Biomedical Research 2016; Special Issue: S53-S59 *ISSN 0970-938X*
www.biomedres.info

An efficient secure authentication on cloud based e-health care system in WBAN.

A. Antony Viswasa Rani*, E. Baburaj

Department of Computer Science and Engineering, Sun College of Engineering and Technology, India

Abstract

The wireless body area network has emerged a new technology for e-health care system. WBAN collects the sensitive data on a patient's body and these data are stored in cloud servers and shared by various users. Various research works are carried out due to its sensitiveness and privacy problems. In sensor networks, spoofing attack is trouble-free to initiate (i.e.) an attacker pretends to be someone else to gain access to restricted resources or to steal information. Most conventional security approaches used cryptographic authentication to prevent spoofing attacks. Due to their computational complexity these security approaches are not always desirable. This paper proposed an Integrated Secure Authentication (ISA) in e-health Care application using cloud environment to use spatial information of Received Signal Strength (RSS), a physical property associated with each node, that is difficult to modify, and not based on cryptography. Similarly, Tri Mode Algorithm is introduced that can secure the data storage and fully authenticated data sharing from the use of Trusted Third Party (TTP). The algorithm can be implemented on three stages SetUP, CheckUP and LockUP. A simulated and analytical result highlights the security, efficiency and simplicity of our proposed scheme is better than the existing approach.

Keywords: Cloud computing, E-health care system, Integrated secure authentication, Received signal strength, Wireless body area network.

Accepted on April 15, 2016

Introduction

Wireless sensor network is a network of distributed autonomous devices that can sense or monitor physical or environmental conditions superlatively [1]. Nowadays, Wireless Sensor Network (WSN) applications have been used in several important areas, such as health care, military, environment monitoring, critical infrastructure monitoring and manufacturing. Existing methods for patients' vital data collection require a great deal of manual work to collect input and analyze the information. These methods are usually slow and error prone, introducing a delay that prevents real-time data accessibility. In a paper [2] the author proposed a new data collection method using cloud computing. It is easily manageable, scalable and reliable. An integrated system based on WSN for monitoring a patient is described in paper [3]. Information Technology is a vital part in disease management [4].

E-Health can include the interaction between patients and health service providers, or peer-to-peer communication between patients and/or health professionals. E-health should be efficient, thereby it decreases costs. It should enhance the quality of care. It should enable consumers to easily obtain health services online from global providers. The new technologies in E-Health care are an important part of medical treatment and follow up procedures. Medical records of patients can be effectively shared with a wide range of users, including staff from health care providers, and their family members. Electronic Health Record (EHR) will become the essential source of information for future health care providers and rapidly take over the role of the paper-based medical records. The first technical challenge regarding data reliability has to do with the importance of having EHR data available to authorized health care providers once they have been created and recorded in a patient. The second technical challenge is data security and privacy of an EHR system. Because data in an EHR are stored and transmitted in a distributed environment over a network, data encryption and access authentication are very important to protect privacy of patient data [5].

Body Sensor Network (BSN) is formed by placing the physiological parameter sensors in the human body, on the body surface or around the body. The technology of Sensor, Pervasive computing, and Intelligent Information Processing is used in BSNs [6]. BSN research has concentrated on health care applications, addressing the weaknesses of the traditional patient data collection, such as imprecision and under sampling. In contrast, BSNs can continuously capture quantitative data from a variety of sensors for longer periods. Sensor nodes are placed in the body to collect physical data and perform preliminary processing. The data are gathered by a sink node and then transmitted to a base station in order to share over the internet, which is the basis of many applications

including health care systems. In such e-health care information systems, patient data are stored in a distributed environment, allowing health care providers in different locations to share and access easily a variety of EHR. Therefore, a reliable, secure, and efficient data storage infrastructure is critical to future health care systems. However, there are several technical challenges, including reliability, security, and adequate online performance that make the design and implementation of such distributed data storage difficult. Access by unauthorized users to patient data may result in misdiagnosis, delays in treatment, or mistreatment.

