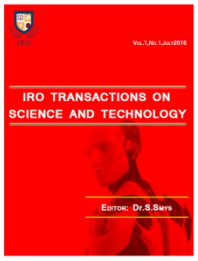
IRO TRANSACTIONS ON SCIENCE AND TECHNOLOGY

IROJOURNALS.COM

VOL.1, NO.1, JULY 2016




# Cloud Abetted WS-BAN forFar-off Healthcare using proposed Cushy Data Network (Cu-DN)

[1.] Dr. Syms, Professor and Head, Karpagam College of Engineeing, Coimbatore – 641048.
[2.] Mr. A. Dinesh Kumar, Research Scholar, Anna University, Chennai -641025
[1.]smys375@gmail.com, [2.]dineshinnov@outlook.com

## Abstract

The trendingprogresses in far-off healthcare systems enables researchers to concentrate on pervading and easily deployable healthcare systems which stands for medical information, applications, and infrastructure in a pervasive and fully automated manner. Security and privacy of data plays a major role in healthcare management system. This system should ensure the confidentiality of patients' data privacy. A major challenge for healthcare is how to provide enhanced services to a growing number of people using limited financial and human resources. Far-off healthcare is reflected a solution to many existing problems and a possible future of the current healthcare services. In simple terms, it can be defined as healthcare to anyone, anytime, and anywhere by removing locational, time and other restraints while increasing both its coverage and quality. These requirements could be effectively supported by universal, efficient and reliable access to healthcare services, providers, and biomedical information that is available at any time. Cloud Abetted wireless body area networks (WBANs) considerably assist resourceful patient treatment of high quality, inappropriately it's a great challenge about the patient's information secrecy and privacy. The traditional scenario focuses on where patients securely stay indoors. This research focuses on providing solution to more practical situation of cloud abetted WBANs in far –off healthcare where patients traverse among blocks outdoors where their data are more vulnerable to attack. This work proposes the secured network in order to provide secrecy and privacy to the patients' data while they are participating in far-off healthcare monitoring system. In this, the whole system is implemented in a cloud abetted wireless sensor body area network. This is of twofold: first, it attempts to secure the inter-sensor communication by multi-biometric based key generation scheme in WBANs; and secondly, the electronic medical records (EMRs) are securely stored in the hospital community cloud and privacy of the patients' data is preserved.

**Keywords:** Cushy Data Network (Cu-DN), Cloud Abetted, Wireless Sensor BAN and EMR.

## 1. Introduction

The use of Wireless Body Area Networks (WBANs) is momentously improving healthcare quality these days. WBANs haveattracted by significant attention because they have a wide range of applications from far-off health monitoring andcomputer abetted recuperation to emergency medical response systems. Other potential applications include interactivegaming, social computing, entertainment, and the military.The challenges coming from rigorous resource constraintsof WBAN devices, and the high demand for both secrecy / privacy and practicality/usability may prevent those applicationsfrom being widely deployed. In reality, secrecy and privacy protection of the data collected by a WBAN,either while stored inside the WBAN or during its transmission out of the WBAN, is a major mysterious problem. A possibleway to solve this problem is to exploit the benefits of cloud computing. However, the cloud also has its own set ofsecurity problems, in that the owner of the data may not have control of where the data is placed. Again,WBANs can in turn help to mitigate security problems with the cloud.Indeed, the integration of WBANs with cloud computing will create a new system named Cloud-abetted WBANs. Thisnew system provides a cloud computing

environment that links different devices from shrunken sensor nodes tohigh-performance supercomputers that process the huge amount of data collected from multiple WBANs. Since the challengesof resource constraints of WBAN devices are not a major concern when coupled with cloud computing resources,WBAN applications can be deployed on Cloud-abetted WBANs at competitive costs. The system also has a feature thatenables its users and applications to access its data from anywhere in the world. Therefore, the security and privacy ofthe data must be protected in the framework of this new system.In this paper, we propose a Cushy Data Network (Cu – DN) to overcome existing shortcomings in CloudabettedWBANs. Our scheme mainly deals with data confidentiality and provides a general paradigm for deploying applicationsin Cloud-assisted WBANs.

