JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

A Survey: Wireless Secure Health Monitoring System

Ayaat H. Qasem[1] , Abeer Salim Jamil[2], Abdul Monem S. Rahma[3]

[1]Department of Computer Science , Information Institute for Postgraduate studies, Iraq

Ms202020599@iips.icci.edu.iq

[2]Department of Computer Technology Engineering, Al-Mansour University College, Iraq

abeer.salim@muc.edu.iq

[3] Computer Science Department Al-Maarif University College, Iraq

monem.rahma@uoa.edu.iq

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10

Abstract:

Healthcare is an essential part of life, it can play a major role in improving the lives of patients, especially the most vulnerable in society, including the disabled, the elderly and the chronically ill. Many healthcare applications have been developed with the help of technology to improve people's lives. This paper includes a studying and evaluating the performance of papers that deal with systems that uses wireless mobile to monitor patients remotely depending on the use of new methods and techniques to monitor patients, which has many advantages by allowing the patient to carry out normal daily activities at home while the patient is still being monitored using wireless device technologies. This type of implementation can be used to reduce the costs of the health sector and increase the empowerment of people to prevent chronic diseases and manage appropriate health activities through patient monitoring; the performance of a group of available research has been studied and evaluated according to the main axes to highlight the most secure and fast performing algorithm.

Keywords: *-Wireless Secure, Wirelesshealth monitoring, wire health monitoring, patient monitoring ,health care monitoring .*

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

1. Introduction

A recent healthcare system should presents better healthcare services to people at any time anywhere in an affordable and patient friendly manner. Currently, the healthcare system is going to change from a traditional approach to a modernized patient centered approach. However, the patient health monitoring system in hospitals or polyclinics in general is still carried out in a conventional way[1]. The nurse or doctor comes to the patient room to check the patient's health progress. This will not be a problem for hospitals or polyclinics in urban areas with adequate numbers of nurses and doctors [2]. However, for hospitals or polyclinics in rural areas with small numbers of medical personnel and limited facilities, this is a problem, because nurses and doctors have to go the extra mile from one room to another in monitoring patient health[3]. If the number of patients is large and the number of medical personnel is inadequate, this monitoring process will take a lot of time and can endanger patients who need priority direct treatment from doctors and nurses[4]. In the traditional way the doctors play the major role. For needful diagnosis and advising they need to visit the patients. There are two basic problems related to this approach. Firstly, the healthcare professionals must be at place of the patient all the time and second, the patient remains admitted in the hospital, wired to bedside biomedical instruments, for a long period of time. In order to solve these two problems we can cutoff connection between the patients and devicess and send their data by one of the wireless technology . Therefore, encryption technologies have also been suggested to overcome the privacy and security problem [5]. There are four major types of encryptions in use nowadays. Each type has advantages and disadvantages: symmetric cipher, asymmetric cipher, key exchange algorithms, and hybrid cipher [6].

2. Literature Survey

Many researches, articles have been published which are related to the security of health monitoring system Table (1) illustrated the comparison between previous studies in terms of the technology used and its disadvantages.

- VinayagaSundaram et al (2015) suggested encryption and hashing algorithms, where used RC-5, Skipjack, and AES. The purposed to be achieved confidentiality assurance where attackers cannot interpret the encrypted-text that was sent, also ensure integrity (the encrypted-text has not been changed) by being used a hashing

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

algorithm. The algorithm is not vulnerable to brute force attacks due to its key length (128 bits), it does not have any weak keys. Confusion and diffusion are also achieved through this algorithm [7].

- **A. VithyaVijayalakshmiand Dr. L. Arockiam (2017)** suggested a multi-level encryption mechanism using Merkle-Hellman and Elliptic Curve Cryptography (ECC) which encrypts the data in two steps: the first step, the data is encrypted by the Merkle-Hellman cryptosystem. In the second step, the cipher text from the first step as an input to the ECC. Then sent the encrypted text generated from two algorithms to the cloud server to be stored there. The purposed to be achieved the security of the sensed data and did not enable unauthorized persons to access it, also improving the computation time [8].

