ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

Severity and Security Analysis of Medical Internet of Things

Stalin David D[1]

PhD Research Scholar, Department of CSE, PSN College of Engineering and Technology, Tirunelveli, Tamilnadu, India[1]

ABSTRACT: Recent trends and the accurate knowledge of human anatomy allow the healthcare professionals to handle the emergency scenario. Remote monitoring of patients by the healthcare professionals or doctors through the utilization of Wireless Sensor Network (WSN) offers the solution to the shortage problem. The special form of WSN used for remote monitoring called Wireless Body Area Network (WBAN) or Wireless Medical Sensor Network (WMSN) utilizes the numerous sensors that collect the data from the human body and send it to the central device for processing (raising the alarm for anomalies detection) and storage. This paper presents the survey of WMSN topologies, data sharing mechanisms, cryptography and attributes-based encryption in privacy preserving in detail.

KEYWORDS: Attribute-based encryption, Cryptography, Data sharing, Security, Wireless Medical Sensor Network.

I. INTRODUCTION

Diverse characteristics of Wireless Medical Sensor Network (WMSN) compared to the generic Wireless Sensor Network (WSN) (human involvement, human involvement, scalability, mobility and reliability) [1]facilitate remote monitoring of patients in healthcare applications. The brief exploration of several health care projects (AlarmNet, MobiCare, MediSN, UbiMone) and their privacy issues convey that the maintenance of strong security against the several attacks is the major requirement for providing the immediate treatment to the patients. An integration of vigor concern tune-up systems with the cloud computing architecture [2, 3]employs the physiological sensing devices that are capable of continuous monitoring and raising the alarm for abnormal situations. This nationwide approach enables the government to create new policies and strategies in order to prevent the epidemic / chronic diseases. The ambiguous plan captures the data confidentiality by using the combination of several encryption mechanisms. The applications of WSN[4]in healthcare system split up into following categories: patient monitoring, axis watching for (chronic and elderly patients and long-term database collection. The extension of application areas of WMSN states that the improvement and upgrade of a system are major requirements to deal the security and privacy issues. With the huge deployment of sensors, the records about the individual deceased are collected and convey them to the links. The investigation of interactions in the data flow between the parties in WBAN [5] in four scenarios such as home, hospital, emergency and open areas identify the requirements of new BAN models. Ensure of the defense and confidentiality purposes depends on threats on telemetry interface, software and sensor interface layers[6]. During the transmission, several protection schemes [7] are engaged to shelter the data. But, the immediate stop provision for insider attack is not possible that leads to the distribution of data among the multiple servers. Vigorous unidentified substantiation procedure [8] provides the high security with the better computational efficiency compared to existing protection schemes.

The analysis of wireless communication protocols [9] conveys that the features for high security and privacy preserving are data bandwidth, frequency band, power consumption, encryption and authentication methods. The vulnerability of WSN against the fault types and external attacks is high and thus the suitable anomaly detection algorithm is required to overcome the issues in vital sign collection and remote monitoring. The identification of the location of the sensor is the prior stage of data collection. The major issues in the remote complex consumption are packet loss and congestion

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

during the data collection process. The data protection mechanism available in research studies conveys the unique characteristics and misbehaviors of nodes in WMSN. The security and performance of WSN depend on two constraints such as cooperation and trust assurance of WMSN nodes [10-13].

Substantial improvements and the diagnostically access of rich patient are the promising aspects of remote health monitoring Quality compromise of data hinder these aspects cause the several security issues. Monitoring of vital signs of normal and attack behavior along the routing paths overcome those issues with the requirement of slots allocation to isolate the emergency and non-emergency situations[14, 15]. Cross- layer design of WMSN associated with numerous protocols specifies the unique constraints for the isolation. These resource constraints as well as the lofty stipulate of defense / privacy introduces the new challenges. Lightweight detection mechanisms [16, 17], Game theory[18] and MAC protocols[19] are employed to improve the trust and security level in remote monitoring.

