devices in IoT have low memory and limited computation resources, thus they are vulnerable to resource enervation attack. When the devices join and commissioned into the network, keying

material, security and domain parameters could be eavesdropped. Possible external attacks like denial of service attack, flood attack, etc., on device and mitigation plan to address these attacks is another big challenge.

Different cryptographic protocols for multi-channel authentication have been proposed in [3]-[10], most of them have been developed for the purpose of secure authentication between devices, users and services, summary of the most important protocol proposals can be found in [11]. Some commendable research work is referred in [12] and [13]. Conventional security and protection mechanism cannot be re-used as IoT based systems are vulnerable to various types of attacks. Due to its diversity of devices and end users, there should be attack resistant and lightweight security solutions. Despite the fast development of computer security mechanisms, the scale and complexity of generated wireless data put major challenges to the representation and understanding of security-relevant network information. Various security mechanisms have been proposed to address these security concerns, but high security level requirements in IoT based systems demands an efficient and secure mechanism to address these security issues.

In this paper, we have proposed a novel Multilayer Security Mechanism using Linear Programmable Pre-coded Matrix Decomposition Method (hereafter referred as "MS_LPMD") for authorization and authentication between the IoT healthcare sensor node, Gateway and HMS server. MS_LPMD exploits significant features that enable IoT Nodes in healthcare systems to securely communicate with the gateway. By establishing a secure channel through authentication mechanism for data communication, MS_LPMD prevents significant malicious activity before entering a medical constrained domain. The proposed MS_LPMD approach is elaborated in this paper in notion with security and performance as key factors. Our protocol ensures a secure communication against passive attacks on the privileged side channel and all attacks on the wireless links. Our novelty lies in avoiding the conventional key-exchange mechanism or protocols, which are prone to have severe attacks and compromises. MS_LPMD model incorporates an efficient, secure and attack resistant lightweight security mechanism that proved to be power efficient, faster, and highly secured on devices over conventional methods.

The remainder of this paper is organized as follows: in Section 2, the proposed MS_LPMD architecture for IoT based healthcare system is elaborated, in Section 3 simulation and experimental results of MS_LPMD are provided and discussed. Finally, Section 3 concludes the paper.

Multilayer Security Mechanism using Linear Programmable Pre-coded Matrix Decomposition (MS_LPMD) Architecture

The Architecture of IoT based healthcare monitoring system using MS_LPMD scheme with patient existing in hospital, home and remote location is shown in Fig. 1. The patient's health related information is recorded by body-worn IoT sensor nodes. i. e., IoT sensor nodes implanted in the patient's body is used to measure the changes in temperature, pulse rate, blood pressure, and respiratory rate and transmit the parameter level to physician working in the hospital or existing in remote location to take necessary steps to prevent a critical incident. Monitoring patient's health related information using IoT based healthcare monitoring system is used to give alert to the hospital to take necessary precaution to save the patient, even before the patient has severe problems like heart attack. Healthcare monitoring systems have multi-modal monitors that concurrently measure and display the related fundamental parameters of the patient. This real-time medical data among sensor nodes must be well protected against attackers and security aspects must be ensured [14].

The proposed MS_LPMD system architecture includes the following main components:

IoT Senor Nodes

It captures bio-medical and context signals from patient's body and communicates the sensed data to healthcare monitoring system via secure gateway for treatment and diagnosis based on medical states. The signal transmitted by IoT node is sent to the secure gateway via wireless or wired communication protocols such as Serial, SPI, Bluetooth, Wi-Fi or IEEE 802. 15. 4. The IoT sensor nodes are enabled with ubiquitous identification within its network.

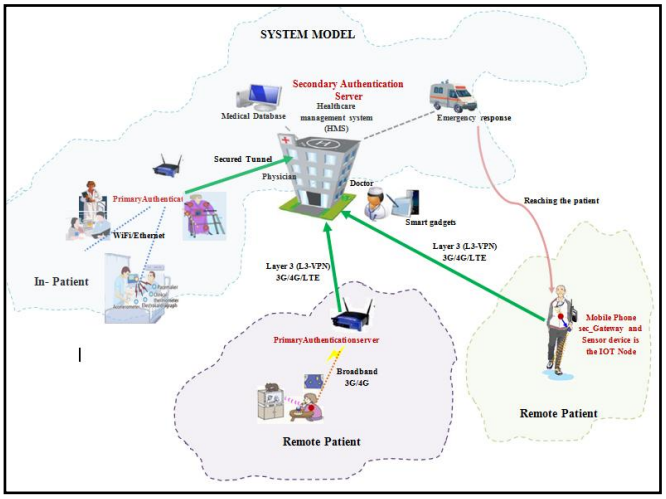


Fig. 1. Architecture of IoT based Healthcare monitoring using MS_LPMD scheme

Secure Gateway

It acts as a primary authentication server. Secure Gateway's objective is to validate authorized access and approve authentication request only for valid IoT Nodes for data secure communication. For valid IoT Nodes, it establishes a secure communication channel via which further data communication takes place. When secure gateway receives request for authentication from IoT Node, it performs MS_LPMD process to approve or reject the request of IoT Node. It supports different protocols and acts as an interface between the IoT Nodes and the HMS server. The main role of a gateway is to support different wireless protocols and inter-device communication. However, in the area of IoT-based healthcare, the role of a gateway has been extended to provide

additional services such as: acting as local repository, to temporarily store sensors' and users' information, providing local processing of sensors' data and bringing intelligence by enhancing with data fusion, aggregation, and interpretation techniques.

HMS Server

It is the back-end system of the IoT based healthcare monitoring system using MS_LPMD scheme. It acts as a secondary authentication server. It consists of hospital healthcare DB server that continuously synchronizes patients health data over time. The collected health information represents a vital source of big data for the statistical and epidemiological medical research (e. g., detecting approaching diseases). Additionally, it has the Web clients as a graphical user interface for final visualization and apprehension.

Our proposed MS_LPMD architecture exploits significant features that enable IoT Nodes in healthcare systems to securely communicate by establishing a secure channel through authentication mechanism via the secure gateway to the HMS server. This prevents significant malicious activity before entering a medical constrained domain. The flow model that illustrates various stages involved in MS_LPMD scheme is referred in Fig. 2.