Cloud computing offers several advantages by allowing users to use infrastructure, platforms and software provided by the cloud providers. They make use of unlimited storage and computing resources. As such, the PHR providers are more and more willing to shift their PHR storage and application services into the cloud instead of building specialized data centres, in order to lower their operational cost. Google Health and Microsoft Health Vault respectively, are the PHR service provided by Google and Microsoft respectively [7]. In health care, the use of cloud computing has been proposed as a means for maintaining health records, monitoring patients, managing diseases and cares more efficiently and effectively, or collaborating with peers and analyzing data. The flawless integration of Wireless BANs and Cloud Computing provides terrific opportunities for pervasive healthcare systems [8].

There are many security and privacy risks while the PHR services are in the cloud for everyone. The privacy of patient's personal health data and who could gain access to the PHRs when they are stored in a cloud server are the main problems. Currently the ABE scheme is used for data access control for PHRs, and greatly reduces the key management complexity for data owners and users. In [9], the authors propose a lightweight identity based encryption, which is suitable for sensors, and developed protocols based on IBE-Lite for a BSN. But the researchers do not concentrate on data communication threats. During the data communication, the spoofing attacks are possible. This area is concentrated and proposed a new algorithm for secure authentication and access control. Data collection is very important in health care, any little problem happened in, this will entirely affect the patient. Today the encryption scheme is used for secure transmission. Any security system used in health care should be fast, because time is an important factor in health care. But if we use encryption, definitely certain delay will occur. So the proposed system uses the physical property Received Signal Strength (RSS) for the security.

This paper proposed an Integrated Secure Authentication (ISA) in e-health care application using cloud environment to use spatial information of Received Signal Strength (RSS), a physical property associated with each node, that is difficult to modify, and not based on cryptography. Similarly, Tri Mode Algorithm is introduced that can secure the data storage and fully authenticated data sharing from the use of Trusted Third Party (TTP). The algorithm can be implemented on three stages SetUP, CheckUP and LockUP. A simulated and analytical result highlights the security, efficiency and simplicity of our proposed scheme is better than the existing approach. The rest of this paper is organized as follows: The related works are reviewed in the next section. In section III, briefly present preliminary notations and concepts for our approach. The proposed system is explained in section IV. The Results and performances are discussed in section V. Finally, the conclusion and future enhancement are in Section VI.

Background

Today a lot of research work is going on in the wireless sensor networks for medical applications. E-health data management is a main problem in modern hospitals [10]. The data generated is large, due to advanced medical techniques. The large amount of high sensitive data generated by medical sensor network introduces many challenges like scalability, availability and security. In [11], the authors propose an efficient and a flexible security mechanism that guarantees confidentiality, integrity and fine grained access control to outsourced medical data. Electronic Patient Record (EPR) management is sensitive which requires a fool-proof security. "Anonymity" and "trust" are two conflicting objectives in participatory sensing networks. Security is the critical requirement for using the e-health data in distributed environments like the cloud because of the data's sensitivity and sharing among different types of users. Using cloud as a storage user can be benefited by its elastic resources and reduced operational cost. Storing the health data in the cloud causes the patient to lose the control of their sensitive personal health data, which makes the necessity of encryption before storing the data to the cloud servers [12]. The need for security in sensor generated outsourced data is described in detail in the paper [13].

Initially the access control is based on various access policies and trust in health care providers like role based access control (RBAC) and attribute based access control (ABAC) [14,15]. ABAC is more flexibility than RBAC. For access control of outsourced data, partially trusted servers are often assumed. The goal is trying to enforce, who has access to which parts of a patient PHR documents in a fine-grained way. Symmetric key cryptography (SKC) based solution is proposed in [16] for fine grained access control. Here, the key distribution is difficult when there are multiple patients. The revocation of a particular user affects the remaining users and also users' write and read rights are not separable. To separate write and read privileges, Public key cryptography (PKC) based solutions were proposed. But here also high key management overhead occurred. Both SKC and PKC affected by scalability. So ABE (Attribute Based Encryption) scheme is introduced in [17,18], then, several works used ABE to realize fine-grained access control of outsourced data [19-22]. These works did not address the multiple data owner settings and patient-centric access control. Later cipher text policy ABE (CP-ABE) [23] is applied in paper [24] to manage the sharing of PHRs. Paper [25] presents an authentication method for WBSN and a secure data transmission using cryptography technique. Papers [26-33] deals with localization and security attacks based on

RSS. All the existing secure access control methods still use the encryption methods that make delay and more complex computations proposed new algorithm for secure access control which uses the physical property RSS which reduces delay and complex computations.

