International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Offline-First Sleep Assessment (OFFSA): Internet of Things Polysomnography Sleep Assessment Framework for Sleep Monitoring in Rural Environment

Novi Azman, Sandy Rachmat Wicaksono, Ernawati Sinaga

Abstract**:** ***Sleep is a mandatory biological requirement for humans that require appropriate proportions and quality. The assessment method in determining the best sleep quality and the medical gold standard is to use a Polysomnography device. The advantages of the Internet of Things can significantly increase the usefulness of Polysomnography in suburban areas. The target location of this framework makes our consideration adhere to the Offline-First Internet of Things method to overcome the limitations of the internet at that location. Unfortunately, there are still problems coming from the concept of the Internet of Things itself, and the problem is in data security. So we propose a framework for Polysomnography devices that connects the Internet of Things with a focus on the security and confidentiality of patient data called Offline-First Sleep Assessment (OFFSA). We enumerate patient medical data and archive encryption to improve patient data security. The confidentiality of our patient data is achieved by encryption on every medical data exchange and is only open on the Graphic User Interface application on the device that has been registered.***

Keywords**: Framework, Internet of Things, Polysomnography, Sleep Assessment**

I. INTRODUCTION

Sleep is one of the mandatory requirements needed by humans. The quality of sleep is very influential on human health. Poor sleep quality can lead to sleep disorders that will have an impact on everyday life. Patients with sleep disorders tend to be prone to suffer from chronic diseases such as obesity, diabetes, and hypertension. In several studies, it was found that there were several relationships between sleep quality and the risk of diseases such as diabetes and obesity [1], obstructive sleep apnea sleep disorders were a risk factor for systemic hypertension [2].

Manuscript published on November 30, 2019.
* Correspondence Author
Novi Azman, Electrical Engineering, Universitas Nasional, South Jakarta, Indonesia. Email: novi.azman@civitas.unas.ac.id
Sandy Rachmat Wicaksono, Engineering Physics, Universitas Nasional, South Jakarta, Indonesia. Email: contact@research.sandyrw.com
Ernawati Sinaga*, Biology, Universitas Nasional, South Jakarta, Indonesia. Email: ernawatisinagaj@unas.ac.id

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

There are several methods for monitoring sleep to determine sleep quality, such as using Polysomnography [3], Photoplethysmography [4], Ballistocardiogram [5], and Actigraphy [6]. However, of the many methods that can be done to assess sleep quality and to know sleep disorders, the method of monitoring with Polysomnography devices is still the primary choice for evaluating sleep in clinical use as in the diagnosis of insomnia [7]. This is because Polysomnography devices can provide more detailed information for sleep monitoring and offer more accurate sleep assessment results [8].

Developments in Internet communication bring a significant change. Internet of Things, where different objects can communicate with each other and exchange information with one another to improve the functionality and performance which is currently invisible already embedded in our environment [9], [10]. The extensive use of the Internet of Things, including its use in the healthcare industry sector. Monitoring patients' health by using biological sensors in the body, the Internet of Things allows patients to be in different locations such as at home, office, public place or in a vehicle. Medical sensors stay connected and send information to the medical party [11]. With the development progress in Information and Communication Technology, medical sensors provide a solution for many medical applications such as monitoring patient activity remotely, diagnosing chronic diseases, and for elderly health care [12].

However, the Internet of Things in the Health Industry remains in its early stages about design, development, and distribution. However, healthcare that utilizes the Internet of Things displays an extraordinary impact has a growing market in the healthcare industry, which will be one of the future health monitoring solutions. The Internet of Things solution has the potential to be able to save around fifty thousand people every year in the United States by avoiding deaths that can be prevented due to hospital errors. This is because it can provide patient safety by coordinating critical patient information and synchronizing resources such as health workers, devices that are used to extract vital data in real-time and instantaneously through the interconnection of devices and sensors. Other studies also reveal that the Internet of Things in the healthcare industry can facilitate better care by reducing costs, reducing direct interactions between patients and health workers, and access everywhere to get quality care [13].

Emerging problems in the use of the Internet of Things in healthcare are due to the development of the Internet of Things itself. There are several issues that we will raise in this paper, and we will submit a proposed framework to answer those problems. The hope is that this framework can become one of the standards or can be another standard reinforcement to produce a better framework for all stakeholders. It is also a gold-standard framework for healthcare Internet of Things in sleep monitoring cases using the Internet of Things-based Polysomnography devices.

Patient privacy is one of the most critical problems in the health industry. This privacy problem is either direct care or medical data sent online. Health data security and patient confidentiality are critical issues in online data exchange, which will have a substantial impact on the success and reliability of all parties in the utilization of the Internet of Things in the healthcare industry [14].