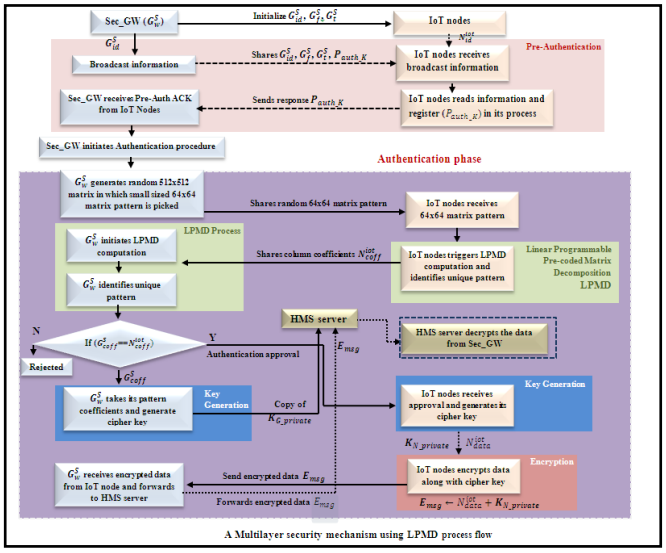


Fig. 2. Flow model of MS_LPMD scheme

The proposed MS_LPMD approach is elaborated in the following sections in notion with security and performance as key factors. The various stages involved in the proposed MS_LPMD scheme is as follows:

A. Pre-Authentication

With the assumption that the Secure Gateway creates station ids for all its IoT Nodes (N_{id}^{iot}). This station id (N_{id}^{iot}) is configured in all legal IoT Nodes. During the pre-authentication phase, the secure gateway in a particular location broadcasts its information. The broadcasted control message contains secure gateway's Network id/BSS (gateway's Id), the frequency, timing etc. Along with the broadcasted information the secure gateway sends a common authentication message, which is referred to as pre-authentication messages to all the IoT nodes irrespective of its geographical presence in that area. All IoT nodes receives the control messages broadcasted by secure gateway. After each IoT Node receives the control message, it reads the information like the gateway's station id, the pre-authentication key, etc., and registers the pre-authentication key in its process. The IoT Node then responds back to the secure Gateway (primary authentication server) indicating that they have read the pre-authentication key and other information and they are ready for data communication. Now the secure gateway (primary authentication server) would challenge each IoT Node for its authenticity. i. e. After receiving the pre-authentication acknowledgement from the IoT Nodes, the secure Gateway initiates a real authentication procedure. Here is where we start using the proposed Multilayer security using linear programmable pre-coded matrix decomposition process as described below.

B. Authentication

Usually, conventional or existing work use Hadamard pattern[15] or Walsh code[16] function (a pre-coded matrix) during authentication for pattern generation. The disadvantages in these methods is that it generates a unique pattern but they are orthogonal. i. e. any 64 x 64 hadamard pattern can be rearranged easily by the hacker or intruder as it always solves the problem called orthogonality factor (summation of all elements either row wise or column wise or diagonal wise is equal to zero), which is the flaw in earlier thought process. In our current approach, we ignored using orthogonality function, while we focused on the usage of non-orthogonality function i. e. we will not be using hadamard or pre-coded orthogonality function or Walsh. We rather generate a 512 x 512 non-orthogonal matrix within which a small sized 64x64 matrix is randomly picked. This process is initiated by the secure gateway. This random 64 x 64 matrix pattern is chunked by secure Gateway and sent to all IoT Nodes. Once the 64 x 64 matrix is received by each IoT Nodes, the computation of LPMD is initiated i. e. the proposed algorithm starts functioning at the IoT Node.

Unique pattern construction by IoT Node using LPMD algorithm

The IoT Node now starts the computation using the 64 x 64 matrix pattern received from the secure Gateway, to find a unique pattern of (64x1 matrix) i. e. to select a particular column in 64 x 64 matrix that satisfies the following pre-set criteria's:

Criteria 1: The elements of particular column in the 64 x 64 matrix upon summation should result in non-orthogonality factor. i. e., ($\sum_{i=1}^{k} e_i \neq 0$), where k=64.

Criteria 2: If the column selected is said to be non-orthogonal upon satisfying criteria 1, then it should ensure that the summated element value should not be greater than '+m' and not less than '-m'. i. e. $-m \geq \left(\sum_{i=1}^{k} e_i\right) \leq +m$, where m = 1.

So, there are possibilities that the 64 x 64 matrix satisfying the above said criteria's can result in,

Case 1: one or more pattern satisfying the conditions

Case 2: only one pattern satisfying the condition

Case 3: none of the pattern satisfying the condition

Case 1: In the first case, where one or more pattern satisfies the set criteria, the selection priority is given to pattern that is above zero or equal to +m rather than below zero or-m pattern. i. e, selection priority is given to +m pattern. i. e. upon computing the column elements, the proposed algorithm verifies to check if there exists a pattern whose $\left(\sum_{i=1}^{k} e_i\right) \leq +m$, if it finds a pattern that satisfies the condition whose value is above zero or equal to +m, then that would be column selected as a unique non-orthogonal pattern for further processing. In case, if there are no patterns that satisfies the condition $\left(\sum_{i=1}^{k} e_i\right) \leq +m$, while there exists patterns that satisfies $-m \geq \left(\sum_{i=1}^{k} e_i\right)$, then the proposed algorithm, selects the first column that generated the pattern which satisfied the condition, $-m \geq (\sum_{i=1}^{k} e_i)$, as its unique pattern for further processing. Fig. 3. displays the unique column pattern of 64x1 matrix identified using 64x64 matrix pattern.

Fig. 3. Single 64x1 columns selected as unique pattern in 64x64 matrix

This reduces the computation time at the IoT Node side. Same manner if there are no-m patterns, all are only +m patterns, then the proposed algorithm, selects the first column that generated the +m pattern as its unique pattern.