Preliminaries

Basic notations

Several basic notations are described for convenience. Let RL denote a set of registered devices in the network which includes user devices and access points, RLd U RLs. RLd is the Registered user's IP address, $\{ip_1, ip_2 \ldots ip_m\}$, m is total number of registered Device IPs. And RLs is the access point's IP address $\{ip_{m+1}\ ip_{m+2} \ldots\ ip_n\}$, n is total no. of registered Station IPs where (0<m<n), t is total no. of registered IPs (m +n). Each IP has its own Training set is denoted as TS, which contains K set of records $TS_{r(ipx,rss)}$, which include ip address and RSS threshold min and max. Ipx means x's IP address, 'x' may be a user or access point. Rss_{ipx} is the Received Signal Strength of x's IP Address. AL is the Authentication list which includes set of AL records ($AL_{r(ipx,th\_rss)}$) of the registered user's or Access point IP address and RSS values. Each IP (user device/Access point) contains the TDB, TDB is the Training Database, contains set of training record $N(r)ip_x$. src_{ip} is the source IP address.

Assumptions

In BSN, the participating devices and users are known (REGISTERED) and their device identifier is static and in fixed location. Transmitting and receiving power is the same. So, we can find out the RSS value with path loss and trained the system. The RSS value should not be changed. This could be chosen as a security parameter.

Received signal strength

Received Signal Strength (RSS) is a property that is closely related to position in network space and is freely offered within the existing wireless networks. The RSS readings at the same physical location are alike, whereas the RSS readings at different physical locations are dissimilar. Thus, the RSS readings extant strong spatial relationship characteristics. The Received Signal Strength value array as s = (s1, s2,…sn) where n is the number of landmarks that are watching the RSS of the wireless nodes and know their locations in the wireless network grid. Usually, the RSS reading at the ith landmark from a wireless node is dispersed as

$$S_i(d_j)[dBm] = P(d0)[dBm] - 10Y\log\left(\frac{d_j}{d_0}\right) + Xi \quad (1)$$

Where P (d0) represents the transmitting power of the node at the local distance d0, Y the path loss exponent and, d_j is the distance between the wireless node j and the ith landmark, Xi is the shadow fading which is given as input. For simplicity, we are assuming the nodes have the same transmission power. If the RSS does not match in consecutive RSS values, then the node is said to be malicious.

Spoofing attacks

IP spoofing is the act of manipulating the headers in a transmitted message to mask a hacker, true identity so that the message could appear as though it is from a trusted source. IP spoofing is used to gain unauthorized access to a computer. The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system. Spoofing attacks affect the network performance as well as facilitate many forms of security weaknesses, such as attacks on access control mechanisms and denial-of-service. Wireless spoofing attacks are easy to launch and can significantly affect the performance of networks. Due to their computational complexity the existing security approaches are not always desirable. Proposed system uses a physical property associated with each device, which is difficult to modify, and not based on cryptography, as the basis for detecting spoofing attacks.

Proposed System

Our proposed system is divided into two phases, Data collection and Data retrieval. In both phases the authentication algorithm is used so that the data are securely stored and accessed. The BSN architecture (Figure 1) contains a variety of sensors. From the sensors the data are collected and given to the aggregator or coordinator and then via an access point it is transmitted. Before getting stored in the cloud, the TTP checks the authentication. If it is successful, then the data are stored into the cloud.

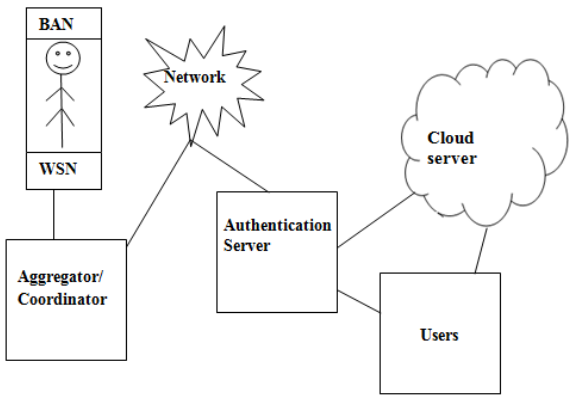

Figure 1. BSN architecture.