This confidentiality protection has increased to be more difficult than direct maintenance compared to online maintenance because one of them is when sending data from the device to the server which can happen things such as interception, interruption, modification, and fabrication by other parties [15]. These problems can have an impact on patient privacy, the confidentiality of data transmission, integrity in receiving data, and data availability.

Authentication is also an essential aspect in terms of creating trust in the system [16]. Other problems regarding access rights to medical data also need to be considered so that the data can only be accessed with specific access rights for those who do have access to the data. Another important thing is how we can ensure that the data is the right patient data, from the right medical device to the right server, and the integrity of data reception.

The contribution of the paper we wrote is to propose a new framework that will be used specifically for monitoring and evaluating sleep disorders that use Polysomnography devices by involving the Internet of Things which focuses on the security and confidentiality of patient data by considering the Offline-First Internet of Things concept.

The rest of the discussion in this paper are as follows. Part II will discuss studies or work from other researchers who have involved the Internet of Things for healthcare and study of the assessment of sleep disorders. This second part will be our foundation to propose this new framework. Part III we will explain the framework we propose. Finally, Part IV is the conclusion of our paper.

II. RELATED WORKS

The existence of the Internet of Things as a technological innovation that connects a collection of sensors and devices to collect, record, transmit, and share data to carry out possible analyzes has been used in a broad field of application [16]–[25]. In recent years, the Internet of Things technology has been used in the healthcare industry because of the development of simplified standard protocols between wired and wireless medical devices [26]. Some have become potential applications in monitoring healthcare where patient data will be collected from several sensors, analyzed, and delivered through a network and distributed to several parties who need it such as doctors, medical personnel who are suitable for patient care, and also for patients and family if needed [13].

One of the more specific uses is the use of the Internet of Things for Electrocardiography devices that have been carried out by several studies [20], [22]. R. Shaikh et al. performed monitoring of Electrocardiography, body temperature, and patient's heart rate in real time using an ARM processor [27]. Mohammed et al. designed an Android application for Electrocardiography monitoring and analysis data using web services and cloud computing, where the data can be further analyzed using third-party software if needed. It also encourages the use of the Internet of Things in the healthcare industry, where biomedical device manufacturers release APIs needed to interact with their products and allow use for further adjustments [28].

Another study says that for an Internet of Things-based Electrocardiography system, it consists of three main parts. First, the Electrocardiography sensor network. The second Internet of Things Cloud Server. And last part, a graphical user interface [29]. Sensor networks Electrocardiography is responsible for producing recordings of cardiac activity from patients and transmitting data that has been generated to the Internet of Things Cloud Server. Then the Internet of Things Cloud Server mainly has the task of storing and analyzing data. For example, specifically used to detect sleep disorders as in several studies that have been done [30]–[34], whereas the last part of the graphical user interface module is commonly used for visualization and data management. This can make the foundation of the parts needed to create a framework of the problems that we raised in this paper to build a sensor network framework for Polysomnography.

Zhang et al. [17] introduced a mobile healthcare network architecture, which focuses on the security of safe data collection and transmission. The security of data collection is obtained by applying secret keys and private keys. Whereas to obtain secure data transmission is enhanced by combining encryption on specific attributes where only predetermined users can access the data. This is implemented because there have been many exchanging and transmitting data in the healthcare Internet of Things network that can be penetrated by third parties or parties that are not part of the party that should have access or data in terms of maintaining the confidentiality of patient data.

Security and data confidentiality are critical topics. For example, in a heart monitoring system that uses the Internet of Things [35], since recording by Electrocardiography devices which are then stored in the Cloud, there may be some security threat such as improperly linked access and unauthorized access [36]. In several other studies, mechanisms have been used, such as anonymity [37], [38] and access control [31], [39]–[43] to ensure the security and confidentiality of recording Electrocardiography devices.

Another study that uses biometrics and radio fingerprinting [11], where it is done to ensure that the data reaches the right patient, the data is taken from the right device, sent to the right destination.

This is an important discussion because, with the many devices that are interconnected on the internet, we do not know that the data is monitored when the entire system does have the right patient. Moreover, how to maintain the integrity of the data obtained, such as about the issue of security challenges in transmitting patient data to a remote medical server can open security threats such as interception, interruption, modification, and fabrication. The threat will have an impact on patient confidentiality, trust in data transmission, and integrity of data reception. Then the use of a user grouping is needed to ensure that the data can be seen with limited access depending on the level of access needed. Anonymity and a secure and encrypted network in sending data with authentication in the form of keys or in the form of identifying different signatures so as not to exchange incorrect data.

