PJAEE, 17 (9) (2020)

PalArch's Journal of Archaeology of Egypt / Egyptology

Attribute-Based Encryption for Securing Healthcare Data in Cloud Environment

C.Krishnan [1] *, T.Lalitha* [2]

[1] Research Scholar, Computer Science, Research and Development Centre, Bharathiar University, Coimbatore

[2] Research Supervisor, Computer Science, Research and Development Centre, Bharathiar University, Coimbatore.

Email I'd: krishnan.peaceful@gmail.com [1], lalithasrilekha31@gmail.com [2]

C.Krishnan [1] , T.Lalitha [2,] Attribute-Based Encryption for Securing Healthcare Data in Cloud Environment- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x, Keywords:Cloud Computing, Security, Encryption, Medical Record, Patient, PHR, AES, GDP

Abstract

Cloud computing techniques store and access many data and programs through the internet instead of a typical local hard drive system. People are still unwilling to set up their health records in the cloud without proper security control. Personal Health Records (PHRs) are a capable patient-centric model for replacing health information and outsourcing to a third party, such as a C.S.P. (Cloud Service Provider). One of the most controversial issues regarding PHRs is the risk to the privacy of patient health-related sensitive information. Associated with the online storage of medical-related information is the fear of exposure to unauthorized people. PHR data outsourced to third parties such as CSP Becomes a threat to the owner of the data. Cryptographic-based conventional encryption techniques encrypt a complete database or file. Nowadays, data owners need to encrypt their health-related information only and not the entire database. This research work concentrates on scalable, secure access control for perturbed PHR information and then outsourcing the data to the cloud environment. This research aims to increase the security, efficiency, and performance of the complete PHR information in a cloud system.

Keywords: Cloud Computing, Security, Encryption, Medical Record, Patient, PHR, AES, GDP

I INTRODUCTION

Cloud computing is the availability of on-demand resources of computer systems, mainly the cloud storage and power of computing expect direct active management by the user. In simple words, cloud computing delivers services from warehouse and control processing, typically through the internet. Cloud computing occupies an extensive range of choices now, from storage, networking and power processing, artificial intelligence, and standard application. This computing network is now becoming the leading choice for many applications. The advantages of cloud computing services include the capacity to scale elasticity. The main issue in cloud computing is the loss of the privacy of any personal data's business value by adopting cloud services by consumers and businesses. With the rise of cloud computing,

service-based computing is becoming the primary paradigm. To use the cloud platform services or to use existing services hosted on clouds, users will have to export their private data to the service provider. Since these service providers are not within the trust boundary, the outsourced data's privacy becomes one of the top-priority problems.

The different kinds of used in PHR are personal data, insurance, etc. The patients' health records include personal information, medical history, examination, and sensitive files. The diagram indicates that confidential information commonly consists of the individual's name, date of birth, age, sex, and height. Then the PHR contains the medical history of the particular person where the conditions, allergy, and the prescription given by the doctor are found. Then in the examination, the patients' total records after the health checkup are records such as pulse rate, heartbeat, sugar level, the result of the blood test, scan report, etc. PHR also includes if any insurance that has taken in the name of the patient. The sensitive information consists of some sensitive records like HIV profiles. The following fig 1 demonstrates the critical identifiers used in the PHR.