Our proposed algorithm leverages an idea to divide the problem of finding a best unique 64-bit pattern being solved is splitted into two problems namely: the Master problem and Sub problem. This division of problems into master and sub-problems has enabled great reductions of computation times of optimization algorithms both in exact methods and heuristics. Details regarding the algorithmic process for master and sub problem is elaborated in Algorithm 1 and 2 in following sections.

Case 2: In the second case, where only one pattern in 64 x 64 matrix satisfies upon computation, the said criteria, then that single pattern would be considered as the unique pattern for further processing.

Case 3: In the third case, where there are no column in 64 x 64 matrix that satisfies the pre-set criteria of non-orthogonality while considering a single 64 column, then the matrix is broken down into chunks say, two 32 x 32 matrix and the computation process is executed to find combination of 2 columns (32 elements each) that satisfies the above set criteria. Same process is initiated to find the first best unique pattern that satisfies the criteria and combination of the all selected unique pattern columns is then combined to form the 64 column element matrix. This process of breaking the matrix into small parts (8x8 matrix) continues as long as our condition is satisfied. Combination of column ids (when multiple column elements form the unique pattern is considered) are collectively stored by the IoT Node for further processing.

Algorithm 1: Unique column coefficient generation using master problem

Algorithm 1: "Master problem"” is the original problem which considers the given 64*64 matrix.
Input: The 64x64 matrix retrieved from secure gateway is considered as input.
1. **Identification of Problem**: Identifying unique column coefficients for authenticating with secure gateway
2. **Initialization step**: From the given problem (P), construct the Master problem (MP) using 64x64 matrix
Initialize unique_ col_coeff=0;
3. Applying Master problem to 64x64 matrix
if (unique_ col_coeff)
Col coeff is identified;
break;
end
if (~unique_ col_coeff)
if (matrix row length == 64)
unique_ col_coeff= Pass 64x64 matrix to sub problem;
if (unique_ col_coeff)
Col coeff is identified; /*unique pattern found in 64x64 matrix
break;
elseif (matrix row length == 32)
unique_ col_coeff = Pass list of 32x32 matrix to sub problem;
if (unique_ col_coeff)
Col coeff is identified; /*unique pattern found in 32x32 matrix
break;
elseif (matrix row length == 16) or (matrix row length == 8)
repeat steps as like in above process set for 32 matrix or64 matrix
end
else
Discard the 64x64 matrix retrieved;
Send request to secure gateway for new 64x64 matrix pattern;
end
Output: set of unique_ col_coeff after applying Master problem.

Fig. 4. displays the unique column pattern of two 32x1 identified using 32x32 matrix pattern.

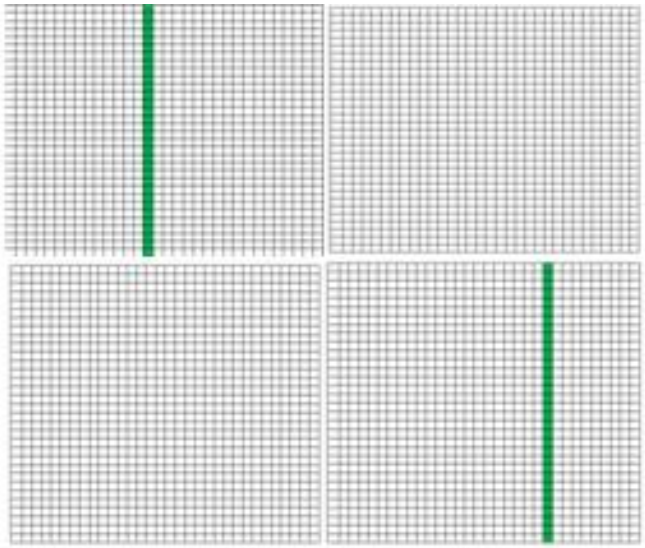


Fig. 4. Two 32x1 column selected as unique pattern in 32x32 matrix

In case even after breaking the matrix into small sub-parts, the above said condition is not satisfied, then the 64 x 64 matrix received from the gateway will be discarded by the IoT Node and it sends a request to Secure Gateway indicating that it was unable to construct the unique pattern using the 64 x 64 matrix it received and hence requests secure gateway for new 64 x 64 random matrix for further computation. We pre-assume that in a random matrix generation pattern the third case would never occur or may occur at a rarest case. Now, after selecting the unique pattern column or
columns (where a single column of 64 x 64 matrix does not satisfy the condition, then as the unique pattern identification is done using sub-matrix say two 32x32 matrix or four 16 x 16 matrix etc), there are possibility that the column selected for unique pattern would be single column or combination of multiple columns to form a 64 element unique pattern matrix. The column ids (if it is a single, it will be a single column id or if it is multiple column combination, then it will be multiple column ids) of the identified unique pattern matrix, will be combined and sent as column coefficients $N_{coeff}^{iot} = \{c_1 \ldots, c_i\}$ where 1 >= i <= 8 by IoT Node to the secure gateway.

Unique pattern re-construction by secure gateway using LPMD algorithm

Secure gateway upon receiving the column coefficients N_{coeff}^{iot} sent from IoT Node, will re-construct the unique pattern using the same LPMD algorithmic process to identify the unique pattern using the same 64x64 matrix it shared with the IoT Node earlier. It generates the column id or set of column ids as its column coefficients $G_{coeff}^{s} = \{c_1 \ldots, c_i\}$ where 1>= i <= 8. Secure Gateway now validates, the column coefficients generated at its end with the column coefficients received from the IoT Node for authenticity. If the column coefficients of secure gateway and IoT Node matches against each other, then the authentication is said to be successful otherwise the IoT Node is considered to be unauthenticated node and its request for data communication is rejected by the secure gateway. i. e.,

if ($N_{coeff}^{iot} == G_{coeff}^{s}$) *then*
"Authentication is successful"
"IoT Node is authenticated as a reliable node for communication"
"Secure Gateway Approves IoT Node's Data Communication Request"
else
"Authentication fails"
"IoT Node is an unauthenticated node"
"Secure Gateway rejects IoT Node's Data Communication Request"
End