In the case of sleep monitoring assessment, as is well known that the main sleep study is using a Polysomnography device to diagnose the patient's sleep quality. This is because the use of Polysomnography is the gold standard in evaluating sleep quality. Polysomnography records biophysiological changes that occur during sleep [3]. However, there are several approaches to monitoring sleep assessment other than using Polysomnography and other devices that use the Internet of Things as in the study of Lin et. al. The study used Doppler radar sensors, automatic radar demodulation modules, and a framework recognition of sleep status with 95.1% accuracy in determining sleep status called SleepSense [8]. Rofouei et al. present non-invasive wearable neck-cuff systems for sleep monitoring [44]. Another study using a lightweight system was made using microphones and accelerometers found on smartphones to determine sleep profiles [45]. Other frameworks, such as LullaBy to capture and monitor sleep environments using microphones, light sensors, and motion sensors [46]. Also, some are commercial off-the-shelf (COTS) based on actigraphy products such as Fitbit and Sleep Tracker, which are generally available. In this paper, we propose a framework that uses Polysomnography tools to assess sleep quality that involves the benefits of the Internet of Things. Aim to be able to maximize the use of the device and reduce the limited access of patients far from health facilities to assess sleep quality by focusing on the confidentiality and security of patient data.

III. PROPOSED FRAMEWORK

The framework we submitted, Offline-First Sleep Assessment (OFFSA) consists of four main sections to maximize the use of Polysomnography combined with utilizing the Internet of Things. This framework is expected to improve access to health in assessing the quality of sleep for areas far from the sleep laboratory and expert doctors. The four parts of the framework we submitted have the following sections. The first part is the sensor network system. Second, the Middleware section. The third part is the Cloud Server section. Last, the fourth part is the Graphic User Interface. The overall communication between parts of this framework uses internet networks in data exchange. Except communication in the sensor network system section with the Middleware section using a Bluetooth network which will be explained in more detail later.

OFFSA framework architecture design was created to improve the mobility of Polysomnography devices by using internet networks in data exchange transactions. Then the device that evaluates sleep can be moved according to the location needed. This will also be able to cut the cost of procuring equipment or the presence of a specialist doctor because the device can be anywhere without the need for a specialist to visit the patient. Except for patient interview sessions, although this session can also be done online too.

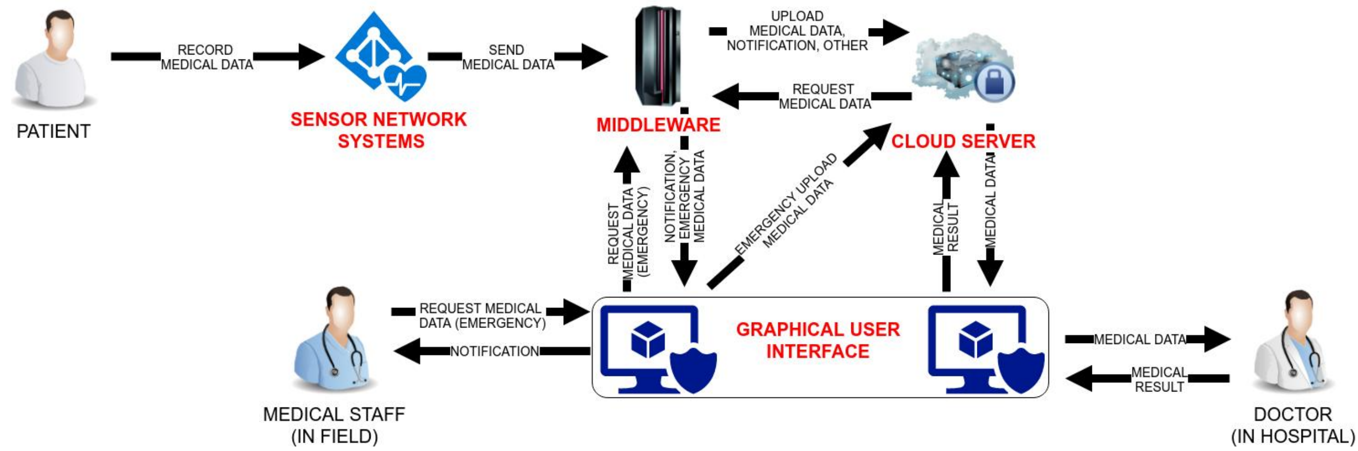

Fig. 1 Oveview of OFFSA Framework

The Offline-First concept that we proposed is due to considering the limitations of internet access in suburban locations or those far from big cities. Therefore, this concept will be a solution for certain regions by storing medical data in advance if there is no connection to the internet network.

The results of recording vital data as well as evaluating the quality of the patient's sleep can later be seen by related parties through a specific web service included in the Graphical User Interface section. The details of the OFFSA framework structure that we submitted are shown in Fig. 1, and we will describe the details of each part of the framework as follows.

A. Parts of the Sensor Network System

The sensor network system part is the part that interacts with the patient's body.