The maintenance of connectivity and trustworthy is an important criterion in the secure link establishment between the MSN nodes. The impact of high resource constraints and the heterogeneous characteristics of the devices in the WMSN make the key management schemes [20-22] as inefficient. Hence, Pauthkey[23] and secure data transmission protocol[24] are employed to meet the constraints and characteristics of MSN nodes. The major objective of the medical device place in the individual stiff is to collect the individual data as unremarkable and universal. Hence, the certificate-less remote anonymous protocol[25] is used to overcome the issues in the security provision. If the clandestine input is leaked during the transmission, the revoking mechanism may helpful to meet the demand. A massive quantity of information generation and collection using the multiple sensors introduce the challenges such as scalability, availability and integrity. Attribute-based encryption schemes [26-29] and the fuzzy-based ABE [30] address the aforementioned issues for providing the swapping connecting the defense and elasticity in health care applications. The introduction conveys that the data protection against the insider attack is the most important concern during the remote patient monitoring system. Besides, the numerous processes involved in cryptographic and attribute-based algorithms causes the computational overhead and time. Hence, the security assurance with less computational overhead is the major limiting factor of WMSN.

The dissertation is structured as follows. Section II describes the WMSN topologies with enhanced techniques, data sharing mechanisms, cryptographic algorithms and ABE schemes in detail. Section III briefly presents the overview of the survey and finally the paper concludes in Section V.

II.RELATED WORK

High security against the new threats with less computational overhead is the major requirement in remote health care monitoring through the WMSN. The security assurance depends on the location of sensors, faults occurred in the network, resource constraints, co-operation and malfunctioning activities. Numerous strategies are employed to assure the high security in data transmission. This division discusses the techniques in detail.

A.Trust evaluation techniques in WMSN

The general scenario of remote patient monitoring system comprises the several processes as follows: data collection through the wireless sensors with resource constraints, analysis of collected data and rising of false alarms if the abnormalities are detected. The addition of assessment hierarchy with the linear regression [12] facilitates the aforementioned processes. The integration contains two operating phases such as detection and training. The generation of models for classification constitutes the training phase and the classification of inputs as abnormal constitutes testing phase. Besides, the detection of abnormal instances by using J48 triggers the forecasting and hence it is restricted with small intervals. The specific action to overcome the restriction is trust relationship establishment between the nodes. The parameters[11] to provide the trust evaluation are listed in Table I.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

TABLE I PARAMETERS FOR TRUST EVALUATION

Parameters	*Description*
subject	First node
Agent	Second node
{*subject, agent, action*}	Trust relationship
T	Trust value

The establishment of trust evaluation includes three ways as follows:

1. The observation of *agent* behavior by *subject* establishes the *direct trust*
2. The non-observation of *agent* behavior by *subject* behavior leads to raise up of recommendations
3. The utilization of *trust* records by *subjects* establishes the historical trust.

After the trust evaluation, the data transmission is initiated between the nodes. Based on the patients priority and the traffic priority, the allocation of bandwidth and the drop probability definition depends on the congestion control protocol [13]. The major function of the sensor network is to collect the statistics and convey them to the destination node. The identification of a location of collected data is the initial stage in data transmission. Hence, the localization techniques are evolved in research studies. The concepts behind the localization are described in Table II.

TABLE II LOCALIZATION CONCEPTS

Concept	*Description*
Laterization	Measurement of distance between the nodes to estimated location
Angulation	Measurement of angle between the nodes to estimated location
Trilateration	Estimation of location based on distance measurement between the three nodes
Multilateration	Location estimation by using the distance measurement between many nodes (> three)
Triangulation	Position estimation by using the two angles of unlocalized nodes from the localized nodes

Range-free and range-based localization techniques[10] are used to estimate the locations of sensor nodes. The mathematical formulations for these methods are illustrated in Table III.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

TABLE III RANGE-FREE AND RANGE BASED METHODS

Method	*Equation*	*Description*
Range-free	Centroid formulation: $(X_{est}, Y_{est}) = \left(\frac{X_i, + \cdots +, X_N}{N}, \frac{Y_i, + \cdots +, Y_N}{N}\right)$	X_{est}, Y_{est} – Estimated locations
	Distance: $D_{ij} = h_{j,A_i} d_{hop}$	d_{hop}-Estimated distance A_i-anchor node h- hop information
	Error: $E_j = \sum_{i=1}^{n} (d_{ji} - d^{ji})$	d_{ji}-Estimated distance
Range-based	Received Signal Strength Indicator (RSSI): $P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\lambda)^2 d^2}$	P_t-Transmittedpower $G_t G_r$-transmitter and receiver antenna gain d-distance λ- wavelength

The location estimation and the trust evaluation among the nodes are over; the necessary sensing data is shared between the sensors to the central station for remote monitoring. Several issues are observed during the data flow process and described in detail in the next section.

