Topsis Method For Detecting a Heart Attack by WBAN

***SHANV MEHRA , ARSHDEEP SINGH, ARASHPREET SINGH**

* lmehra581@gmail.com

Corresponding email id arashpreetsingh30@gmail.com
arshdeepnur41@gmail.com

ELECTRICAL ENGINEERS, DIPS POLYTECHNIC COLLEGE TANDA

Under the Guidance of **ER SIMRANJIT KAUR** (HOD EE)

ABSTRACT: In today world many individuals are died from heart attack,Cancer etc. in this research paper we are going to detect the symptoms of heart attack with the help of WBAN technique which is known as wireless body area network it allows health care professionals to check asses and treat people without needing to be personally there biosensor that have been miniaturized have the advantage of being able to be implanted in on or off the bodies of dwellers and then they can relay physiologic data via wireless to cloud computers .In this research paper we conclude that which patient is suffering from heart attack or not by TOPSIS Method.TOPSIS (Technique for Order Preference by similarity to ideal solution) is MCDM Method (Multi Criteria Decision Making) that is used for findout best alternative.

• INTRODUCTION

A Wireless Body Area Network is a wireless network consisting of a collection of small bio-medical units positioned on the body's surface, beneath the epidermis, within the body, or in close enough proximity towards the body. WBAN is defined by IEEE 802.15.6 , which was published in 2012, is the only WBAN benchmark available. IEEE 802.15.6 is a secured, short-range connectivity system that supports a wide variety of data rates to meet the needs of a variety of purposes. The ultra-low-power detectors can check the body's key physiological signs and, sometimes in cases, can even administer a medication straight into the body. The scholars Toorani [16] examined the primary agreement processes for MK setup in the WBAN specification. He believes that four key-establishing mechanisms in the norm are vulnerable to Key Compromises and online frauds result in failure to meet the forward secrecy condition. Attacks are also possible using one of the methods. A pre-shared master key should be enabled or created. During the connection process, both the hub and every node should be secure connectionless communication, and a Pair-wise Temporal Key must bi created and exchanged between Both parties must be involved in each conversation. Alam et al. [18] describe a novel use of WBAN Wearable's for protection and critical applications in Oil and gas refineries, as well as the diverse petroleum industry, present challenging situations. Inter-WBAN Exchanges are depicted in this architecture, in which the WBAN supervisor functions as a versatile device that remotely connects body sensors to external network devices using wifi or broadband cellular networks like GSM, GPRS, 3G, and LTE. This work [19] provides a contrast between several WBAN techniques as well as new challenges. Also, with some case reports based on actual installations and experiments in the fields and computations, the paper will examine radio channel analysis, energy consumption reduction, and cohabitation challenges in WBAN.WBAN investigates cohabitation issues and approaches for disturbance reduction.

In [20], Venkatasubramanian et al. proposed a key agreement, fuzzy vault, and biometric-based privacy technique as part of the PSKA idea for WBAN. This feature enables neighboring WBAN sensors to securely agree on a symmetrical encryption key, minimizing the need for key information prior to deployment. PSKA, while powered by human energy, requires more processing time. This prevents attackers from leveraging critical details as no pre-deployment is necessary. PSKA prioritizes physiological parameters to ensure secure inter- sensor interactions. PSKA employs a fuzzy vault to lock and unlock.

Li et al. [21] propose a biometric-based access control solution that combines key production, distribution, and governance with a low-power cryptosystem. This identification technique generates keys using physiological signals, such as electrocardiogram data. Vital signs from a person's blood are securely recorded and transferred. This method encodes information packets using AES and DES.

During key synthesis and transmission, the IPI transmitter binary encoding is used to generate a secret key.

In their study [22], Ali and Khan present a secure key agreement approach for intersensor transmission using the Discrete Wavelet Transform. (DWT). This method use EKG data to generate encryption keys for inter-sensor interactions. During the interchange phase between sensors, iris or fingerprint attributes are employed to lock and release modules using watermarking. Once a watermark is sent to the transmitter, the block must be sealed before being released. The watermark is then deleted at the recipient's end. The most important steps in this strategy are feature generation and key agreement.