This paper proposed an Integrated Secure Authentication (ISA) in e-health care application using cloud environment to use spatial information of received signal strength (RSS), a physical property associated with each node, that is difficult to modify, and not based on cryptography. Similarly, Tri Mode Algorithm is introduced that can secure the data storage and fully authenticated data sharing from the use of Trusted Third Party (TTP). The algorithm can be implemented on three stages SetUP, CheckUP and LockUP. The authentication is

used to store the data to the cloud and also access the data from the cloud. Patient vital parameters are collected by various sensors using BSN and the collected data are stored in the cloud through the TTP. When the data is accessed by the registered users the authentication is verified by its IP address and its RSS value.

SetUP mode

This is the initial mode, which is used to train our system. Using the SetUp algorithm the data are trained and generated the authentication list. For each IP/device present in the e-health system, the proposed method has to calculate its RSS threshold value from the packet transmission. For each IP/ device, the proposed system has to calculate RSS for k transmissions, and takes the mean value and find out the RSS minimum and maximum threshold value.

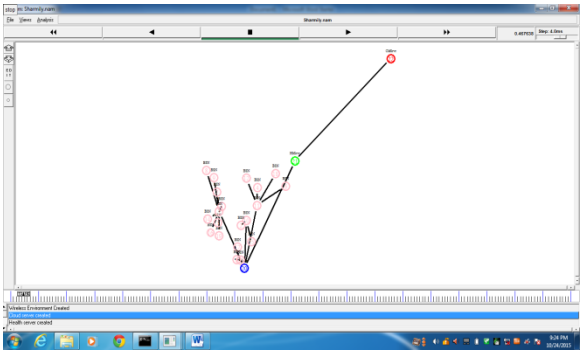

Figure 2. *BSN environment.*

When the packets received by the Trusted Third Party from the registered IP list, it checks the k value. If it is less than k-1, then extract the RSS value from the packet, and store the training set record in the Training data base. If it is k-1, then write the training set record in the database and calculate the RSS mean value for the particular IP using the Equation (2) and calculate the standard deviation using Equation (3) and then find out the rss-min and rss-max threshold value using Equation 4 and Equation 5 respectively. Then the values are placed in the Authentication list AL.

The mean of a data set is simply the arithmetic average of the values in the set, obtained by summing the values and dividing by the number of values. Hence the mean of the RSS is calculated as

$\mu_{ipx} = rss_{ipx}(1 \leq i \leq k; x \in RL)$ (2)

The Standard Deviation of a data set is the arithmetic average of the squared differences between the values and the mean. The standard deviation is the square root of the variance. Hence the variance of the RSS is calculated as

$\delta_{ipx} = (rss_{ipx} - \mu_{ipx})^2 (1 \leq i \leq k: x \in RL)$ (3)

The RSS threshold is calculated as the addition of mean value and standard deviation. Hence the th_rss_{ipx} calculated as

$thmax\ (rss_{ipx}) = \mu_{ipx} + \delta_{ipx}$ (4)

$thmin\ (rss_{ipx}) = \mu_{ipx} - \delta_{ipx}$ (5)

Algorithm: Set Total no.of samples k per IP

At each IP Packet received at TTP

1. If src_{ip} is in the Registered list (RL) then
2. If N (src_{ip} in TS) < k-1 then
3. extract rss
4. store TSr (ipx, rss) in TDB
5. else if N (src_{ip} in TS) = k-1 then
6. extract rss
7. write TSr (ipx, rss) in TDB
8. read TSr (ipx= src_{ip}) from TDB
9. Cal.1: Calculate the mean value of rss_{srcip}
10. Mean μ_{ipx} (ipx= src_{ip}) using (2)
11. Cal.2: Calculate S.D. value of rss_{srcip}
12. S.D δ_{ipx} (ipx= src_{ip}) using (3)
13. Cal.3: Calculate Min & Max Threshold value of rss_{srcip}
14. thmax ($_{ipx}$) (ipx= src_{ip}) using (4)
15. thmin ($_{ipx}$) (ipx= src_{ip}) using (5)
16. write AL (ipx, thmin ($_{ipx}$), thmax ($_{ipx}$)) where ipx= src_{ip}
17. end if
18. end if