B.Data sharing

Loss and stolen of small size sensors and the identification of targets by an adversary requires the physical compromise. The secure lightweight system for MSN enables the key management scheme and provides the fine-grained access control. The lightweight system[16] comprises following phases: scheme initialization, regular use, user command and security analysis. Each phase of the light weight detection system employs the key generation mechanisms to validate the data delivery. The data tracking, specification requirements for authentication and the proof verification employs the watermarking protocols [14] to identify the fault location in MSN. Due to the several security issues, the lightweight and watermarking protocols face the difficulties in immediate treatment provision. The inclusion of power position authority to the traditional game theory approach under the Stackelberg Security Equilibrium [18] provide the solution to the problems in information maintenance. The mathematical formulation for positional authority is described as

$$P(S, J) = \sum_{i=1}^{n} \frac{\alpha_i S_i}{ps(\beta_i J_i)} \quad (1)$$

Where, S – sensors
J – jamming factor
α_i – No. of sensors placed within the body
$ps(\beta_i)$ – Position of jamming
ReTrust [17] models specify the following unique features of MSN compared to WSN based on (1):
1. Latency – The description of latency depends on the oomph utilization and the applications
2. Flexibility – Automatic monitoring of physiological readings by using the non-invasive sensors
3. Efficiency – trustworthy and exact of signals from the body sensors.
The overall trust estimation with the above differentiations is defined as follows:

$$T_{AB}^{total} = \epsilon_i \times T(A: B, act_1) + \cdots + \epsilon_p \times T(A: B, act_p) \quad (2)$$

Where, $\epsilon_i \ldots \epsilon_p$ – Weights of each action
A – Master node

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

B – Sensor node
$act_1 \ldots act_p$ – Measures
Depends on the weight value (high or low), the corresponding trust value is correspondingly defined. Large size data collection and transmission through the number of sensors induce the crucial problem, defense and isolation reasons in MSN.

C. Cryptography
The flexible strategy to transmit the data in a secure manner called hospital WSN security [24] and that includes the following stages:
1. *System setup* – transmit of ciao communication (Node ID, coordinate) by each sensor nodes
2. *Compressed sensing* – The signal samples related to the messages are compressed, encrypted and integrity protected through the hashing mechanisms to prevent the malicious modifications and reduce the energy consumption.
3. *Encryption* – Execution of lightweight algorithm for key update
4. *Control aggregation* –Utilization of Patient Health Information (PHI) facilitates the direct aggregation of Patient Personal Aggregator (PPA) to Room Controller (RC).
5. *Server aggregation* – Transmission of aggregated messages to the PC server

PauthKey [23], OPFKA [20] and Elliptic Curve Cryptography (ECC) [21] employs the aforementioned processes to provide the end-to-end security.

D. Attribute-based Encryption Scalability, availability and the integrity are the major challenges in the WMSN due to the high sensitive and large size data transmission among the nodes. ABE algorithms [26, 27, 29] address these issues to augment the defense level. The preliminaries of ABE include several processes as follows:
1. *Bilinear maps creation*–Mapping of two generators (G_1, G_2) of prime order (p, q) by using the injective function (e).
2. *Bilinear Diffie-Helman Problem (BDHP)* – Computation of injective function for new group from random numbers (a, b, c)
3. *Decisional BHDP* – Computation of hash value (h) for injective function to make the decision
4. *Key policy scheme* – The sequential processes of set-up, key generation, encryption and decryption constitutes key policy scheme
5. *Defense entertainment for ABE* – Submission of questions and access control structures by adversary, passing of encrypted text to the relevant queries by the challenger
6. *Access tree formation* – Decryption of ciphertext by using the key only if the assigned attributes are satisfied the tree structure.

.