Algorithm 2: Unique pattern identification using sub problem

Algorithm 2: "Sub problem" is used to find the unique 64x1 matrix pattern's column coefficients.
Input: The matrix pattern from master problem is given as input to the sub problem.
find len_{matrix}; /*Find length of the matrix*/
If (len_{matrix} == 64) then
/*Find unique pattern that satisfies the said conditions
for i = 1: len_{matrix} /*Parse column by column (64x1) matrix */
if (($\sum_{i=1}^{k} e_i \neq 0$) && (-$m \geq \left(\sum_{i=1}^{k} e_i\right) \leq +m$))
Store $col_{elements}$ /*column is said to be the unique pattern column*/
Store col_{coeff} /* column coefficients are identified */
Set unique_ col_coeff = 1;
return ($col_{elements}$, col_{coeff}, unique_ col_coeff);
else if (len_{matrix} == 32) then
Get the list of all 32x32 matrix;
l_{matrix}=length (list of32x32 matrix) ; /* Find the list length
for i=1: len_{matrix}
/*Find unique pattern that satisfies the said conditions
if (($\sum_{i=1}^{k} e_i \neq 0$) && (-$m \geq \left(\sum_{i=1}^{k} e_i\right) \leq +m$))
Store $col_{elements}$; Store col_{coeff}
if ($col_{elements}$==64)
Set unique_ col_coeff = 1;
return ($col_{elements}$, col_{coeff}, unique_ col_coeff);
end
end
end
Repeat similar steps for 16x16 matrix and 8x8 matrix until unique matrix element pattern is identified.
end
Output: Unique pattern and its column coefficients are obtained.

The Secure Gateway being the primary authentication server validates the authenticity of the IoT Node. Secure Gateway verifies and approves IoT nodes data communication request only if it is said to be an authenticated node otherwise it

rejects the request. Secure Gateway establishes a secure communication channel between authorized IoT Nodes for subsequent data communication.

Proposed MS_LPMD scheme is built to protect the confidentiality, integrity and availability of network data by making the system reliable and protecting the system from malicious attacks which can lead to information disclosure. Unlike other certificate-based method that requires computation-intensive process the proposed model incorporates an effective authentication mechanism that proved highly secured on IoT devices. Key objective of the proposed mechanism is that there is no key sharing across the wireless channel for authenticating devices. Rather only secret unique coefficients are sent through the medium blocking any malicious activity by eavesdropper. Thus by approving authorized IoT Nodes, the gateway securely and efficiently controls remote end-user IOT Nodes for further communication. Once the authentication by secure gateway is done successfully, IoT Node (medical sensor device) is authorized as a trusted entity so that data from IOT Node's side is transmitted to the HMS (secondary authentication) server through the secure gateway (primary authentication). Fig. 5. displays the line diagram for pre-authentication and authentication process using MS_LPMD scheme.

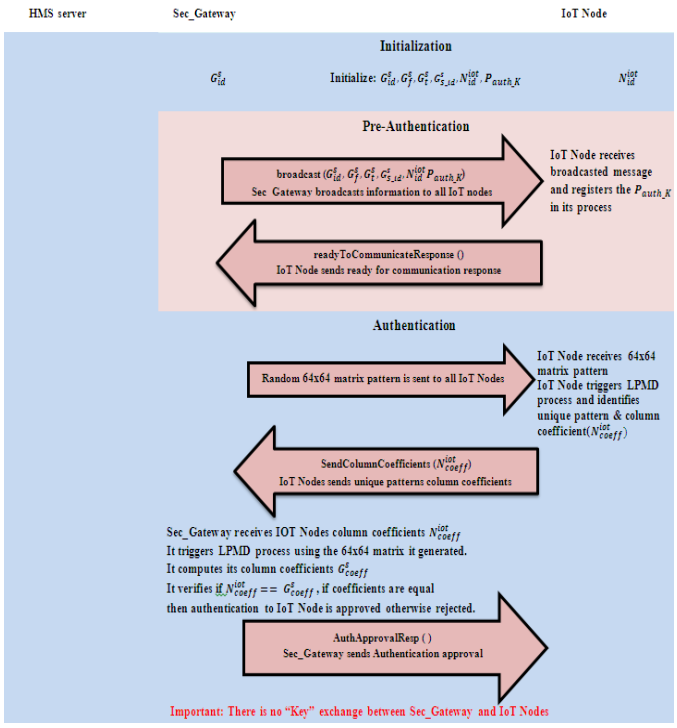


Fig. 5. Line diagram illustrating pre-authentication and authentication phase in MS_LPMD scheme

2. 3 Data Confidentiality:

Secure Gateway sends response to IoT Node indicating whether it was approved or rejected for further communication. Simultaneously the secure gateway fetches the first consecutive 16 elements and last consecutive 16 elements of the unique 64x1 matrix pattern to form a 32 bit cipher key ($\boldsymbol{K}_{N\_private}$)for subsequent data encryption and communication. The cipher key($\boldsymbol{K}_{G\_private}$) generated by the secure gateway is then shared with the HMS (secondary authentication) server through secure Layer 3-VPN (3G/4G/LTE). Authenticated IoT Nodes, receives the approved response for further communication from the secure gateway. Using the column coefficients, the first consecutive 16 elements and last consecutive 16 elements of the unique 64x1 matrix pattern are merged to form a 32 bit cipher key ($K_{N\_private}$) for subsequent data encryption and communication. Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can read it. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. In our proposed LPMD scheme, using the cipher key ($K_{N\_private}$) the IoT Node encrypts the original data turning the original message (O_{msg}) to encypted message or ciphertext (E_{msg}). Encrypted message is then passed through the secure tunnel or communication channel created through authentication process to the secure gateway. Secure Gateway upon receiving the encrypted message forwards it to the secondary authentication server or HMS. We pre-assume that the communication channel between secure gateway and the HMS is a secure Layer 3-VPN (3G/4G/LTE) connection. Once the encrypted message is received by the HMS server, it decrypts the message using the cipher key to retrieve the original message. Proposed scheme uses a simple but effective cryptographic functions for cipher text generation and exchange across secure gateway. Line diagram illustrating data confidentiality phase in MS_LPMD scheme is displayed in Fig. 6.