## 2. Related works

The related work scan be categorized in four fragmentsbased on the modules that establish the cloud abetted secure far-offhealthcare system i.e., far-off healthcare monitoring systems, cloud computing based architectures, and physiological valuebased key agreement and security for Cushy Data Network. A PDA-Based Patient-Monitoring System is a mobile patient monitoringsystem that uses a personal digital assistant (PDA) and a wireless local area network (WLAN). CodeBlue is an Adhocsensor network infrastructure for emergency medical care comprising low-power physiological sensors andPDAs. CodeBlue was proposed to improve the ability of first responders to evaluate patients while performingtheir normal duties. The MobiHealth System is an end-to-end healthcare platform for ambulant patientmonitoring deployed on UMTS and GPRS networks. The mobile healthcare systems discussed above are not cloudbasedand hence face the problems of accessibility, storage, and computational capabilities. The idea of connecting a mobile device to a cloud in order to get valuable information through queries,such as "what is the average temperature of nodes within a mile of my location?". The VMware hospital secure, private cloud provides services via an infrastructure-as-a service (IaaS) or software-as-a-service (SaaS) model.Microsoft aims to manage the health of the user or subject by monitoring and tracking the health condition orbody activity via body sensor network leveraging cloud computing. Dossia is a Personal health record serviceoffered by some of the largest employers in the United States. In case of physiological value based security, used electrocardiogram (ECG) data to generate cryptographic keys using discrete wavelet transform(DWT) for feature extraction. The scheme functions by physicallyshaking the communicating devices. In a cluster-based secure key-agreement protocol for WBANs ispresented, considering the network as a heterogeneous sensor network consisting of a powerful high-end sensor (Hsensor)node and several low-end sensor (L-sensor) nodes.PVs are used as a means for security in WBANs.The above-mentioned health monitoring systems are either fixed infrastructure systems or lack the ubiquitousnature of communication with no plug-n-play capabilities. The physiological value-based key agreement schemesdiscussed above are based on a single biometric value and hence lack sufficient randomness and key length. Thework presented in this paper provides a secure cloud-oriented platform – Cushy Data Network (Cu-DN), where the health of patients is monitored securely byusing sensors strapped on the human body, as well as concentrating on the secrecy and privacy of Electronic Medical Record (EMR) of patients. In this research the cloud castoff in the Cushy Network with a heavy coupled encryption and decryption system to ensure the confidentiality of patients' Electronic Medical Record (EMR).

## 3. Proposed System

The proposed system consists of sensors attached to a patient i.e. Body Sensors (BS), a client interface/data reader, Far-off base station (FBS), and a hospital open cloud as shown in Figure 1. The computational servers would be deployed using the hospital open cloud. The proposed tiered model has two modes: the indoor-patient mode and the outdoor-patient mode. In indoor–patient mode, the hospital provides connectivity to the hospital open cloud through their local servers, while in outdoor-patient mode the patient is connected to the hospital open cloud via FBS. In the indoor-patient mode, the patients are are kept under observation. The sensors capable of measuring human biological values are attached to their bodies to sense the BVsi.e. electrocardiogram (ECG) and electroencephalogram (EEG) values. Each patient has a personal server i.e. Body Server and is responsible for gathering data from sensors on the patient's body, and a client interface/data reader totransfer data from Body servers to the Open Cloud. In outdoor-patient mode, the patient is considered to be outside the observation and not located in the server's range.Thus, the patient must connect to a Far-off base station (FBS), which transfers the patient's data to thehospital community cloud. If the patient is not within the range of the FBS, Cumulative Transmission will happen with the help of neighboring Body Server which is called as inter-body communication that routes the Electronic Medical Record (EMR) from far patient to near patient of Far-off Base Station (FBS). Once the data is absorbed to the cloud, it will be stored in the EMR system of the hospital. This systemconsists of the hospital servers like main server, application server, and database server etc. An EnterpriseCloud (EC) with Eucalyptus database would be used to store data in buckets and objects. The received data (BVs) aresecurely stored in the Eucalyptus database using database schema redesign and cryptographic technique.