III.SURVEY DISCUSSION

Various techniques for trust-assurance, fault identification, sensor location estimation, secure link formation and trust assurance among the nodes are depicted. The literature review can be described as Table IV. The review of congestion control, trust assurance, and fault detection in WMSN addresses the issues of power consumption, violation of links due to the wrong information propagation among the nodes and the unique features description. The maintenance of low false alarm ratio with the quick detection of patient abnormalities is the major consideration in the design of WMSN. To meet this constraint, the decision tree architecture is integrated with the linear regression formulation for efficient anomaly detection. But, the lack of mobility support and the dynamic adjustments of the route still investigating parameter in the trust evaluation mechanism.
High liability of conviction supervision schemes against the number of attacks is ignored in traditional trust mechanisms. This ignorance turns the research work into two-tier architecture of attack resistant and the trust management schemes. The incorporation of Collection Tree Protocol (CTP) with the conviction supervision plan provides the trade-off between high security and malicious behaviors detection. The cross-layer WBAN architectural framework (MAC frame and PHY frame) suffers from major challenges of new protocols generation which require the optimized solutions. To increase the lifetime of a network, the MAC framework is integrated with the energy harvesting architecture and power positional authority inclusion.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

The key materials embedded in the individual deceased caused the overlapping and its elimination requires the unique features. The existence of resource constraints and the heterogeneous characteristics make the authentication schemes as inefficient form. Certificate and certificate-less protocols are evolved in research studies address the issues in application level security provision. Key management complexities for user and data owner are higher in cryptographic algorithms. For that, the numerous statistics possessor scenarios and the division of users in multiple security domains reduce the key management complexities and achieve the fine-grained access control. The attributes related to the cipher text should gratify the admittance control structure for decryption of messages. The brief analysis of security mechanisms in WMSN conveys that the transaction flanked by the defense and computational overhead is the major requirement. To meet this, the cooperation and the split-up of data into multiple parts are the necessary stages in watching of disable persons.

TABLE IV INFORMATION ABOUT SECURE DATA TRANSMISSION SCHEMES IN WMSN

Techniques	***Author & Ref***	***Year***	***Description***	***Advantages***	***Limitations***
Wireless Medical Sensor Network (WMSN)					
Distributed Trust evaluation	He et al [11]	2012	Identification of unique features of MSN and the introduction of relevant node behaviors to detect the malicious nodes.	1. Effective identification of malicious behaviors 2. Secure unicast routing	1. Packet loss due to congestion 2. Less discrimination performance between the physiological signals
Congestion Control	Yaghm aet al [13]	2013	Assign of network bandwidth to the signals from the diverse patients consider the congestion situation in parent / child nodes.	1. Continuous monitoring while movement 2. Mobility support	1. More power consumption 2. Wrong information propagation leads to positional error
Localization Technique	Alrajeh et al [10]	2013	An investigation of the suitability of localization techniques for WSN applications and static sensors. The deep analysis of range / range-free localization techniques is also presented	1. Capability to take care of limited resources 2. High energy efficient with less hardware size	1. Less robustness 2. Less resilient to sensor failures for high critical systems
Sensor Fault Detection	Salem et al [12]	2013	Anomaly detection algorithm detects the instances and classifies them in normal and abnormal ways by using regression prediction.	1. Quick anomaly detection 2. High detection accuracy 3. Low false alarm rate	1. Less security due to unique operational requirements 2. High vulnerability to the attacks
Data Sharing in WMSN					
Retrust	Stalin David et al [17]	2018	Development of light weight trust management scheme called ReTrust and perform the experimental validation using collection tree protocol.	1. Efficient malicious / fault detection 2. Enhanced security and network performance	1. Stringent resource constraints lead to high-security demand for real-time applications