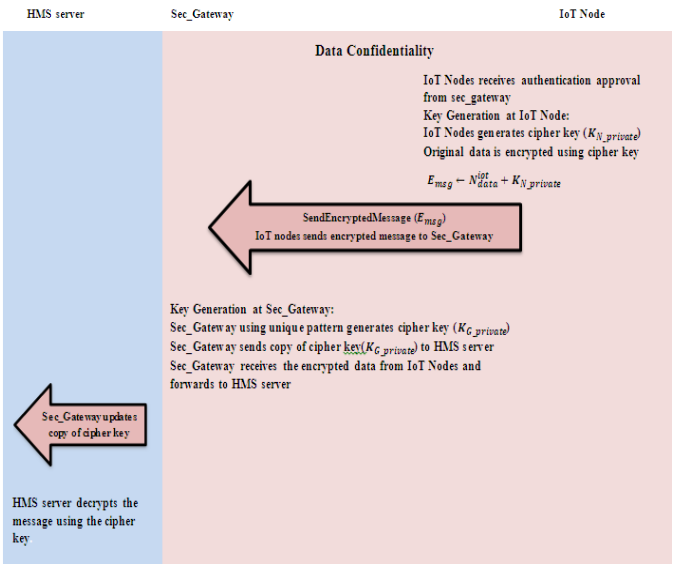


Fig. 6. Line diagram illustrating data confidentiality phase in MS_LPMD scheme

Simulation and Experimental Analysis

Performance of the proposed MS_LPMD approach using the test bed setup was evaluated using MATLAB simulation engine. The MS_LPMD algorithm was developed using self-written script in MATLAB integrated with Raspberry Pi based IoT sensor from Libellium [17] as shown in Fig. 7.

Our experiment consists of a pack of IoT healthcare sensors and gateway from Libelium, and HMS server integrated to setup a test bed environment as shown in Fig. 8.

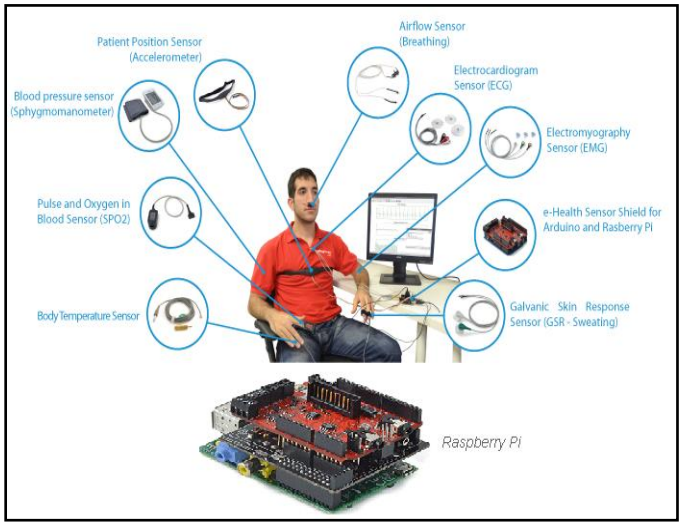


Fig. 7. IoT healthcare sensor nodes integrated using Raspberry Pi from Libellium

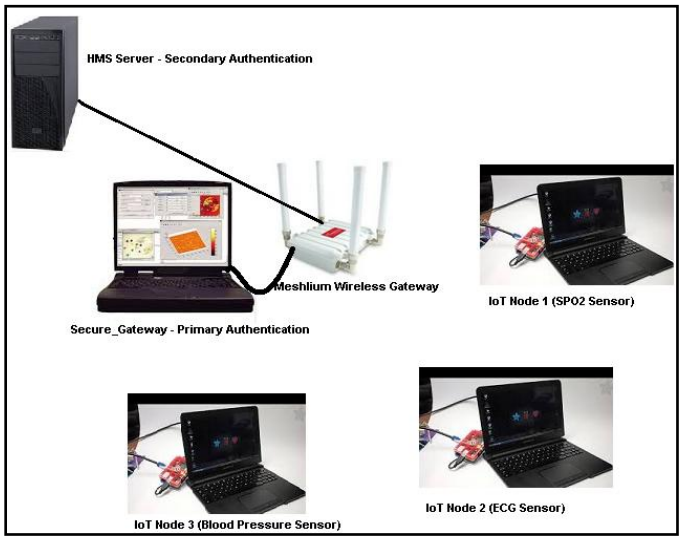


Fig. 8. IoT Testbed for MS_LPMD scheme experimentation

Security analysis and performance of the proposed MS_LPMD approach was analyzed using the following metrics:

Receiver Operating Characteristic:

Performance of proposed MS_LPMD approach is evaluated by analyzing ROC against existing ECDH scheme. ROC considers only the True Positive Rate (TPR) or True Acceptance Rate (TAR) and False Positive Rate (FPR) or False Acceptance Rate (FAR). The True positive or True Acceptance in this case occurs when an authorized IoT Node authentication at secure gateway results in a success i. e. the percentage of times secure gateway correctly verifies a true claim of authenticated IoT Nodes identity. A false positive or false acceptance on the other hand occurs when an unauthorized IoT Node attempts for authentication at secure gateway and results in success, i. e. the percentage of times secure gateway produces a false accept. A false acceptance occurs when an unauthenticated IoT Node is incorrectly approved for data communication by secure gateway. The ROC curve referred in Fig. 9. proves that in the proposed MS_PLMD scheme, the attempt made by authorized IoT Nodes success rate increases (True positive rate is higher) while the attempt made by unauthorized IoT Nodes success rate never occurs nor is very minimal.

The ROC curve in Fig. 9. proves that the performance of MS_LPMD is better compared to existing ECDH scheme due to the factor that in MS_LPMD scheme uses non-orthogonality factor for unique coefficient generation which in-turn is used for cipher key providing higher security ensuring confidentiality, integrity and authenticity at the receiver. i. e. even if the eaves dropper hacks the column coefficient shared across the medium, generating the unique pattern using MS_LPMD algorithmic process becomes difficult for the attacker and hence would not be able to generate the cipher key for false acceptance at secure gateway.