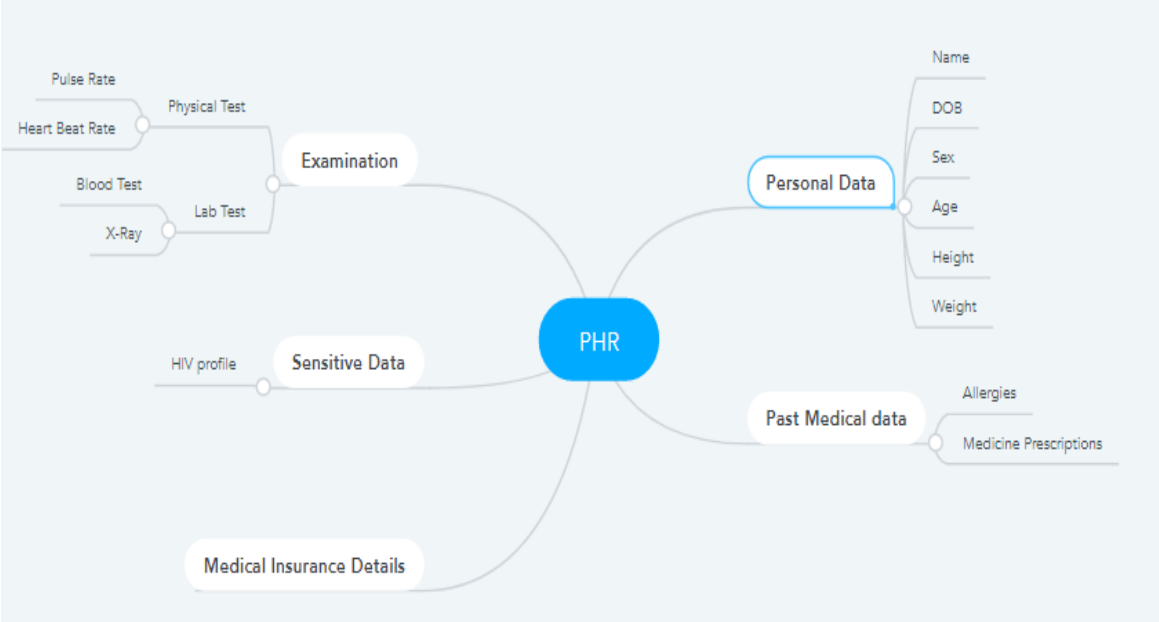

Fig 1 Major PHR Attributes

The second part of this paper describes the various authors about the secure storing of patient records. In the third part, the proposed architecture is explained. The fourth part deals with the result and discussion part. Finally, the fifth part concludes the proposed system.

II LITERATURE REVIEW

Attributes are one of the critical components in the ABE (Attribute-Based Encryption) scheme. Managing health records and cloud environment attributes assure privacy, secrecy, and security of health-related data. Emmanuel Kusi Achampong et al., 2015 use the ABC scheme to increase the privacy of health-related data and review the merits and demerits of a

different kind of ABE. At the same time, this proposed work to search for a solution to increase the current condition and use another type of ABE for securing health records in a cloud environment. ABE type of encryption decreases the internet communication cost and offer managing access system EHR (Electronic Health Record) in the cloud. In this research paper, the authors analyze the various kinds of ABE techniques and supply the suggestion of a better security method to increase the security level in a cloud system[1].

PHR (Personal Health Record) is a kind of health-related data managed by the people in cloud systems to exchange data globally. Cloud contains some sensitive type of information. Unauthorized people are tried to access this kind of sensitive data. Different types of issues are occurring like flexibility, privacy, scalability, and security for maintaining PHR. Rojitha Abdulla et al., 2013 proposes a novel method to encrypt PHR information before third-party people with HASBE (Hierarchical Attribute Set-Based Encryption). It provides the solution to the issues mentioned above with managing access control on health-related information. KPABE is the primary technique used to encrypt PHR content privately [2].

PHR permits the maintenance of their medical-related data in a centralized manner; it makes it possible to access, store, and distribute personal information related to their health. Due to PHR's cloud technology growth, service suppliers transfer their applications into the cloud to use the benefits of different types of resources and decrease the cost needed for an outfit. But before moving PHR data into the cloud encrypt, the health information is required. For every patient, PHR information is encrypted, and several people have the authority to access the data. Numbers of users can access the PHR information; every user can encrypt their PHR information using cryptography keys. Typical cryptographic techniques are mainly developed for a single user only. Ming Li et al., 2010 designed a new architecture for control the accessing mechanism to PHR in cloud systems. ABE method to encode every patient's health-related information to make possible scalable control. Here the authors split the proposed design into many security-related domains to decrease the complexity of supplying keys, where every maintained only a subgroup of the people. Using this method, every user has complete control of their privacy level, and the complexity level of key management is reduced. This new framework is efficient; provide the user right on a demand basis and providing the facility to access at the time of emergency condition also [3].

Hao Wang et al., 2018 proposes a secure EHR scheme based on ABE and the recent blockchain concept to attain privacy, integrity, authentication, and maintain access control. ABE, IBE (Identity Based Encryption) encodes medically related information in this proposed system and IBS (Identity Based Signature) to employ digital kind signatures. To accomplish various purposes of IBE, ABE, and IBS in a single cryptosystem, the authors propose a C-AB/IB-ES novel concept. This concept helps manage the system, and no need to offer various kinds of cryptographic methods for various security issues. The blockchain concept also ensures the traceability and integrity of medical information. At last, the authors describe the applications of insurance view [5].