- **Reem Jamal and others[2017]:**

designed a remote monitoring system for patients in An intensive care unit (ICU) , which can be used to read the medical signs such as (heart rate, temperature value and oxygen saturation percentage) from the patient's body beside checking the pacemaker device and send the values to the remote area. The proposed system deals with the patient vital signs as an input to send them to a computer in the nursing room by a transmitter-receiver system which composed of two Arduino kits connected with Bluetooth devices. The signal received by computer is processed and if there is an abnormal condition a message will be send to doctor mobile through Global System for Mobile Communications (GSM). The mechanism of the system is to send the medical signs to doctors in a remote area. The computer sends these values to doctor's mobile. Finally, visual basic language was used to implement the frame work of the system[9].

- **Shiva Prakash and Ashish Rajput (2018)** used a hybrid algorithm that included the advantage of the two algorithms: the symmetric key algorithm is AES (advanced encryption standard) and the asymmetric key algorithm is ECC (elliptic curve cryptography), in which ECC was used to generate and

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

share keys, and AES is to encrypt and decrypt data. The purposed to be achieved data integrity and confidentiality with minimal use of system resources thus providing data security as well as the proposed hybrid algorithm provides greater security than AES and consumes less resources and time than ECC [10].

- **Dian Rachmawati et al (2018**) useda hybrid cryptosystem method consisting of the symmetric algorithm is Tiny Encryption Algorithm (TEA) and the asymmetric algorithm is LUC, which is the file encrypt and decrypt by TEA and the encrypting and decrypting of the TEA key by LUC. The result of this method fulfilled the requirements of the integrity side in the encryption, where the encrypted text size was increased by sixteen bytes with an increase in the length of the plain text by eight characters. Also, this system can secure the file with many different extension [11].
- **Dian Rachmawati et al (2018)** used a hybrid cipher system is a combination between the algorithm of IDEA (International Data Encryption Algorithm) symmetry and the algorithm of knapsack asymmetry. The most prominent results achieved are: (1) It was found that the IDEA and Knapsack algorithms meet data integrity standards. The result of the message decoding test is that the encrypted text will be the same as the initial plain text (the original message). The result is that the decryption test of the encryption key will be the same as the key that was used to encrypt the messages[12].
- **Ahmed H. Mohammed and Mohamed MosaJafer (2019)** proposed an algorithm that relies on a lightweight encryption called (LWAES (lightweight Advanced Encryption Standard)). The goals to be achieved this system first: highest speed into encrypt and decrypt by replacing the mix columns stage found in AES with simple SHIFT operations because the mix columns stage is the most requested computational stage in AES design, and thus it consumes most of the time needed for encryption and decryption. This process took the time from the start of the sensor reading to the moment the user recalled it from 1 to 8 seconds. Second, the modified LWAES

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

algorithm provides Security was good to a WoT, with the encryption process was faster and lightweight in the storage process [13].

- **Poornima M. Chanal and Mahabaleshwar S. Kakkasageri (2019)** suggested the hybrid confidentiality algorithm that combines AES, ECC, and MD5 algorithms. Geo-encryption, also known as location-based encryption, is also used in integration with hybrid algorithms to ensure the confidentiality of all devices. The purpose of this suggested being achieved powerful confidentiality for data transmission for the IoT[14].

- **PavithraKanagaraj and ManivannanDoraipandian (2020)** proposed the hybrid cryptosystem, included the advantages of each (Advanced Encryption Standard (AES)) is a symmetric algorithm and (Rivest - Shamir - Adleman (RSA)) is an asymmetric algorithm to produce a hybrid algorithm. 4086 bits of paired keys are produced by RSA. In order to be provided better security for the system where it is difficult to attack, it is provided good key management, and it was also found that the calculation time that the program takes is less compared to the original algorithms [15].

- **Haider K. Hoomod et al (2020)** used the Speck-SHA3 (SSHA) algorithm resulting from a modification to the (Secure Hash Algorithm 3) SHA-3 by replacing the KECCAK function with another very fast algorithm Speck, which produces a very fast algorithm with a strong security level and is reliable in the validation of the data produced by the sensors. This algorithm achieved SSHA, the speed of this algorithm was much faster than the SHA-3 algorithm, with the ability to provide a good level of data security and integrity in a WoT environment compared to the level of security provided by the original SHA-3 algorithm[16].