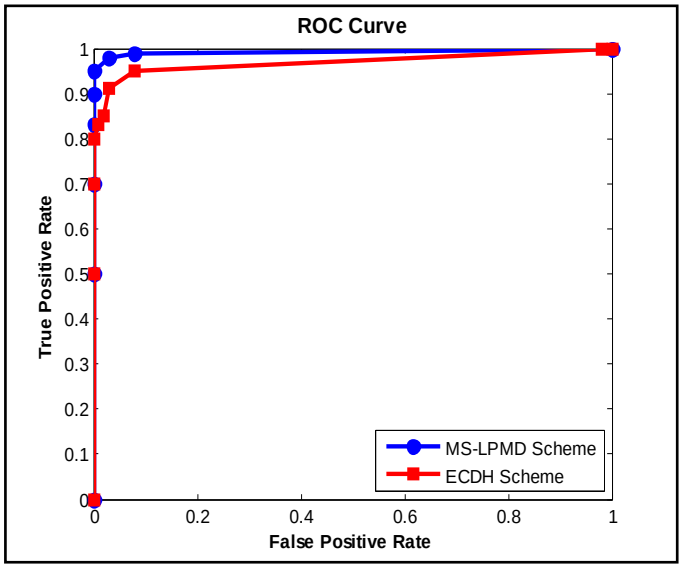


Fig. 9. ROC curve comparison graph between MS_LPMD Vs Existing ECDH scheme

Fig. 10. below displays secure gateway authenticates authorized IoT Node which using the cipher key encrypts glioblastoma cancerous cell image and sensor data and sends them in encrypted format, the same at HMS server is decrypted to retrieve the original image and sensor data for further processing.

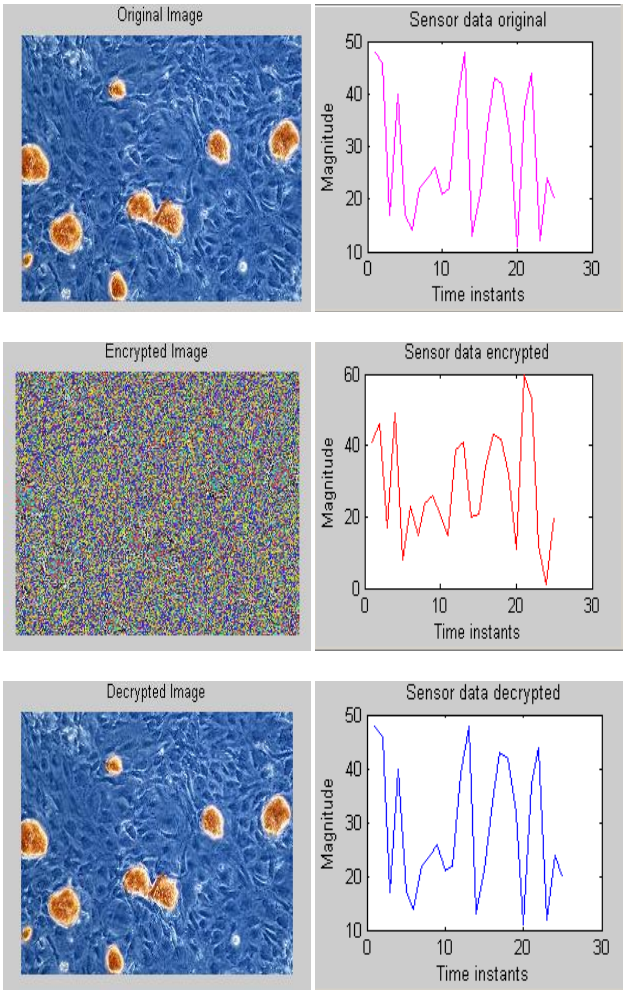
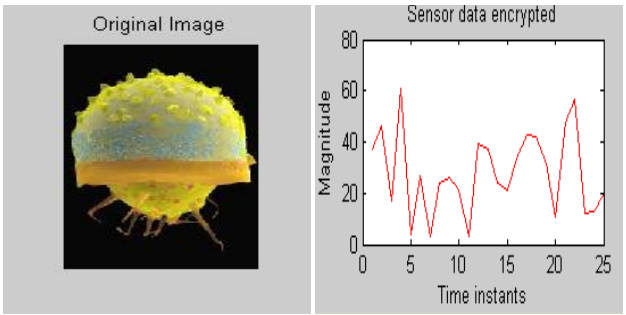


Fig. 10. Authorized IoT healthcare sensor node's data retrieved at HMS server using MS_LPMD scheme

While Fig. 11. displays eaves dropper trying to access the column coefficient shared through the medium, but unable to decrypt the encrypted image and sensor data to its original format as the attacker is unable to find the unique pattern to generate the cipher key for decryption.



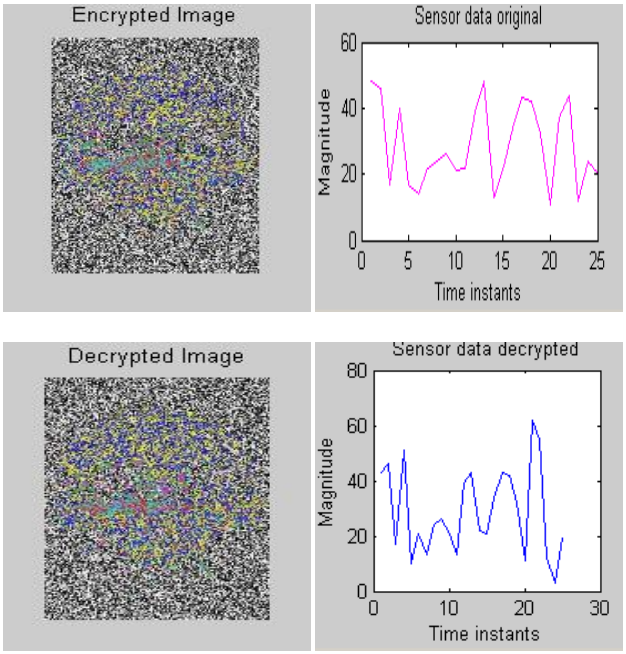


Fig. 11. External attacker or Eaves dropper fails to retrieve original data in MS_LPMD scheme