CheckUP mode

The second mode is very important, and in this phase only, the authentication of the user is verified and they are allowed/ denied the access of e-health system. This process is done at TTP. TTP verifies the authentication by receiving the packet from any one of the IP. When a packet is received at TTP, it checks whether the Particular IP belongs to the registered list and also present in the authentication list. If it is, then it extracts the rss value, and this value is compared with the authentication list and if it is between the min and max threshold value, the authentication is successful and the data is sent to the cloud server or get the data from the cloud server. Otherwise the authentication is failed

Algorithm: Require: A new Packet received at TTP

1. If src_{ip} in RLd & srcip in AL (ipx) then
2. extract rss_{srcip}
3. read thmin (rss_{srcip}), thmax (rss_{srcip}) from AL
4. if thmin (rss_{srcip}) ≤ rsssrcip ≤ thmax (rss_{srcip}) then
5. authentication success
6. send data to cloud server
7. else
8. authentications failed
9. end if
10. else if src_{ip} in RLs & src_{ip} in AL (ipx) then
11. extract rss_{srcip}
12. read thmin (rss_{srcip}), thmax (rss_{srcip}) from AL
13. if thmin (rss_{srcip}) ≤ rsssrcip ≤ thmax (rss_{srcip})then
14. authentication success
15. Get data from cloud server
16. Send pack to src_{ip} with th(rss_{srcip})

17. else
18. Authentication failed
19. end if
20. else
21. Authentication failed
22. end if

LockUP mode

It verifies the TTP. When a new packet is received at the user, it verifies the IP address and verifies the rss value. If it contains the correct threshold the Accept the packet, otherwise drop the packet.

Algorithm: Require: A new Packet received at User

1. If src_{ip} is TTP_{ip} then
2. extract rss_{srcip}
3. extract th_rss_{pack} from packet
4. If $rss_{srcip} \leq th\_rss_{pack}$ then
5. Accept the packet
6. else
7. Drop the packet
8. end if
9. end if

Results and Discussion

The proposed system has been designed and simulated using NS2 and dotNet. The health care system and the authentication system are analyzed. Data freshness: Data freshness algorithm is used in the Setup mode. Initially during training, for all the devices registered in our system we are calculating the RSS value and its threshold are defined. Later, if variations occur for continued access ie if any access is denied due to some environmental changes, then the data freshness algorithm is fired and a new dynamic threshold is defined for the particular device/users and it is updated in the database.

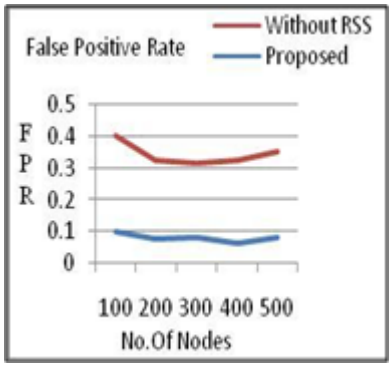

Figure 3. *False positive rate in data collection phase.*

The wireless body sensor network is implemented in NS2. The diagram (Figure 2) describes the wireless environment with body sensor nodes, aggregator, health server and the cloud server. The BSN nodes are represented as pink node, the aggregator is represented as blue node, the health server is colored as blue and the cloud server is differentiated with red color node.

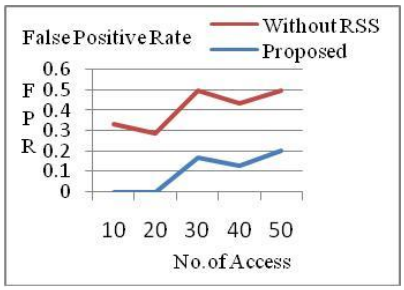

Figure 4. *False positive rate in data retrieval phase.*

The efficiency of our authentication system is verified by the parameters: False Positive Rate, False Negative Rate, Sensitivity, Specificity and Accuracy. The False Positive Rate (FPR) is the proportion of negatives cases that were incorrectly classified as positive, as calculated using the equation:

$$FPR = \frac{False\ Positive}{False\ Positive + True\ Negative} \quad (6)$$

The false negative rate (FNR) is the proportion of positive cases that were incorrectly classified as negative, as calculated using the equation:

$$FNR = \frac{False\ Negative}{False\ Negative + True\ Positive} \quad (7)$$

Sensitivity (True Positive Rate) measures the proportion of positives that are correctly identified (eg. the percentage of authorized person who are correctly identified)

$$Sensitivity = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (8)$$

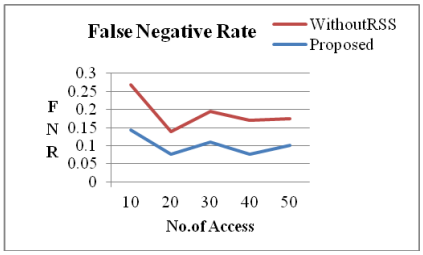

Figure 5. *False negative rate in data retrieval phase.*

Specificity (True Negative Rate) measures the proportion of negatives that are correctly identified. e.g., the percentage of unauthorized person who are correctly identified).