The sensor network system consists of several sensors needed to meet the needs of a Polysomnography device. Responsible for getting vital patient data needed. The sensors contained in this section meet the needs of a Polysomnography device. An electrocardiogram to record heart activity data when the patient starts to sleep, while sleeping, and wake up. The electroencephalogram records the brain activity of the patient to determine the sleep stage of the patient. Electromyogram records the movements of patients in sleep to get a sleep profile. Electrooculogram to record the activity of eye movements of patients while sleeping. Also, related sensors used later as respiratory effort. If it is indeed needed, other sensors can be added such as pulse oximetry to measure SpO2 in the blood and also heartbeat, and Blood Pressure to see and record changes in blood pressure when the patient starts, falls asleep and wakes up. It can also be a room camera to record patient movements while sleeping. Alternatively, other sensors needed on sensor network systems. In the sensor network system section, the data received is raw data from the device that is sent on a Bluetooth network with a defined API and given a signature on the medical device. It is hoped that the addition of the signature will not overlap the data during the reception in the Middleware section.

B. Middleware Section

The Middleware section is part of the task of collecting and temporarily storing medical data obtained from parts of the sensor network system. The whole process can be visualized shows in Fig. 2. Medical data is recorded and collected during a sleep monitoring session before being sent to Cloud Server. This section does not automatically become a transit point for data, but in this section checks the suitability of the device's signature. After the signature data is matched, then the data received from the medical device on the sensor network part of the system is given a patient signature so that it will not be confused later on the Cloud Server.

Furthermore, because medical data from the recording results in one session is large size, in the Middleware section, it also breaks down smaller files so that there is no failure to send data at once. This is a consideration because the OFFSA framework has the goal of using its devices to be placed in suburban areas or far from big cities with limited internet network conditions.

Then checksum the medical data file using methods like BLAKE2, MD5, SHA-1, CRC32, or other methods that are done before and after file splitting. Checking file checksums is done to maintain the integrity of medical data sent that the data is genuine and error-free.

After the medical data file that has been enumerated becomes a smaller size file and has received a file checksum. The medical data file is then entered into an archive format such as .tar.gz and is encrypted by giving a random password to the archive. Then as has been done before, after this stage the fragments of the medical data file are carried out to check the checksum of the file which will be used to maintain the authenticity of the medical data being sent. The entire file checksum data and archive password will be entered into the JSON file separately. Medical data files that have been enumerated and encrypted as well as JSON files that contain checksums of medical data files and archive passwords will be sent to Cloud Server in parallel alternately. File sending is carried out in the Secure File Transfer Protocol (SFTP), while JSON files are sent through Secure Socket Layer with REST API endpoints by authentication with API keys and authorization, as well as protection in session states to maintain the security of data entering the Cloud Server.

The whole process is done automatically by utilizing Cron jobs on the Middleware device, but it is still necessary to choose from a manual override just in case.