In their paper [23], AL-Rassan et al. proposed an ECG-based key management technique for wireless body area networks generates keys based on biological characteristics of humans. Using biochemical parameters and pre-Loading procedures to ensure WBANs' secure intersensor connectivity. Following the collection of ECGs. The key establishment phase is used to construct features based on physiological measurements keys. Prior to installing pre-distribution using the recommended ECG-based method, A key bank is used to load large key sizes into the sensor network, and each sensor is assigned its own key.

[26] Ali and Khan present a key management and consensus method that allows WBAN sensor nodes. To Establish a shared secret key with the private server. This solution protects WBANs by selectively forwarding, denial of service, and replaying threats by providing a response authentication mechanism acrossnodes. The proposed method generates a secure key based on the ECG signal. The values conveyed are a portion of the feature attributes are formed by the peak intensities of the individual's ECG signal. [27] is another likelihood-based TMS that uses the exponential probabilistic model .Describe a node's reputational value, assuming similar future behavior.

METHODOLOGY:-

Sr no	ATTRIBUTES	DESCRIPTION
1	NAME	User Name
2	DOB	User Date of Birth
3	MOB NO	PATIENT Mobile Number
4	Age (in years)	User age
5	Gender	Male/female
6	Email address	User Email id
7	ADDHAR NO	User Adhaar no

➢ METHODOLOGY

Algorithm:-Detecting and monitoring Heart Attack.

1. Firstly registration can be done in the system via mobile using some personal information including Name of the patient, Age, Date of Birth, Adhaar Card, Mobile number, address etc.

2. After the registration, enter the data which patient is suffering from symptoms like blood pressure, Diabetes, Cholesterol, obesity, sugar.

3. All information regarding health is collected by different bio sensors.

4. Then the data is collected gathered by doctor and categorized the data.

5. If the doctor detect that the patient is infected by the symptoms of heart attack then electronic record is sent to patient and provide urgent is sent to patient and provide urgent medications to the patient so that patient is safe from heart attack, avoid death rate and if the patient condition is critical health care use entry ambulance.

6. The system continuous check the patient until the user recover Case study:-

In this section, we will implement the TOPSIS Technique for helping specialist and consultant to detect and monitor which diseases that patient has chance infected by it then advising him in electronic health care four patient data from experts and classifies which patient is suffering from heart or not on the basis of symptoms like Blood pressure, Diabetes, Sugar, Cholesterol, Obesity and other symptoms like breathing issues Body pain, Chest pain.

- **Construct a decision matrix:**

Patients	**Blood Pressure**	**Diabetes**	**Sugar**	**Obesity**	**Cholesterol**
Patient 1	130	130	150	40	200
Patient 2	80	100	120	50	180
Patient 3	90	150	190	90	110
Patient 4	160	110	110	110	250

Patients	**Blood Pressure**	**Diabetes**	**Sugar**	**Obesity**	**Cholesterol**
Patient 1	0.544	0.425	0.514	0.363	0.521
Patient 2	0.335	0.327	0.411	0.454	0.469
Patient 3	0.377	0.49	0.651	0.818	0.268
Patient 4	0.67	0.686	0.377	1	0.652

- **Calculated the Wheightage normalized matrix:**

Patient	**Blood Pressure**	**Diabetes**	**Sugar**	**Obesity**	**Cholesterol**
Patient 1	0.1088	0.085	0.1028	0.0726	0.1042
Patient 2	0.067	0.0654	0.0822	0.0908	0.0938
Patient 3	0.0754	0.098	0.1302	0.1636	0.0572
Patient 4	0.134	0.1372	0.0754	0.2	0.1304