$$Specificity = \frac{True\ Negative}{True\ Negative + False\ Positive} \quad (9)$$

The accuracy is the proportion of true results (both true positives and true negatives) among the total number of cases examined.

$$Accuracy = \frac{True\ Result}{True\ result + False\ result} \quad (10)$$

For our analysis, the system assumes 20% of the access/nodes are attacker. Proposed system got a better result when compared to previous works in terms of efficiency, complexity

and overhead which is shown in the graphs below. False positive Rate (Figure 3 and Figure 4) and False Negative Rates (Figure 5 and Figure 6) for data collection and retrieval phase are shown in figures. The Accuracy of our authentication system is shown in Figure 7. Authentication Sensitivity and Specificity is shown in Figure 8 and Figure 9 respectively.

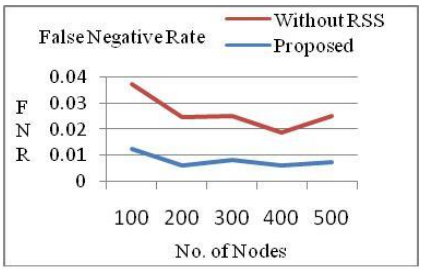

Figure 6. *False negative rate in data collection phase.*

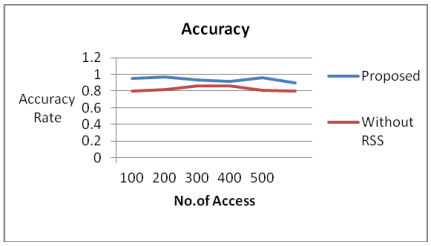

Figure 7. *Authentication accuracy.*

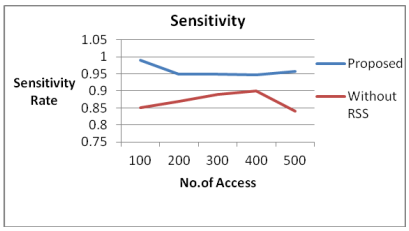

Figure 8. *Authentication sensitivity.*

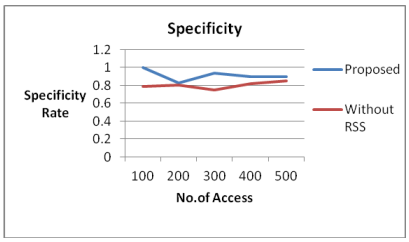

Figure 9. *Authentication specificity.*

From the graph the overall system performance in terms of accuracy, False Positive, False Negative, Sensitivity and specificity is above 95%. Thus our system is implemented with better results than the existing authentication system.

Conclusion and Future Enhancement

This paper investigated the authentication problem in cloud based e-health system by proposing a Tri Mode algorithm. The RSS value received by a device present in the e-health system is trained and stored in the authentication list using the SetUP algorithm. The user authentication is verified by the CheckUp algorithm and the user is either allowed or denied to access or store the data from or to the cloud. This work concentrates on a single health care authority. In future add More than one health care authority and also the outside attacker should be analysed. In the future also proposed to design a method for public sharing and data publication.