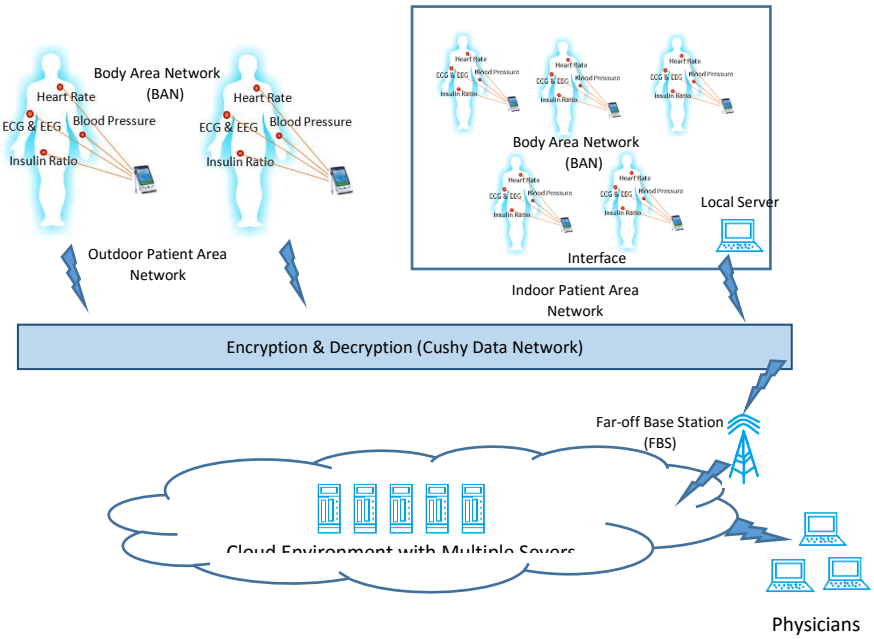



**Figure: 1 – System Architecture**

## 4. Cushy Data Network (Cu-DN)

The Network which is formed with a string Encryption and Decryption Scenario for the effective secure communication between the system and devices as shown in Figure 2.

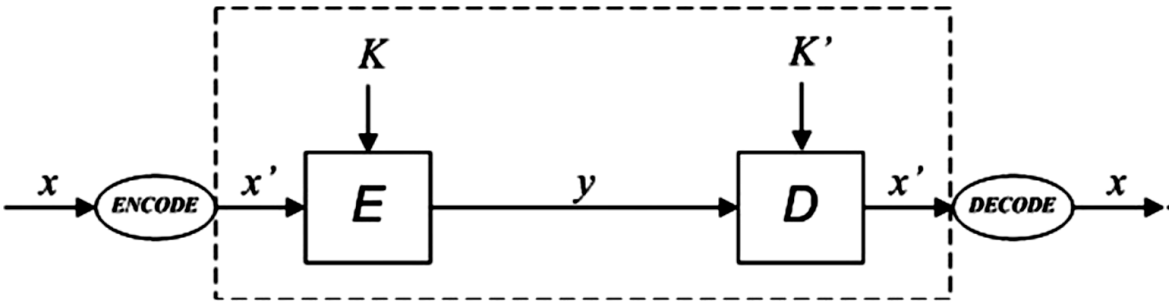



**Figure: 2 – Encryption and Decryption System**

Here the system has Multi-valued and Ambiguous Scheme (MAS) to overcome existing shortcomings in CloudabettedWBANs. In this scheme. It mainly deals with data confidentiality and provides a general paradigm for deploying applications in Cloud-abetted WBANs. The concepts behind cryptosystems and unambiguous languages are categorize in two way. The first, we give a new method to design cryptosystems as the standard approach to protectdata. In this, users are able to encode data with a secret key that can only be decoded by the intendedreceivers. The obtained cryptosystems possess interesting properties such as allow the use of unambiguous languages thatare generally not codes. Also, the cryptosystems contain a trapdoor which can be reduced to an undecidable problem. Thesecond, the scheme for data confidentiality that is suitable for use in Cloud-abetted WBANs.

The procedure ENCODE encodes a word u -> A*, u = $u_1u_2,\ldots,u_n$, $u_i$-> A, obtaining m-bit blocks of encoded words. Concretely,we use a while loop to scan the word u from left to right. Then, each m-bit block of the encoded words can be produced usingthe nested while loop. Indeed, the condition (count <= k) and ($|w_j|$< m) guarantees that the length of the word used to producethe block $w_j$ is less than or equal to k, and $w_j$ does not exceed m bits. Depending on the encoding situation, the PAD ($w_j$) iscalled to pad $w_j$ in order to gain the m-bit block. Next, the exclusive-or of two bitstrings is used to create masks on m-bitblocks constituting the output.

*procedure ENCODE (u)*
*i = 1, j = 10;*
*whilei<= n do*
*count = 1;*
*while (count <= k) and ($|w_j|$ < m)do*
*if$|w_je_g(u_i)|$<= m then*
*$w_j = w_je_g(u_i)$, count = count + 1, i = i + 1*
*else PAD ($w_j$);*
*if$|w_j|$ < m then PAD ($w_j$);*
*if j = = 1 then $w'_j = w_j$ XOR S else $w'_j = w_{j-1}$ XOR $w_j$;*
*j = j + 1;*
*returnw = $w'_1 w'_2$ ….. $w'_{j-1}$*

The DECODE procedure takes an encoded word w of q m-bit blocks as inputw = $w'_1 w'_2$ ….. $w'_q$, $|w'_j|$ =m, and produces theoriginal word u -> A*as output. At first, the m-bit secret key S is used to remove the masks of input blocks. Then, each block isdecoded separately. The EXTRACT ($w_j$, tmp) extracts words in X from $w_j$, then stores them in the array tmp. Then, the corresponding original words can be obtained from tmp using $d_g$.