Transmission Overhead:

As discussed before, once an authentication is approved for an valid IoT Node by secure gateway, the IoT Node initiate data communication through the secure communication channel established between the authorized IoT Node and secure gateway. Data transmission over size constrained IEEE 802. 15. 4 radio links, the messages must be additionally split into several packet fragments due to their extensive message size of 16. Transmission overhead comparison was done between the proposed MS_LPMD scheme and existing ECDH scheme. As referred in Table. 1, the measure transmission overhead of the existing ECDH scheme was 1724 bytes which cause in total of 28 packet fragments for the complete transmission of all messages from IoT Node to the HMS server. In contrast, for the proposed MS_LPMD scheme the measure transmission overhead (TO) was 1178 bytes and it cause 17 fragments totally. As the result, from the analysis its found that the transmission overhead in the proposed MS_LPMD scheme reduces by 29% compared to the existing ECDH scheme.

TABLE. 1. Performance comparison with proposed MS_LPMD and EDCH scheme

Scheme	$\text{Latency}^{\text{comm}}_{\text{node\_gw}}$	$Latency^{comm}_{gw\_HMS}$	TO bytes
Existing ECDH	8. 009 sec	~ 7 sec	1724
Proposed MS_LPDM	5. 001 sec	~ 7 sec	1178
Proposed MS_LPDM improvements (%)	21	0	29

Communication Latency:

Latency is defined as the time required from sending a request (from Iot Node) to confirming the response (Secure Gateway) between two peers. This metric is vital for time-critical applications such as IoT-based healthcare domains. To estimate communication latency, the time which is spent from IoT sensor node to the HMS server ($\text{Latency}_{\text{node}}^{\text{comm}}$) is calculated. This processing time deduced from the summation of communication latency from IoT healthcare sensor node to secure gateway ($\text{Latency}_{\text{node\_gw}}^{\text{comm}}$)and from secure gateway to the HMS server ($\text{Latency}_{\text{gw\_HMS}}^{\text{comm}}$) which can be written as:

$$\text{Latency}_{\text{node}}^{\text{comm}} = \text{Latency}_{\text{node\_gw}}^{\text{comm}} + \text{Latency}_{\text{gw\_HMS}}^{\text{comm}}$$

In this work, to compute the communication latency from the IoT Node to secure Gateway and from secure Gateway to HMS server, Matlab script was employed to track the time taken between each requests and responses. According to our analysis, the proposed MS_LPMD scheme achieves an almost better latency, it takes up to ~ 12 sec for complete communication. However, the existing EDCH approach required communication time upto ~15 sec for complete communication. As shown in Table 1, the latency required for communicating between the IoT Node and secure gateway was about 4. 008 sec for the proposed MS_LPMD approach whereas this time increases to about 8. 009 sec in existing ECDH scheme, while the latency time taken for communicating between the secure gateway and HMS server was about approximately 7 sec in existing scheme and approximately around 6 sec in proposed scheme. Thus, regarding the latency from the IoT Node to the secure gateway, the proposed MS_LPMD scheme obtains about 21% improvement compared to the existing EDCH approach.

Throughput, Encryption Time and Encryption Frequency:

Higher security level has always been an inverse factor to bandwidth and data throughput in wireless networks. When the security level increases, it consumes certain bandwidth by decreasing the overall throughput due to frequent updates of control messages. MS_LPMD approach was architected considering the dynamic nature of network and their topologies with respect to application based architecture. Existing methods like AES, ECDH etc have shown considerable improvement in the security level but their performance in terms of Encryption frequency, Data throughput and Encryption time were not commendable against new challenges. Based on the analysis, the MS_LPMD scheme was able to perform data communication to the HMS server with minimum encryption time and maximum throughput when compared to all the existing algorithms. The enhanced authentication mechanism implemented using non-orthogonality function for generating the unique pattern used for creating the cipher proved to be efficient compared to other existing algorithms. Experimental analysis conducted for various applications like audio (*. WAV,. *. MP3), image (*. JPG, *. JPEG, *.. TIFF, *. DOC, *. TXT, *. PDF etc) and data have shown that the encryption time taken for MS_LPMD is lesser by 25%-35% compared to existing algorithms. This proves that MS_LPMD scheme is better suitable for critical application centric future wireless network. Proposed scheme is a light-weight mechanism as it consumes only 1 or 2 bytes for secret coefficient transmission which is low compared to existing algorithms that consumes 4 to 32 bytes for secret key exchange. Additionally the encryption frequency also proves to be equivalent and better than existing algorithm, ensuring effective encryption-decryption process. Based on the analysis, the MS_LPMD scheme proves to be better ad effective method compared to other existing schemes. The Fig. 12. illustrates the comparison between various algorithms against MS_LPMD scheme.

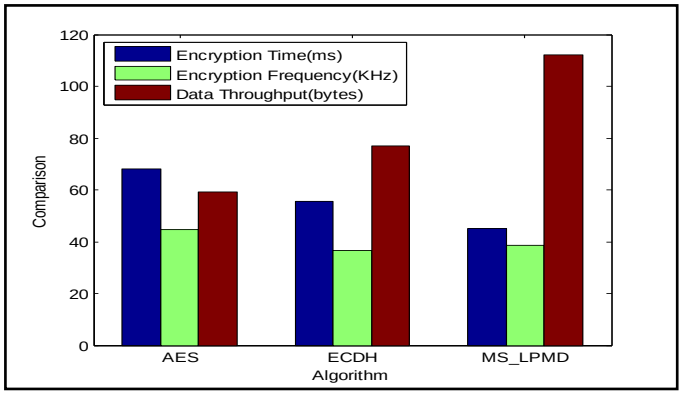


Fig. 12. Encryption Time, Encryption Frequency and Data Throughput Vs Various Algorithms

Number of Hits:

The number of hits required by Eaves dropper to retrieve the appropriate unique pattern for cipher key generation using the secret column coefficients. Fig. 13. shows the comparison of various algorithm for identifying the cipher key. Proposed MS_LPMD scheme displays higher number of hits required for identifying the correct cipher key using the column coefficients, the reason being that the cipher key is not exposed or exchanged between devices as like in other existing schemes ensuring higher security level compared to other existing approaches.