The medical field faces a challenge to adopt a cloud system due to the large quantity of data and storing patient health information. Conventional methods follow the people-centric technique for managing EHR. It makes a significant issue for the people who have to access their health information. So, better authorization mechanisms are required for secure, safe, and manage EHR data in cloud systems. Maithilee Josh et al., 2018 designed a new centralized, identifier-based authentication approach using ABE and agree to secure patient health information usage. This technique transmits service issues from users to healthcare institutions and permits easy allocation of HER access permission to medical data service providers. Here the authors elaborated on this new ABE technique and developed a prototype to describe that. This system also generates an elaborate type graph showing the attributes and roles of various healthcare institutions users with their associations [6].

Healthcare information is stored and managed in server-based cloud technology. PHR model required privacy and security against hackers. Various security methods save private data from unknown people and loss the data. Md. Irfan et al., 2013 designed a new architecture for securely sharing PHR in a cloud environment. This architecture reduces many health data user's and owners' complexity and ensures the privacy rate than existing techniques. ABE encryption model is enhanced to maintain dispersed ABE tasks with the MA-ABE. This new system also supports an active rule management system. It is one of the server-based model and issues critical management with an identifier. The main intention of this current work is to improve the guarantee for privacy control [9].

The practical and improved method focuses on data processing, accessing the information, and storage to plan to use the official purposes that should receive comparable data and retain the usual. Illegal users get access to the data that provides apt for mobile computing. ABE process over the cloud catches the following, the private span of a key, ciphertext, rekeying extent, public size of a key, estimation expense on the data manager, evaluation on the amount n the user. This proposed work deals with cloud computing based on security purposes. KSS.Trinadh Samudrala et al. made a new cryptography technique with two unique algorithms, namely blowfish and AES is projected. By obtaining symmetric and asymmetric encryption that afford an adequate security level by offering a private key that can be used for various people's decryption method at the same duration. In cloud technology, the critical, challenging problem is user authentication and protecting cloud information. The proposed work can be attained to utilize the efficient blowfish and AES attributes based on encryption mechanism and offers the safety for information contrast to semi-trusted CSP. However, CA(Central Authority) and WAA (Weight attribute authority) provide less security for the large consumed cloud. The outcome is delivered by the proposed HHABE technique that offers efficient reliability and protected information to the conventional HHABE method that provides collaboration, flexibility, and delegation of full data and clarifies the report [10].

Due to the rapid growth of communication technologies quality of the services increased in all sectors. ICT plays a significant role in the medical domain also. Simultaneously, increasing the merits of this ICT technology, a cloud-based system is also necessary. But securing the data

and privacy is the central issue in the cloud environment. Nureni Ayofe Azeez et al., 2019 presented a review report of different techniques used for managing security in electronic health records. Merits and demerits of the security techniques are elaborated in their research work. At last, the authors proposed a new dependable framework for securing e-health records. It assures efficiency, guarantee, and reliability for accessing medical data [11].

By managing the large volume of data, industrial people can use big data techniques. But cloud-based systems are given a better solution to manage a high volume of information. Many researchers concentrate on this field because of its configuration, maintenance, and providing demand-based services. A cloud-based system consists of many benefits; it has many issues like securely maintaining data. Yujiao Song et al., 2019 say that the current ABE technique has not managed privacy problems during the critical development phase. In this research article, the authors developed a new ABE technique that takes care of the user's security during key distribution [12-14].

III PROPOSED ARCHITECTURE

Over the past few years, the growth of communication technology increased day by day. Due to this reason, various new concepts like IoT, cloud, and mobile networking techniques are introduced. Specifically, most organizations generate a massive volume of data daily. Managing and storing a high volume of data is one of the significant issues. Cloud-based systems have overcome the problems mentioned above. But assuring privacy and security to the user is a substantial concern in cloud-based applications. Overcome privacy and security challenges in cloud-based medical systems, various types of security techniques are used. This research work considers AES (Advanced Encryption Standard) and GDP (Geometric Data Perturbation techniques for preserving patient health-related information [15]. The following fig 2 shows the proposed framework for the PHR privacy system. Healthcare professionals, patients, and insurance people are the significant stakeholders of healthcare systems. The patient's sensitive information is stored on the PHR and encrypted using the GDP, DES, Diffie-Hellman and AES technique. The encrypted data stored on the cloud-based server. From the server, healthcare staff members retrieve the patient-related data.