- **Cecil C Nachiar and others (2020)**

collecte data from sensors are stored in Arduino memory and transmitted to smartphone through Wi-Fi module. They proposed system is used to process, analyse and display patient's

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

collected data with auto alarm. they proposed system has been very reliable with average delay of 14s and low power consumption with standing time of nearly 4 hr.[17]

- **HayderNajm et al (2021)** proposed an algorithm that consists of modifying the SHA-3(Secure Hash Algorithm 3) with Salsa20 algorithm is a stream cipher and high-speed for the purpose of producing the secure and high-speed algorithm in the validation process of the sensor data in WoT environment. In addition, this modifies also produces beginning values for the SHA-3 algorithm that was unknown and so unidentifiable by the prying. [18]

Table (1) The Comparison Between Previous StudiesNotes: A (Encryption Data), B (integrity Data) and C (Authentication Data)

S.no.	Title of Article	Security	Time	The Technique Used	A	B	C
1	[8]	Provides an acceptable level of security	Slow	ECC, MERKLE-HELLMAN	✓	✗	✓
2	[10]	Rather good security	Not provide sufficientspeed for encryption/decryption operations	AES,ECC	✓	✓	✗
3	[14]	Not very strong in E\D processes	It takes a medium time	AES, ECC, and MD5. Geo-encryption	✓	✓	✗

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

4	[5]	Acceptable level of security	Takes a longer encryption process	AES , RSA	✓	✗	✗
5	[7]	Good security	It takes a medium time	RC-5, SKIPJACK, AES	✓	✓	✗
6	[11]	Acceptable level of security	Slow	TEA,LUC	✓	✓	✗
7	[12]	Good security	Takes a longer time in the encryption process.	IDEA, KNAPSACK	✓	✓	✗
8	[13]	Security does not excellent	Slow	LWAES	✓	✗	✗
9	[16]	Very good security	Speed	SSHA	✓	✓	✗
10	[18]	Good security	It takes a medium time	SHA-3, Salsa20	✓	✓	✓
11	[17]	Acceptable level of security	speed	Arduino+smart phone	✗	✓	✓

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

12	[9]	Acceptable level of security	slow	Arduino+GSM	✗	✓	✓

3.Wireless Technologies Types

This section presents deceive Wi-Fi, Bluetooth, Li-Fi, and Zig-Bee wireless protocol that has IEEE802.15. 7 standards, 802.11 a/b/g standards, 802.15.4, and 802.15.1 while IEEE standards defended just MAC and physical layer.

a. Li-Fi

The Li-Fi represents IEEE802.15.7 Standard Light-Fidelity. It has been applied for Personal Area Wireless (PAN) networks. Data parallels are transmitted to the array of LEDs, which data rate speeds are 10 Gbps [19].

b. Wireless Fidelity (Wi-Fi)

Wi-Fi is considered as one of the major wireless networks following the IEEE standard 802.11n/a/b/g for WLANs. Users are enabled for browsing the Internet and connecting the cloud at broadband speeds (offered via network vendor) [20, [21].

c. **Bluetooth**

Bluetooth is developed for replacing cables about PC peripherals with low-cost and short-range devices. It is operating in a frequency band of 2.4GHz, and a maximum capacity of 720 Kbps might be shared via devices within 10 meters of each other. Its disadvantage is that maximum of 8 devices communicating on a single network [22, 23].

d. ZigBee

The Zig-Bee transceivers operate on unlicensed scientific, industrial, as well as Industrial, Scientific, Medical (ISM) radio spectrums. 16 channels, every one of which supports 250 data rates, were assigned at 2.4GHz [24, 25].

Table (2) is summarizing the 4 wireless protocol types, each one of the protocols is deriving the standards of IEEE, security, costs, normal range, frequency bandwidth, data transmission speed, network topology, power consumptions, and year of manufacture.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

TABLE (2) RELATION OF THE LI-FI, BLUETOOTH, ZIGBEE, WI-FI, WITH A PROTOCOL WIRELESS [19]