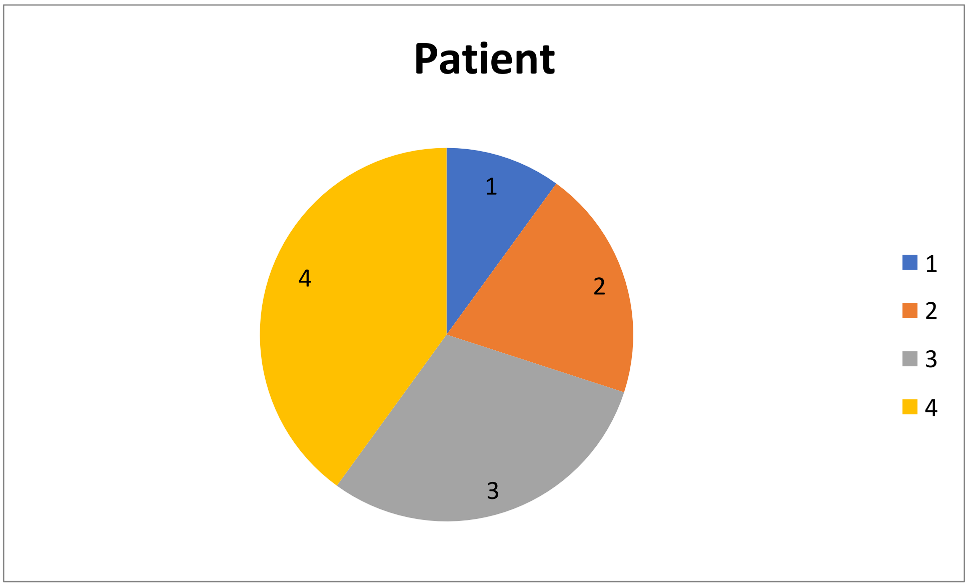
In this step we calculate ideal best or idea worst minimum value of ideal best or maximum value is ideal worst.

Patient	**Si+**	**Si-**	**Si++Si-**	**Pi**
Patient 1	0.144	0.334	0.478	0.301
Patient 2	0.68	0.32	1	0.68
Patient 3	0.072	0.089	0.161	0.477
Patient 4	0.15	0.51	0.66	0.227

Then rank the criteria based on performance score. By this we can identify which patient is suffering from health disease or not.

Patient	Pi	Rank
1	0.301	3
2	0.68	1
3	0.477	2
4	0.227	4

RESULT:- The patient 2 which has highest rank that patient has high chance of suffering from heart attack. The patient 2 which has lowest rank that patient is not suffers from heart attack.



Conclusion

In this paper we implemented TOPSIS method for detecting which patient is suffering from heart attack or not and we concluded that the patient two which has lowest rank that patient is not suffers from heart attack.

REFERENCE

[1] Wei, Fushan, et al. "A provably secure password-based anonymous authentication scheme for wireless body area networks." *Computers & Electrical Engineering* 65 (2018): 322-331.

[2] El Azhari, Maryam, et al. "Relay based thermal aware and mobility support routing protocol for wireless body sensor networks." *International Journal of Communication Networks and Information Security* 8.2 (2016): 64.

[3] Ibrahim, Maged Hamada, et al. "Secure anonymous mutual authentication for star two-tier wireless body area networks." *Computer methods and programs in biomedicine* 135 (2016): 37-50.

[4] Pathania, Shikha, and Naveen Bilandi. "Security issues in wireless body area network." *Int J Comput Sci*

Mobile Comput 3.4 (2014): 1171-8.

[5] Sinha, Sourav, Neeraj Kumar Goyal, and Rajib Mall. "Early prediction of reliability and availability of combined hardware-software systems based on functional failures." *Journal of Systems Architecture* 92 (2019): 23-38.

[6] Zou, Shihong, et al. "A survey on secure wireless body area networks." *Security and communication networks* 2017.1 (2017): 3721234.

[7] García-Valls, Marisol, Abhishek Dubey, and Vicent Botti. "Introducing the new paradigm of social dispersed computing: Applications, technologies and challenges." *Journal of Systems Architecture* 91 (2018): 83-102.

[8] Borkar, Gautam M., and Anjali R. Mahajan. "Security aware dual authentication-based routing scheme using fuzzy logic with secure data dissemination for mobile ad-hoc networks." *International Journal of Communication Networks and Distributed Systems* 21.2 (2018): 157-186.

[9] Kavitha, Y., M. Lavanya, and A. Mounika. "A secure IoT-based modern healthcare system using body sensor network." *International Journal of Innovative Research in Science, Engineering and Technology* 6.3 (2017): 156-160.