References

1. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Commun Mag 2002; 8: 102-114.
2. Rolim CO, Koch FL, Westphall CB, Werner J, Fracalossi A, Salvador GS. A cloud computing solution for patient's data collection in health care institutions. 2nd International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED '10), St. Maarten, 2010.
3. Rotariu C, Manta V, Ciobotariu R. Integrated System Based on Wireless Sensors Network for Cardiac Arrhythmia Monitoring. Adv Electric Comput Eng 2013; 13: 95-100.
4. Pohoață S, Graur A. HDTV System for Parkinson's Disease Diagnosis. Adv Electric Comput Eng 2013; 13: 91-96.
5. Yang KQ. Secure and efficient data replay in distributed eHealth care information system. International Conference on the Information Society (i-Society), London, 2010.
6. Lai X, Liu Q, Wei X, Wang W, Zhou G, Han G. A Survey of Body Sensor Networks. Sensors 2013; 13: 5406-5447.
7. Li M, Yu S, Ren K, Lou W. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In Security and Privacy in Communication Networks 2010; Springer Berlin Heidelberg.
8. Wan J, Zou C, Ullah S, Chin-Feng L, Zhou M, Wang X. Cloud-Enabled Wireless Body Area Networks for Pervasive Healthcare. Network IEEE 2013; 27: 56-61.
9. Chiu CT, Wang H, Zhong S, Li Q. IBE-Lite: A lightweight Identity Based Cryptography for Body Sensor Networks. IEEE Transact Info Technol Biomed 2009; 13: 926-932.
10. Ahmed S, Abdullah A. E-healthcare and data management services in a cloud In High Capacity Optical Networks and Enabling sTechnologies (HONET) 2011.
11. Ahmed L, Abdelkrim H, Abdelmadjid B, Yacine C. Secure and Scalable Cloud-based Architecture for e-Health Wireless Sensor Networks. International Conference on Computer Communication Networks (ICCCN), Munich, Germany, 2012.
12. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Transactions on Parallel and Distributed systems 2013; 24: 131-143.
13. Rani AAV, Baburaj E. Security in sensor generated outsourced data: An overview. Int J Appl Eng Res 2015; 10: 161-165.

14. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM TISSEC 2001; 4: 224-274.
15. Scholl M, Stine K, Lin K, Steinberg D. Draft security architecture design process for health information exchanges (HIEs). Report, NIST, 2009.
16. di Vimercati SDC, Foresti S, Jajodia S, Paraboschi S, Samarati P. Over encryption: management of access control evolution on outsourced data. VLDB 2007.
17. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine grained access control of encrypted data. CCS 2006.
18. Li M , Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wireless Commun 2010; 17: 51-58.
19. Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. CCS 2008.
20. Ibraimi L, Petkovic M, Nikova S, Hartel P, Jonker W. Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes Centre for Telematics and Information Technology, University of Twente, 2009.
21. Yu S, Wang C, Ren K, Lou W. Attribute based data sharing with attribute revocation. 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2010.
22. Xin D, Yu J, Yuan L, Yingying C, Guangtao X, Minglu L. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. Comput Security 2014; 42: 151-164.
23. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. IEEE S& P 2007.
24. Ibraimi L, Asim M, Petkovic M. Secure management of personal health records by applying attribute-based encryption. 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth) 2009.
25. Xu G, Liu S, Liu Y. A Secure Transmission Protocol for Wireless Body Sensor Networks. J Software 9: 2043-2049.
26. Chen Y, Trappe W, Martin RP. Detecting and Localizing Wireless Spoofing Attacks. 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks 2007.
27. Yang J, Chen Y, Trappe W. Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. IEEE Transaction on parallel and distributed system 2013; 24: 44-58.
28. Chen Y, Kleisouris K, Li X, Trappe W, Martin RP. A Security and Robustness Performance Analysis of Localization Algorithms to Signal Strength Attacks. ACM Trans Sensor Networks 2009.
29. Chen Y, Yang J, Trappe W, Martin RP. Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks. IEEE Transactions Vehicular Technol 2010; 59: 2418-2434.
30. Lau EEL, Boon-Giin L, Seung-Chul L, Wan-Young C. Enhanced Rssi-Based High Accuracy Real-Time User Location Tracking System For Indoor And Outdoor Environments. Int J Smart Sensing Intel System 2008; 1: 534-548.
31. Papamanthou C, Preparata FP, Tamassia R. Algorithms for Location Estimation Based on RSSI Sampling. LNCS 2008.
32. Viani F, Rocca P, Oliveri G, Trinchero D, Massa A. Localization, tracking, and imaging of targets in wireless sensor networks: An invited review. Radio Sci 2011; 46: 1-12.
33. Vaghefi RM, Buehrer RM. Received Signal Strength-Based Sensor Localization in Spatially Correlated Shadowing. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2013.

***Correspondence to:**

A. Antony Viswasa Rani

Department of Computer Science and Engineering

Sun College of Engineering and Technology

India