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

Lightweight	He et al [16]	2014	Lightweight and secure MAN system with hash-chain based key update employment is discussed. Besides, the lightweight protocol extended to provide backward secrecy.	1. Powerful mobile adversary 2. High feasibility for real-time applications	1. Compromise threat hinders the adoption in WMSN 2. Stemming of sensitive medical data
Fault tolerance	Goudar and Potkonjak[14]	2014	Addressed the issues in the robust watermarking approach to leave the primary / secondary semantic metrics.	1. High semantic accuracy 2. Effective recovery of bio-signal semantics 3. Robustness preservation	1. High power consumption 2. Less realization performance of network operation.
MAC	Qi et al [19]	2015	Briefly surveyed the progress involved in energy harvesting techniques for wireless and battery powered WBAN. They enabled the sensor node lifetime operation by using novel energy utility architecture	1. High significant on real-time online health services 2. Effective support for life-time operation	1. Lack of energy / traffic awareness induces the limitation in lifetime 2. Less security
Game theory	Somasundaram and Sivakumar[18]	2015	Briefly discussed the Game Theory with Stackelberg Security Equilibrium (GTSSE)-based patient monitoring.	1. High system flexibility level 2. Less energy consumption / information loss rate	1. Lack of isolation between the emergency and non-emergency 2. Abnormality detection to monitor the vital signs
Prioritization	Ullah et al [15]	2015	The cross layer WBNA design architecture with issues and challenges is presented. Briefly reviewed the strength and weakness of cross layer protocols employment in WBAN.	1. Efficient path selection for emergency 2. Low temperature and hop count	1. Secure inter-sensor communication is critical 2. Overlapping introduces the difficulties in patient health monitoring
Cryptography-WMSN					
OPFKA	Hu et al[20]	2013	The Ordered-Physiological-Feature-basedKey Agreement (OPFKA) allowed the belonging of two sensors in Body Area Network (BAN).	1. Low computational overhead 2. Feasible and efficient architecture	1. Lack of secure links between end-to-end communication leads to less trustworthiness 2. High resource constraints limit the performance.
PAuthKey	Porambage[23]	2013	Pervasive lightweight authentication and keying mechanism for WSNs in distributed IoT applications are proposed.	1. End-to-end security 2. Safety alarm creation if an abnormality exists. 3. Accurate data transmission.	1. Less guarantee of confidentiality 2. Scarcity due to resource constraints
Publish & Command Protocol	Sanchez et al [22]	2014	Publish and command protocols are proposed based on Ciphertext ABE (CP-ABE) schemes. The implementation of Lattice-Based Access Control (LBAC) policies by the sensors are showed.	1. Guarantee of confidentiality 2. Fine-grained access control based on LBAC	1. High latency for alarm provision 2. Minimal network lifetime

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

Secure Data Transmission Protocol	Stalin David et al [24]	2018	The novel design of hospital WSN security is presented. The requirements for hospital WSN security and the necessity of secure data transmission are pointed.	1. Feasible security for real-time applications 2. Less energy consumption and communication overhead	1. Eavesdropping and DoS attacks introduced in sensor network applications
ECC	Lee et al [21]	2014	Secure and efficient key management scheme based on ECC algorithm to protect Patient's medical information in the healthcare system is proposed.	1. Less energy cost for signature generation and verification 2. Reduction in time consumption	1. Collection of individual data in unobtrusively and ubiquitously manner leads to security issues
Certificate less Protocol	Padma et al [25]	2016	Certificate-less remote anonymous authentication protocol is proposed to overcome the individual data collection challenges.	1. Computational efficient 2. Highly scalable and security against the existential forgery	1. Lack of consideration of data management 2. High sensitive data gathering

IV. CONCLUSION

In this paper, an overview of various secure data sharing techniques on WMSN is presented. From the survey, it is observed that the trade-off between the storage overhead and security assurance is the major issue in healthcare monitoring applications. Data protection against the insider attacks is the difficult issue in traditional methods since they were not easily identified. Besides, the semi-trusted server's utilization caused the compromise and malfunctioning during the data sharing. This process facilitated the split-up of data into three servers and their cooperation among them are the major requirements once the user request is enabled. Hence, the presented survey provides the future directions to server split-up architecture, hash verifier and key exchange mechanism to assure the security in healthcare applications.