[10] Pattani, Kunal M., and Palak J. Chauhan. "Spin protocol for wireless sensor network." *International Journal of Advance Research in Engineering, Science & Technology* 2.5 (2015): 96-98.

[11] Thamilarasu, Geethapriya. "iDetect: an intelligent intrusion detection system for wireless body area networks." *International Journal of Security and Networks* 11.1-2 (2016): 82-93.

[12] Gupta, Megha. "Hybrid intrusion detection system: Technology and development." *International Journal of Computer Applications* 115.9 (2015): 5-8.

[13] Rai, Kajal, and M. Shyamala Devi. "Intrusion detection systems: A review." *Journal of Network and Information Security Volume* 1.2 (2013).

[14] Ghafir, Ibrahim, Martin Husak, and Vaclav Prenosil. "A survey on intrusion detection and prevention systems." *Proceedings of student conference Zvule, IEEE/UREL. Brno University of Technology*. Vol. 1014. 2014.

[15] Masdari, Mohammad, Safiyyeh Ahmadzadeh, and Moazam Bidaki. "Key management in wireless body area network: Challenges and issues." *Journal of Network and Computer Applications* 91 (2017): 36-51.

[16] Jin, Tan, and Wang Yijing. "The research of secure transport protocol based on node's clock characteristics for body area networks." *International Journal of Security and Its Applications* 8.5 (2014): 457-470.

[17] Lin, Chu-Hsing, and Yi-Yi Lai. "A fingerprint-based user authentication scheme for multimedia systems." *2004 IEEE International Conference on Multimedia and Expo (ICME)(IEEE Cat. No. 04TH8763)*. Vol. 2. IEEE, 2004.

[18] Zaghouani, Emna Kalai, Adel Benzina, and Rabah Attia. "ECG based authentication for e-healthcare systems: Towards a secured ECG features transmission." *2017 13th international wireless communications and mobile computing conference (IWCMC)*. IEEE, 2017.

[19] McCraty, Rollin, and Fred Shaffer. "Heart rate variability: new perspectives on physiological mechanisms, assessment of self-regulatory capacity, and health risk." *Global advances in health and medicine* 4.1 (2015): 46-61.

[20] Choudhary, Tilendra, and M. Sabarimalai Manikandan. "Robust photoplethysmographic (PPG) based biometric authentication for wireless body area networks and m-health applications." *2016 Twenty Second National Conference on Communication (NCC)*. IEEE, 2016.

[21] Anwar, Muhammad, et al. "Securing data communication in wireless body area networks using digital signatures." *Technical Journal* 23.02 (2018): 50-55.

[22] El Kandoussi, Asmaa, and Hanan Elbakkali. "Security based partner selection in inter-organizational workflow systems." *International Journal of Communication Networks and Information Security* 10.3 (2018): 462.

[23] Toorani, Mohsen. "Cryptanalysis of Two PAKE Protocols for Body Area Networks and Smart Environments." *Int. J. Netw. Secur.* 17.5 (2015): 629-636.

[24] Shanmugapriya, I., and K. Karthikeyan. "Reputation based incentive scheme for secured data privacy in Wireless Body Area Network Communication." *Adv. Comput. Sci. Technol* 10.7 (2017): 2095-2117.

[25] Kumar, P., and A. Sharma. "Survey on authentication process in body area network." *The International Journal of Electronics Engineering Research* 9.6 (2017): 913-921.

[26] Zhang, Jie, et al. "An improved protocol for the password authenticated association of IEEE 802.15. 6 standard that alleviates computational burden on the node." *Symmetry* 8.11 (2016): 131.

[27] Khan, Muhammad Khurram, and Saru Kumari. "An improved user authentication protocol for healthcare services via wireless medical sensor networks." *International Journal of Distributed Sensor Networks* 10.4 (2014): 347169.

[28] Nam, Junghyun, et al. "Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation." *Plos one* 10.4 (2015): e0116709.

[29] Shin, Seulgi, Sung Woon Lee, and Hyunsung Kim. "Authentication protocol for healthcare services over wireless body area networks." *International Journal of Computer and Communication Engineering* 5.1 (2016): 50.