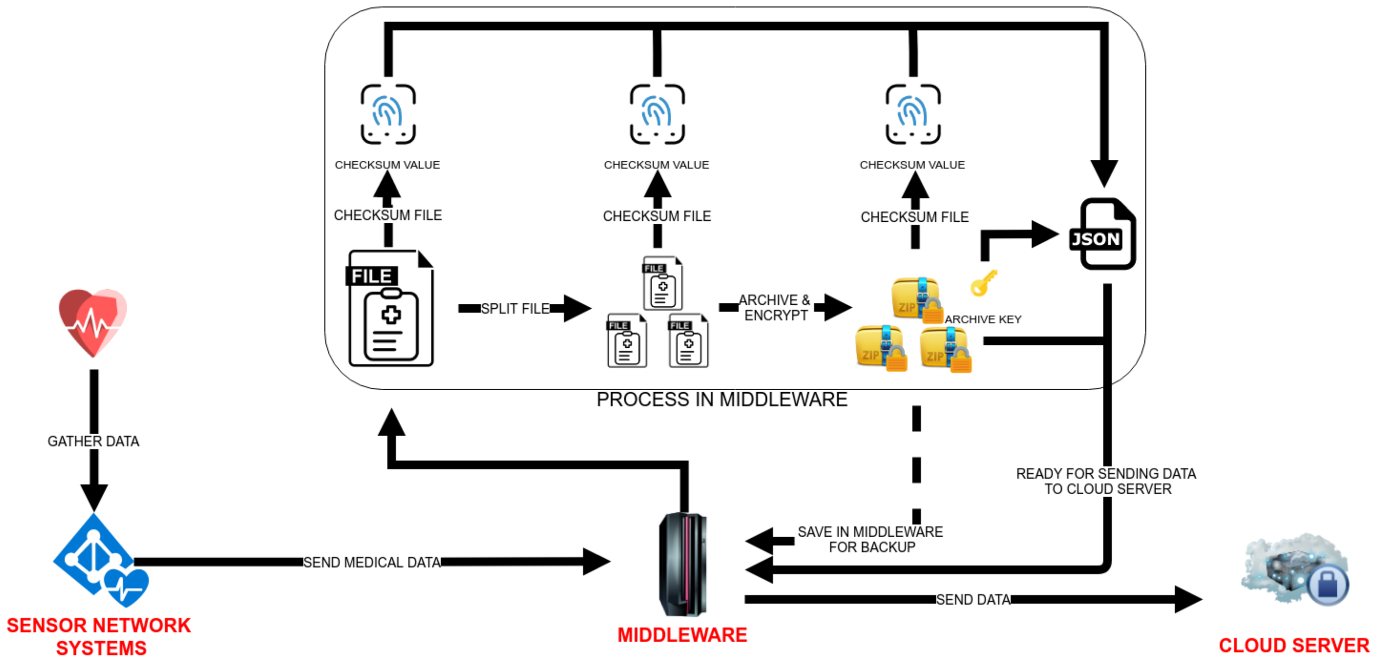

Fig. 2 Medical data processing in Middleware

The selection of Middleware devices can be done by meeting the following criteria, having Bluetooth and internet connectivity, then having the ability to do the things mentioned above. So we propose in the Middleware section of this framework to use mini or microcomputer devices such as Raspberry Pi or Intel Galileo devices.

As a precaution for some things that might occur, such as the connection between Middleware and Cloud Server devices or an error in uploading data. Then the concept of this framework is to prioritize if there is a condition that the device cannot connect to the Cloud server with the Offline-First concept. Medical data of patients who have been encrypted without a JSON file in this section will disappear automatically after seven days. We propose that if there are data that does not reach Cloud Server, health workers can upload data. Other cases such as the absence of an internet connection at all, the data will remain in the Middleware device until it is manually removed. The overall information is whether the Middleware device is connected to Cloud Server or there is data not sent, and there is data that does not correspond to the checklist and requires re-uploading, and other. The status appears in the application's Graphical User Interface section.