REFERENCES

[1] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, pp. 55-91, 2011.
[2] N. D. Han, L. Han, D. M. Tuan, H. P. In, and M. Jo, "A scheme for data confidentiality in cloud-assisted wireless body area networks," Information sciences, vol. 284, pp. 157-166, 2014.
[3] C.-w. Shen, C.-H. Hsu, C.-c. Chou, and T.-C. Tsai, "Toward a Nationwide Mobile-Based Public Healthcare Service System with Wireless Sensor Networks," Mobile Information Systems, vol. 2016, 2016.
[4] S. Juneja, S. Kendre, and U. Patkar, "Healthcare Analysis via Wireless Sensor Network," 2016.
[5] S. S. Ahmad, S. Camtepe, and D. Jayalath, "Understanding data flow and security requirements in wireless Body Area Networks for healthcare," in 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015, pp. 621-626.
[6] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in 2014 IEEE Symposium on Security and Privacy, 2014, pp. 524-539.
[7] X. Yi, J. Willemson, and F. Nait-Abdesselam, "Privacy-preserving wireless medical sensor network," in 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 118-125.
[8] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," Multimedia Systems, vol. 21, pp. 49-60, 2015.
[9] C. H. Vallejos de Schatz, H. P. Medeiros, F. K. Schneider, and P. J. Abatti, "Wireless medical sensor networks: Design requirements and enabling technologies," Telemedicine and e-Health, vol. 18, pp. 394-399, 2012.
[10] N. A. Alrajeh, M. Bashir, and B. Shams, "Localization techniques in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 2013, 2013.
[11] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, pp. 1164-1175, 2012.
[12] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, "Sensor fault and patient anomaly detection and classification in medical wireless sensor networks," in 2013 IEEE International Conference on Communications (ICC), 2013, pp. 4373-4378.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

[13] M. H. Yaghmaee, N. F. Bahalgardi, and D. Adjeroh, "A prioritization based congestion control protocol for healthcare monitoring application in wireless sensor networks," Wireless personal communications, vol. 72, pp. 2605-2631, 2013.

[14] V. Goudar and M. Potkonjak, "On Admitting Sensor Fault Tolerance while Achieving Secure Biosignal Data Sharing," in Healthcare Informatics (ICHI), 2014 IEEE International Conference on, 2014, pp. 266-275.

[15] F. Ullah, A. H. Abdullah, M. Q. Jan, and K. N. Qureshi, "Patient data prioritization in the cross-layer designs of wireless body area network," Journal of Computer Networks and Communications, vol. 2015, p. 5, 2015.

[16] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," IEEE journal of biomedical and health informatics, vol. 18, pp. 316-326, 2014.

[17] Stalin David D, 'A new expert system based on hybrid colour and structure descriptor and machine learning algorithms for early glaucoma diagnosis' Multimedia Tools and Applications , published by Springer(SCI Journal, IF : 1.595),Vol.77(2018),pp.1-12, ISSN: 1380-7501 (Print) 1573-7721 (Online),2018.

[18] M. Somasundaram and R. Sivakumar, "Game Theory Based Security in Wireless Body Area Network with Stackelberg Security Equilibrium," The Scientific World Journal, vol. 2015, 2015.

[19] X. Qi, K. Wang, A. Huang, H. Hu, and G. Han, "MAC protocol in wireless body area network for mobile health: a survey and an architecture design," International Journal of Distributed Sensor Networks, vol. 2015, p. 1, 2015.

[20] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in INFOCOM, 2013 Proceedings IEEE, 2013, pp. 2274-2282.

[21] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," in The International Conference on Information Networking 2014 (ICOIN2014), 2014, pp. 453-457.

[22] P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. Suarez-Tangil, "Secure publish-subscribe protocols for heterogeneous medical wireless body area networks," Sensors, vol. 14, pp. 22619-22642, 2014.

[23] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," International Journal of Distributed Sensor Networks, vol. 2014, 2014.

[24] Stalin David D, 'Textures and Intensity Histogram Based Retinal Image Classification System Using Hybrid Colour Structure Descriptor', Biomedical & Pharmacology Journal, Vol.11 (1),pp. 577-582(2018).

[25] M. S. Padma, D. J. W. Wise, M. S. Malaiarasan, and M. N. Rajapriya, "Ensuring Authenticity and Revocability for Wireless Body Area Network using Certificateless Cryptography," 2016.

[26] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy, 2013, pp. 31-36.

[27] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE transactions on parallel and distributed systems, vol. 24, pp. 131-143, 2013.

[28] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-health wireless sensor networks," in 2012 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1-7.

[29] Y. Tian, Y. Peng, X. Peng, and H. Li, "An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks," International Journal of Distributed Sensor Networks,Vol.2014, pp.1-9, 2014.