*procedure DECODE(w)*

*i = 1, j = 1;*
*while j <= q do*
*if j = = 1 then* $w_j = w'_j$ *XOR S else* $w_j = w_{j-1}$ *XOR* $w'_j$;
*EXTRACT* ($w_j$, *tmp);*
*count = 1;*
*while (count <= length(tmp)) do*
$u_i = d_g(tmp[count])$, *count = count + 1, i = i + 1;*
*j = j + 1;*
*return* $u = u_1 u_2 \ldots u_{i-1}$

## 5. Conclusion

The paper offered a cloud abetted secure structure for far-off healthcare system that focuses on inter-sensorcommunication security as well as patients' data security and privacy with the presence of Cushy Data Network (Cu-DN). The proposed system uses multiple biometricsto generate a common key for inter-sensor communication with more accuracy and defensibility. The proposed framework will be evaluate in terms ofsecurity of inter-sensor communication and the results indicate that the proposed system is a viable solution for thenext generation far-off healthcare systems. The proposed framework is beneficial as it provides a complete cloud-abettedframework and security solution for a ubiquitous far-off healthcare monitoring System.

## References


[1] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 (2014) (2014) 371–386.
[2] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014) (2014)355–370.
[3] A. Wang, X. Zheng, Z. Wang, Power analysis attacks and countermeasures on intru-based wireless body area networks, KSII Trans. Internet Inform. Syst. 7 (5) (2013) 1094–1107.
[4] X. Zhang, Y. Xia, S. Luo, Energy-aware management in wireless body area network system, KSII Trans. Internet Inform. Syst. 7 (5) (2013) 949–966.
[5] S. Rezvani, S.A. Ghorashi, A novel wban mac protocol with improved energy consumption and data rate, KSII Trans. Internet Inform. Syst. 6 (9) (2012) 2302–2322.
[6] Y. Park, D. Kim, M. Jo, H.P. In, Content-centric wbans for bio medical service, in: Proceedings of the 3rd International Conference on Internet (ICONI),Korean Society for Internet Information (KSII), December 2011, pp. 155–158.
[7] S. Saleem, S. Ullah, K.S. Kwak, A study of ieee 802.15.4 security framework for wireless body area networks, Sensors 11 (2) (2011) 1383–1395.
[8] M. Li, W. Lou, K. Ren, Data security and privacy in wireless body area networks, IEEE Wireless Communication. 17 (1) (2010) 51–58.
[9] D. He, C. Chen, S. Chan, J. Bu, and P. Zhang, ―Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks‖, IEEE Journal of Biomedical and Health Informatics, vol. 17, no. 3, pp. 664-674, 2013.

[10] Ramesh Kumar; RajeswariMukesh; ―State Of The Art : Security In Wireless Body Area Networks‖International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 4 No. ,05 May 2013 ,pages 622-630, ISSN : 2229-3345
[11] J. Liu, Z. Zhang, X. Chen, K. S. Kwak, ―Certificateless Remote Anonymous Authentication Schemes for WirelessBody Area Networks‖, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 332-342, 2014.
[12] H. Xiong, ―Cost-Effective Scalable and Anonymous Certificateless Remote Authentication Protocol‖, IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2327-2339, 2014
[13] Mohammad H. Al Shayeji, AbdulRahman R. Al-Azmi, AbdulAziz R. Al-Azmiand M.D. Samrajesh, Analysis and Enhancements of Leader Elections algorithms in Mobile Ad Hoc Networks.
[14] Qi Dong, Donggang Liu, Resilient Cluster Leader Election for Wireless Sensor Networks.
[15] EiriniKarapistoli* and Anastasios A Economides, ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks.
[16] SuhasMathur, Chunxuan Ye, Rajat Mukherjee, Akbar Rahman And Yogendra Shah, Wade Trapee and Narayan Mandayam, Exploiting The Physical Layer for Enhanced Security. PP: 63 – 70, October 2010
[17] Rohan Nanda and P Venkata Krishna, Mitigating denial of service attacks in hierarchical wireless sensor networks. PP: 14 – 18, October 2011.
[18] Rajkumar, Sunitha K R, Dr.H.G.Chandrakanth, A Survey on Security Attacks in Wireless Sensor Network, International Journal of Engineering Research and Applications (IJERA), Vol.2, PP:1684-1691,2012.
[19] Safdar Ali Soomro, Sajjad Ahmed Soomro, Abdul GhafoorMemon, Abdul Baqi, Denial of Service Attacks in Wireless Ad hoc Networks, Journal of Information &CommunicationTechnology, Vol. 4, No. 2, 2010.