C. Cloud Server Section

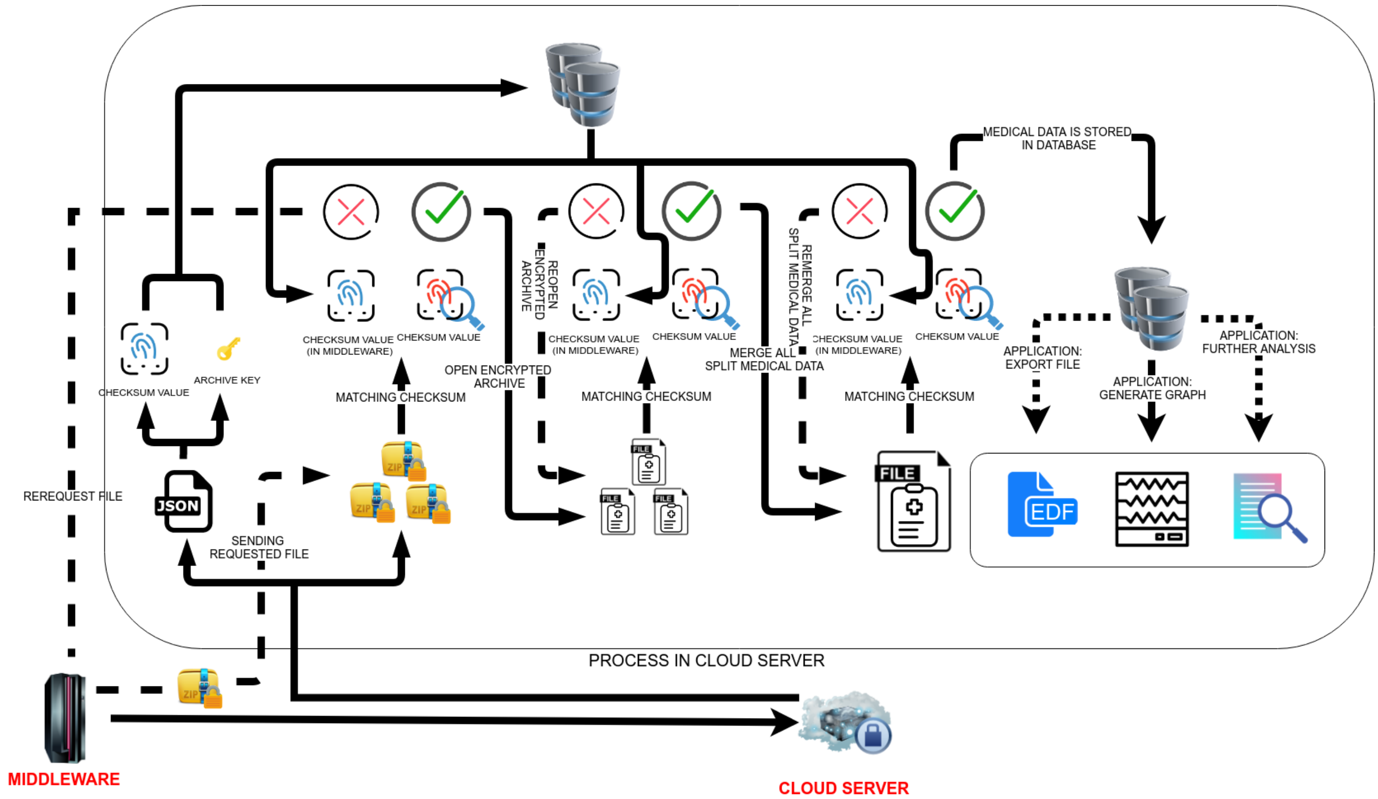

Fig. 3 Data validation process from split medical data into database and some application of processed data

This section does the most work from the entire OFFSA framework. In this section, medical data is sent by the Middleware device in the form of files that are enumerated and encrypted as well as JSON files. JSON data received by the REST API provided will be interpreted and entered into the column in the appropriate table in the database.

The split medical data file received will be done matching the checksum of the file between the checksums in the file with checksums that have been interpreted from JSON files from the database. If there is a difference in checksum, it can be ascertained that the file has different content, so the Cloud Server will notify the application of the Graphical User Interface so that the relevant party knows that there is a file that was defective at the time of upload. Cloud Serve also requests automatic sending of defective files to Middleware devices. If the upload fails several times again, then the request to the Middleware device will stop and give a notification to the relevant officer to do the upload manually.

The split medical data file that has passed the checksum matching will be removed from the archive by calling the archive password from the database. After that, the checksum value returns. At this stage, if the checksum does not match, what is done is opening the file again because the most significant possibility is that the extraction of the file failed.

After matching the checksum successfully, the next step is to combine the split file into complete medical data. After that, back to the last check file match, if there is a difference in the checksum value, the file merge will be repeated.

The next step after the medical data file has returned to its intact state, and the next step is to enter the patient's medical data database, one table per session per patient with a column corresponding to the data taken, for example, the vital heart data is inserted into the ECG column on the table. After medical data is stored on the Cloud Server, it can be used for further purposes.

One of the further uses of the patient's medical data is to make the visualization of the results of the data into data that can be used by the expert doctor to provide medical information. This visualization will appear in the Graphical User Interface section of the application contained in the framework. Making this visualization will always load data from the database; it will consume resources from Cloud Server. Therefore, we propose to always make it into an image or other files that do not require to load medical data from a database, such as creating a Scalable Vector Graphic file for each graph of the appropriate medical data. So generating a graphic image file that contains data from the database is only done once, the rest if related parties such as doctors only open the graphic image file. It is hoped that in making the graphic image can save the use of resources from Cloud Server. The next process can also be making files in other medical standards such as the European Data Format for other medical purposes. It can also be in the Cloud Server section, and there are data analysis and other processes that will help the medical and patient to increase speed in the process of evaluating sleep quality. In short, the Cloud Server functions to ensure integrity. In this section, it also shares the right to access patient data; for example, some stakeholders only receive data from Middleware devices by matching the checksum value. Then the Cloud Server also combines split files into one and then combines them again to be included in the database. Cloud Server also interacts with the Graphical User Interface section to provide notifications in the process that occurs. Furthermore, Cloud Server performs the next process, such as making visualization of the patient's medical data, generating other standard files such as European Data Format for other purposes, and it is possible to do other things such as data analysis and other actions.

D. Graphical User Interface Section

The Graphical User Interface Section is actually divided into access according to user clusters and access locations in the framework section. The Graphical User Interface on the Middleware device has a function that is to be able to see notifications about the status of processes that occur on Middleware devices. Still, in this section, the medical team can also upload medical data manually to the Cloud Server if the Middleware device cannot resolve an error. The last function in the Graphic User Interface on Middleware devices is to retrieve medical data that has been split and encrypted to allow manual uploads outside Middleware devices such as those on a medical party that has a Graphic User Interface application and the computer has a signature registered with Cloud Server. User Interface Graphics contained on computers or external devices outside the framework have one function, namely uploading medical data files to Cloud Server.

The other Graphic User Interface is located on a computer belonging to a specialist doctor, which has a function to access medical recording image data on Cloud Server. Another function is to make medical reports and to store and access the results of reading medical data in the Cloud Server and the internal computer of the doctor's work encrypted. The next function is to regenerate visualization from medical data, so expert doctors have the right to re-generate visualization from the data. Furthermore, the Graphic User Interface on the computer working by a specialist is exporting other used files as in the European Data Format format.

Patient medical data can only be accessed on applications included in this system framework with end to end encryption by paying attention to the device signature. The security is sought to prevent Man In The Middle attacks from occurring. Data exchange on the communication path is always encrypted and is only open in the Graphic User Interface application. The ability of tiered data access is needed so that parties other than experts can see the data to ensure patient confidentiality and security.