		Technolog Wireless			
Sequence of numbers	**Parameters**	**Li-Fi**	**Wi-Fi**	**Bluetooth**	**ZigBee**
I.	Standard IEEE	802.15.7	802.11 a/b/g	802.15.1	802.15.4
II.	Mode of Operation	Utilizing light waves	Utilizing radio waves	Utilizing short-wavelength UHF radio waves	Utilizing radio waves
III.	Speed Transfer Data	1 G bps	150Mbps	25Mbps	250 k bit/s
IV.	Frequency Bandwidth	10000GHZ	2.40GHz, 4.90 GHz and 5.0GHz	2.4 – 2.485 GHz	2.4GHz
V.	Network Topology	Point to point	Point to point	Piconet	Start
VI.	Range	10m	10-100 m	10 m, 100 m, Based on classes	10 -100m
VII.	Power Consumption	Low	Medium	High	High
VIII.	Cost	Low	High	High	High
IX.	Year	2001	1990	1998	1998
X.	Security	Highly	Less	Not	Less

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

4.Analysis and Recommendation

Content protection for wireless health monitoring is a very important topic, and the best way to protect is using security concepts.Therefore, there are three concepts that are used to data securityin healthcare monitoring system, which are Encryption Data and integrity Data and Authentication Data, where after a presentation of a group of techniques used for security, the results were as follows: The most important criteria used in security are speed and the three above concept which are illustrate in table (1), When fully secure algorithm the system, it will take more time compared to light weight algorithm security , which takes less time . This means that lightweight algorithms is faster than fully secure algorithms on the one hand speed. while, In terms of security, fully security algorithm is more secure becauseit is more complex, as in lightweightalgorithm. So, choice of any type of algorithms depends on type and need of the device used. That is, if there is a need to use it in real time or offline. As for the algorithms, some of them use high of security but slow algorithms and others, and some use lightweight algorithms, that are faster but less secure. Therefore, it is possible to use the method of hybridization between algorithms to make them more robust, high security, and be fast at the same time. This applies to lightweight algorithms that can be made more robust by strengthening them with other algorithms.

5.Conclusion

This paper presents a literaturesurvey in wireless health care monitoring techniques for contents security. Although, an essential and various types of health care systems techniques have been proposed in this study, most of the techniques are vulnerable to secure system.some of them provide more security for the system, but are computationally expensive and cannot be applied in real-time because they are slow. While others based algorithms are fast, but not provide a significant degree of system security., so we suggest hybridization between algorithms. for the purpose of avoiding disadvantages and benefits of the advantages of each algorithm, in order to build a fast and robust algorithm that can be implemented in real-time.

6. References

[1] P. A. Pawar, “Heart rate monitoring system using IR base sensor &Arduino Uno,” Proc. 2014 Conf. IT Business, Ind. Gov. An Int. Conf. by CSI Big Data, CSIBIG 2014, pp. 1–3, 2014, doi: 10.1109/CSIBIG.2014.7057005.

[2] M. AsaduzzamanMiah, M. H. Kabir, M. SiddiqurRahmanTanveer, and M. A. H. Akhand, "Continuous heart rate and body temperature monitoring system using Arduino UNO and Android device," 2nd Int. Conf. Electr. Inf. Commun. Technol. EICT 2015, no.Eict, pp. 183–188, 2016, doi: 10.1109/EICT.2015.7391943.

[3] P. W. Digarse and S. L. Patil, "Arduino UNO and GSM based wireless health monitoring system for patients," Proc. 2017 Int. Conf. Intell.Comput. Control Syst. ICICCS 2017, vol. 2018- January, pp. 583–588, 2017, doi: 10.1109/ICCONS.2017.8250529.

[4] S. K. Pahuja and N. Sethy, "Real time measurement of heart rate and it's variability," 2017 Innov. Power Adv. Comput. Technol. i-PACT 2017, vol. 2017-January, pp. 1–6, 2017, doi: 10.1109/IPACT.2017.8244990.

[5] A. B. And J.-M. B. Saad El Jaouhari, "Security Issues Of The Web Of Thing." 2017.

[6] S. K. Ghosh, S. Rana, A. Pansari, J. Hazra, And S. Biswas, "Hybrid Cryptography Algorithm For Secure And Low Cost Communication," *2020 International Conference On Computer Science, Engineering And Applications, Iccsea 2020*. 2020, Doi: 10.1109/Iccsea49143.2020.9132862.

[7] B. Vinayaga Sundaram, M. Ramnath, M. Prasanth, And J. Varsha Sundaram, "Encryption And Hash Based Security In Internet Of Things," *2015 3rd International Conference On Signal Processing, Communication And Networking, Icscn 2015*. 2015, Doi: 10.1109/Icscn.2015.7219926.