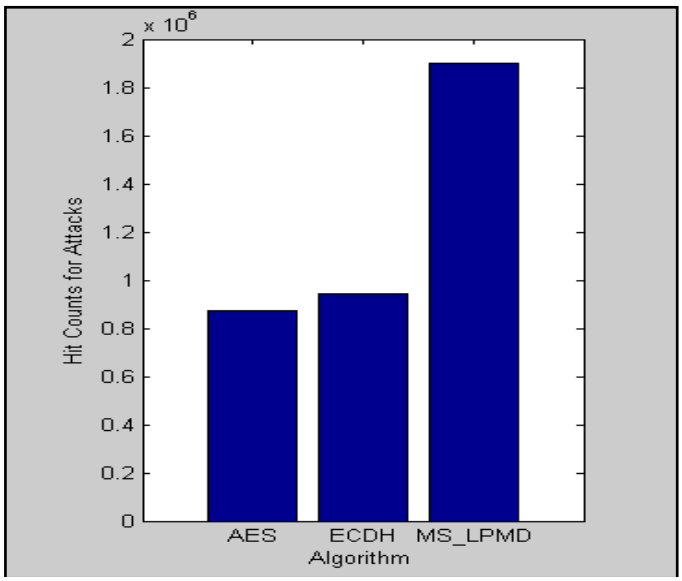


Fig. 13. Number of hits required for identifying the cipher key across various algorithms

Conclusion

In this paper, we presented a secure and light-weight protocol based authentication and authorization architecture for IoT-based healthcare system. IoT sensor nodes in healthcare systems are extreme computing resource constrained nodes that cannot cope-up with complex cryptographic techniques that are conventionally used. To alleviate this limitation, after thorough research with modern test-bed (software-hardware co-designed IoT test bed) and further mathematical analysis, we have proposed an architecture that employs a simple light-weight computational process for unique pattern identification and cipher key generation by IoT Node. The proposed MS_LPMD approach was formulated keeping in view all these challenges to bring out an efficient, unified and robust security mechanism that meets the current and future requirements. It has outperformed other existing approaches such as AES, EDCH etc, in terms of higher security level and trust worthiness factor. The performance analysis revealed that our proposed MS_LPMD approach has less communication overhead and latency between the IoT Node and secure gateway. Our test-bed computed results on standard simulation constraints shows an average reduced overhead of 29% and latency of 21%, compared to EDCH. Therefore, the presented architecture is a very promising solution to provide scalable and reliable end-to-end security for IoT-based healthcare systems. The work can be still enhanceable in the areas of new attacks and security concerns arising due to problems like hidden node, collision, interference etc.

References

[1] ITU-T Internet Reports, Internet of Things, November 2005.

[2] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo. A survey on facilities foR experimental Internet of Things Research. IEEE Commun. Mag., 49:58-67, 2011.

[3] C. Gehrmann, C. J. Mitchell, and K. Nyberg, “Manual authentication for wireless devices, ” RSA Cryptobytes, vol. 7, no. 1, pp. 29-37, 2004.

[4] S. Laur and K. Nyberg, “Efficient mutual data authentication using manually authenticated strings, ” in Proc. CANS 2006. Springer-Verlag, December 2006, pp. 90-107.

[5] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, “Talking to strangers: Authentication in ad-hoc wireless networks, ” in Proc. NDSS’02. The Internet Society, February 2002.

[6] J.-H. Hoepman, “The ephemeral pairing problem, ” in Proc. 8th Int. Conf. Financial Cryptography. Springer-Verlag, February 2004, pp. 212-226.

[7] S. Vaudenay, “Secure communications over insecure channels based on short authenticated strings, ” in Proc. CRYPTO 2005, Springer-Verlag, August 2005.

[8] S. Creese, M. Goldsmith, R. Harrison, B. Roscoe, P. Whittaker, and I. Zakiuddin, “Exploiting empirical engagement in authenticated protocol design, ” in Proc. SPC 2005. Springer-Verlag, April 2005, pp. 119-133.

[9] M. C˘ agalj, S. C˘ apkun, and J.-P. Hubaux, “Key agreement in peer-to-peer wireless networks, ” IEEE (Special Issue on Cryptography and Security), vol. 94, pp. 467-478, 2006.

[10] F.-L. Wong and F. Stajano, “Multi-channel protocols, ” in Proc. Security Protocols Workshop 2005. Springer-Verlag, 2006.

[11] T. Kindberg and K. Zhang, “Context authentication using constrained channels, ” HP Laboratories, Tech. Rep. HPL-2001-84,. April 2001. [Online]. Available: http://www. hpl. hp. com/techreports/2001/HPL-2001-84. pdf

[12] Anindya Bakshi, Bluetooth Secure Simple Pairing, wirelessdesignmag. com, cover story December 2007

[13] Fast, Reliable and Secure Digital Communication using Hadamard Matrices-Pal S. K, DRDO Scientist Analysis Group, Published on “Computing: Theory and Applications”, 2007 ICCTA IEEE Publications.]

[14] H. Wang, D. Peng, W. Wang, H. Sharif, H. Hwa Chen And A. Khoynezhad, ”Resource-aware secure ECG health care monitoring through body sensor networks”, IEEE Wireless Communications, 2010:vol. 17, p. 12-19.

[15] W. Ouyang, W. K. Cham, “Fast algorithm for Walsh-Hadamard transform on sliding windows”, IEEE Trans. on Pattern Analysis and Machine Intelligence 32, 165-171, 2010.

[16] S. Kak, “Classification of random binary sequences using Walsh-Fourier analysis”. IEEE Trans. On electromagnetic Compatibility EMC-13, pp. 74-77, 1971.

[17] Libellium, https://www. cooking-hacks. com/documentation/tutorials/ehealth-biometric-sensor-platform-arduino-raspberry-pi-medical