IV. CONCLUSION

Evaluating the quality of sleep using a Polysomnography device is a gold standard that is still used today. Unfortunately, this device is still not affordable for the entire community in need. Therefore, we propose a framework by utilizing the Polysomnography device by combining it on the Internet of Things, which focuses on the security and confidentiality of patient data. The safety of patient data is done by dividing and encrypting the patient's medical data archive. While the confidentiality of patient data is done by encrypting data at the time of delivery and is only open in the Graphic User Interface application on devices that have been registered. However, considering the target location of this framework, we adhere to the concept of Offline-First Internet of Things. So that in locations that have limited internet can still monitor sleep quality. Hopefully, the Offline-First Sleep Assessment (OFFSA) framework can be a standard framework for cases of assessing sleep quality.

ACKNOWLEDGMENT

Authors are grateful to Kemenristekdikti for Grant fiscal year 2018-2019 contract number 007/KM/PNT/2018.

REFERENCES

1. K. Spiegel, K. Knutson, R. Leproult, E. Tasali, and E. Van Cauter, “Sleep loss: a novel risk factor for insulin resistance and Type 2 diabetes,” J. Appl. Physiol., vol. 99, no. 5, pp. 2008–2019, Nov. 2005.
2. D. Brooks, R. L. Horner, L. F. Kozar, C. L. Render-Teixeira, and E. A. Phillipson, “Obstructive sleep apnea as a cause of systemic hypertension. Evidence from a canine model.,” J. Clin. Invest., vol. 99, no. 1, pp. 106–109, Jan. 1997.
3. C. A. Kushida et al., “Practice parameters for the indications for polysomnography and related procedures,” An update for 2005, vol. 28, no. 4. pp. 499–521, 01-Apr-2005.
4. J. Haba-Rubio et al., “Obstructive sleep apnea syndrome: effect of respiratory events and arousal on pulse wave amplitude measured by photoplethysmography in NREM sleep,” Sleep Breath., vol. 9, no. 2, pp. 73–81, 2005.
5. K. S. Park, S. H. Hwang, D. W. Jung, H. N. Yoon, and W. K. Lee, “Ballistocardiography for nonintrusive sleep structure estimation,” in 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2014, pp. 5184–5187.
6. S. Ancoli-Israel, R. Cole, C. Alessi, M. Chambers, W. Moorcroft, and C. P. Pollak, “The Role of Actigraphy in the Study of Sleep and Circadian Rhythms,” Sleep, vol. 26, no. 3, pp. 342–392, May 2003.
7. M. J. Sateia, K. Doghramji, P. J. Hauri, and C. M. Morin, “Evaluation of Chronic Insomnia,” Sleep, vol. 23, no. 2, pp. 1–66, Mar. 2000.