[8] D. L. A. A.Vithya Vijayalakshmi, "Enhancing The Security Of Iot Data Using Multilevel Encryption," *International Journal Of Advanced Research In Computer Science*, Vol. 8, No. 9. Pp. 841–845, 2017, Doi: 10.26483/Ijarcs.V8i9.4959.

[9] Reem Jamal Abbas Rawaa Abdel RidhakadhimSirajQays Mahdi," Design and Implementation of Patient Monitoring System for Medical Sign using GSM and Microcontroller,IEEE,2017.

[10] S. Prakash And A. Rajput, "Hybrid Cryptography For Secure Data Communication In Wireless Sensor Networks," *Advances In Intelligent Systems And Computing*, Vol. 696. Pp. 589–599, 2018, Doi: 10.1007/978-981-10-7386-1_50.

[11] And M. A. B. Dian Rachmawati , Amer Sharif , Jaysilen, "Hybrid Cryptosystem Using Tiny Encryption Algorithm And Luc Algorithm." 2018.

[12] D. Rachmawati, M. S. Lydia, And W. A. Siregar, "Hybrid Cryptosystem Implementation Using

Idea And Knapsack Algorithm For Message Security," *Journal Of Physics: Conference Series*, Vol. 1090, No. 1. 2018, Doi: 10.1088/1742-6596/1090/1/012030.

[13] A. H. Mohammed And M. M. Jafer, "Secure Web Of Things Based On A Lightweight Algorithm," *1st International Scientific Conference Of Computer And Applied Sciences, Cas 2019*. Pp. 216–221, 2019, Doi: 10.1109/Cas47993.2019.9075831.

[14] M. S. K. Poornima M. Chanal, "Hybrid Algorithm For Data Confidentiality In Internet Of Things." 2019.

[15] P. Kanagaraj And M. Doraipandian, "Design And Implementation Of Hybrid Cryptographic Algorithm For The Improved Security," *Lecture Notes In Electrical Engineering*, Vol. 672. Pp. 397–405, 2020, Doi: 10.1007/978-981-15-5558-9_36.

[16] I. S. A. Haider K. Hoomod, Jolan Rokan Naif, "Modify Speck-Sha3 (Ssha) For Data Integrity In Wot Networking Based On 4-D Chaotic System." 2020.

[17] Cecil C Nachiar; N. Ambika; R. Moulika; R. Poovendran," Design of Cost-effective Wearable Sensors with integrated Health Monitoring System",IEEE,2020.

[18] H. K. H. Hayder Najm , Rehab Hassan, "Data Authentication For Web Of Things (Wot) By Using Modified Secure Hash Algorithm-3 (Sha-3) And Salsa20 Algorithm." 2021.

[19] M. R. Mallick, "A comparative study of wireless protocols with Li-Fi technology: A survey," in Proceedings of 43rd IRF International Conference, 2016.

[20] G. A. Naidu and J. Kumar, "Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi," in Innovations in Electronics and Communication Engineering, Springer, 2019.

[21] Z. N. Abdul Khaleq; CROOCK, MuayadSadik; TARESH, Ali Abdul Razzaq.Indoor Localization System Using Wi-Fi Technology.IRAQI JOURNAL OF COMPUTERS, COMMUNICATION, CONTROL & SYSTEMS ENGINEERING, 2019.

[22] M. S. Balan, S. Musale, R. Saptarshi, P. Sawant, S. Somwanshi, and P. Zadge, "Comparative Study and Performance Evolution of Wireless Data Transmission Techniques for an Integrated Bathymetry Survey for Reservoir," Int. J. Comput. Appl, 2015.

[23] A. J. SALIM, et al. A polygonal open-loop resonator compact bandpass filter for Bluetooth and WLAN applications. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2018.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3685-3697
https://publishoa.com
ISSN: 1309-3452

[24] P. Aruna and N. Vetrivelan, “Survey and Comparative Study of Wireless Technologies for Enchanced MANET,” Int. J. Appl. Eng. Res, 2015.

[25] K. Ekhlas; HAITHAM, Russul.Performance Analysis of IEEE 802.15. 4 Transceiver System under Adaptive White Gaussian Channel. International Journal of Electrical & Computer Engineering (2088-8708), 2018.