8. F. Lin et al., "SleepSense: A Noncontact and Cost-Effective Sleep Monitoring System," IEEE Trans. Biomed. Circuits Syst., vol. 11, no. 1, pp. 189–202, 2017.
9. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
10. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
11. K. Habib, A. B. Torjusen, and W. Leister, "A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth," 2014.
12. P. Verma, S. K. Sood, and S. Kalra, "Cloud-centric IoT based student healthcare monitoring framework," J. Ambient Intell. Humaniz. Comput., vol. 9, no. 5, pp. 1293–1309, 2018.
13. M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring," Comput. Networks, vol. 101, pp. 192–202, 2016.
14. D. Meltzer, "Securing the Industrial Internet of Things," Inf. Syst. Secur. Assoc. J., pp. 24–30, 2015.
15. Y. Ren, R. Werner, N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," IEEE Wirel. Commun., vol. 17, no. 1, pp. 59–65, 2010.
16. J. Mohammed, C. Lung, A. Ocneanu, A. Thakral, C. Jones, and A. Adler, "Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing," in 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), 2014, pp. 256–263.
17. K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, "Security and privacy for mobile healthcare networks: from a quality of protection perspective," IEEE Wirel. Commun., vol. 22, no. 4, pp. 104–112, 2015.
18. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015.
19. M. S. Hossain and G. Muhammad, "Cloud-Based Collaborative Media Service Framework for HealthCare," Int. J. Distrib. Sens. Networks, vol. 10, no. 3, p. 858712, Mar. 2014.
20. Y. Li, L. Guo, and Y. Guo, "Enabling Health Monitoring as a Service in the Cloud," in 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014, pp. 127–136.
21. M. Hassanalieragh et al., "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges," in 2015 IEEE International Conference on Services Computing, 2015, pp. 285–292.
22. L. Hu, M. Qiu, J. Song, M. S. Hossain, and A. Ghoneim, "Software defined healthcare networks," IEEE Wirel. Commun., vol. 22, no. 6, pp. 67–75, 2015.
23. A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 47–65, 2013.
24. B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services," IEEE Trans. Ind. Informatics, vol. 10, no. 2, pp. 1578–1586, 2014.
25. L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE Internet Things J., vol. 2, no. 6, pp. 515–526, 2015.
26. M. M. Hassan, H. S. Albakr, and H. Al-Dossari, "A Cloud-Assisted Internet of Things Framework for Pervasive Healthcare in Smart City Environment," in Proceedings of the 1st International Workshop on Emerging Multimedia Applications and Services for Smart Cities, 2014, pp. 9–13.
27. R. A. Shaikh and others, "Real time health monitoring system of remote patient using ARM7," IJICA, vol. 1, no. 3--4, pp. 102–105, 2012.
28. M. Bazzani, D. Conzon, A. Scalera, M. A. Spirito, and C. I. Trainito, "Enabling the IoT Paradigm in E-health Solutions Through the VIRTUS Middleware," in Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 1954–1959.
29. Y. Zhang et al., "First Trial of Home ECG and Blood Pressure Telemonitoring System in Macau," vol. 3, no. 1, pp. 67–72, 1997.
30. J. S. Karthika, J. M. Thomas, and J. J. Kizhakkethottam, "Detection of life-threatening arrhythmias using temporal, spectral and wavelet features," in 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2015, pp. 1–4.
31. M. Li, X. Sun, H. Wang, Y. Zhang, and J. Zhang, "Privacy-aware access control with trust management in web service," World Wide Web, vol. 14, no. 4, pp. 407–430, 2011.
32. S. Chen, W. Hua, Z. Li, J. Li, and X. Gao, "Heartbeat classification using projected and dynamic features of ECG signal," Biomed. Signal Process. Control, vol. 31, pp. 165–173, 2017.
33. P. Cheng and X. Dong, "Life-Threatening Ventricular Arrhythmia Detection with Personalized Features," IEEE Access, vol. 5, pp. 14195–14203, 2017.
34. R. Ghorbani Afkhami, G. Azarnia, and M. A. Tinati, "Cardiac arrhythmia classification using statistical and mixture modeling features of ECG signals," Pattern Recognit. Lett., vol. 70, pp. 45–51, 2016.
35. H. Wang, Z. Zhang, and T. Taleb, "Editorial: Special Issue on Security and Privacy of IoT," World Wide Web, vol. 21, no. 1, pp. 1–6, 2018.
36. X. Sun, M. Li, H. Wang, and A. Plank, "An Efficient Hash-based Algorithm for Minimal K-anonymity," in Proceedings of the Thirty-first Australasian Conference on Computer Science - Volume 74, 2008, pp. 101–107.
37. X. Sun, H. Wang, J. Li, and Y. Zhang, "Injecting purpose and trust into data anonymisation," Comput. Secur., vol. 30, no. 5, pp. 332–345, 2011.
38. J. Zhang et al., "On Efficient and Robust Anonymization for Privacy Protection on Massive Streaming Categorical Information," IEEE Trans. Dependable Secur. Comput., vol. 14, no. 5, pp. 507–520, 2017.
39. M. E. Kabir, H. Wang, and E. Bertino, "A Role-Involved Conditional Purpose-Based Access Control Model BT - E-Government, E-Services and Global Processes," 2010, pp. 167–180.
40. L. Sun, H. Wang, J. Yong, and G. Wu, "Semantic access control for cloud computing based on e-Healthcare," in Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2012, pp. 512–518.
41. P. Vimalachandran, H. Wang, Y. Zhang, B. Heyward, and Y. Zhao, "Preserving patient-centred controls in electronic health record systems: A reliance-based model implication," in 2017 International Conference on Orange Technologies (ICOT), 2017, pp. 37–44.
42. P. Vimalachandran, H. Wang, Y. Zhang, G. Zhuo, and H. Kuang, "Cryptographic Access Control in Electronic Health Record Systems: A Security Implication BT - Web Information Systems Engineering – WISE 2017," 2017, pp. 540–549.
43. H. Wang, J. Cao, and Y. Zhang, "A flexible payment scheme and its role-based access control," IEEE Trans. Knowl. Data Eng., vol. 17, no. 3, pp. 425–436, 2005.
44. M. Rofouei et al., "A Non-invasive Wearable Neck-Cuff System for Real-Time Sleep Monitoring," in 2011 International Conference on Body Sensor Networks, 2011, pp. 156–161.
45. T. Hao, G. Xing, and G. Zhou, "iSleep: Unobtrusive Sleep Quality Monitoring Using Smartphones," in Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems, 2013, p. 4:1--4:14.
46. M. Kay et al., "Lullaby: A Capture & Access System for Understanding the Sleep Environment," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, 2012, pp. 226–234.