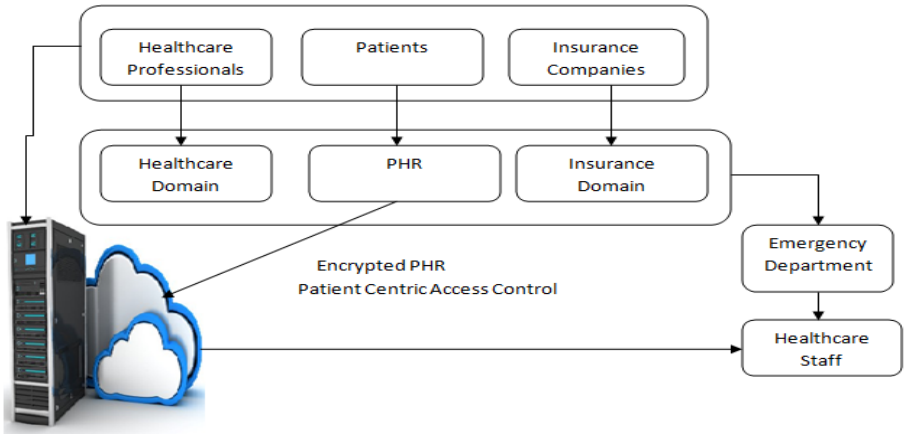

Fig 2 Framework of Proposed PHR Privacy System

AES

AES's original name is Rijndad. It is taking the plain text that is made of random-seeming characters. AES is additional security as it makes use of a critical expansion method where the initial key is used to come up with the series of new keys called round tickets. AES's overall concepts focus mainly on four steps used in each round, byte substitutions, mix columns, and add round access, shift rows. AES is the method used to change the necessary information to something that cannot be read. This part of the technique is called encryption. The process uses a known external piece of information for uniquely changing the data [16]. This process is also reversible when applied again to put the data back to its original form. This process is named decryption. In the field of healthcare, cloud computing develops the efficiency of the industry while decreasing the costs. Cloud computing provides healthcare data sharing in a more leisurely, safer way. Some of the main benefits of cloud computing are security cost, scalability, data storage, and collaboration.

Based on the size of the essential, three kinds of AES approaches are available. They are AES-128, AES-192, and AES-256. AES 128 technique uses the length of the key is 128 bit to decrypt and encrypt a group of contents. AES 192 techniques use 192 bit, and AES 256 uses 256-bit length. In 128-bit key length, the AES technique contains ten iterations. 192-bit key length technique consists of 12 iterations, and a 256-bit length technique includes 14 iterations. Each iteration includes various processing steps like exchanging, transposing, and integrating input plain data to change it into encrypted text.

The following steps are used to encrypt 128 bit block data.

- Obtain the group of round keys from the cipher key.
- Declare the state array with the plaintext content.
- Include the preliminary round key to the initial state array.
- Execute nine rounds of state operation.
- Carry out the tenth and last round of state operation.
- To Copy the last state array out as the ciphertext

GDP

GDP contains a formation of random series geometric type transformation, including the multiplicative type transformation R, translational kind transformation Ψ, and distance type perturbation (S. Balasubramaniam et al., 2015).

$$G(X) = RX + \Psi + \Delta ----------(1)$$

The element R represented the rotation matrix value, and Ψ denotes the importance of translation type transformation, and the final element Δ represents the random matrix data.

S. Balasubramaniam et al., 2015 redefined the GDP formula as the following equation (2)

$$G.D.P.Data = XR + T + G.N - - - - - - - - - - - - - (2)$$

From equation 2 denotes the given original information, R represents the rotation type matrix, T indicates the transpose kind matrix, and GN specifies the Gaussian kind noise.

DES

The Data Encryption Standard (DES) is one of the familiar techniques to encrypt the data. It was initiated by IBM in the year of 1970. New versions of DES are double DES, and triple DES.

- Initially, 64 bit plain text block is handed over to an IP (Initial Permutation) method.
- The preliminary permutation executed on plain text.
- After that the IP generates two halves of the permuted block called LPT (Left Plain Text) and RPT(Right Plain Text)
- Every LPT and RPT to go through 16 rounds of encryption procedure.
- Finally, LPT and RPT are combined and a FP(Final Permutation) is performed on the integrated block
- The outcome of this procedure generates 64 bit cipher text.

Diffie-Hellman

It is a kind of asymmetric type cryptography approach first introduced by Ralph Merkle. Typically the sender and receiver needs to exchange their keys. But this Diffie-Hellman approach avoids exchanging the keys between sender and receiver parties.

Key Exchange Procedure

- Users agree two big prime number n and g
- Sender select the another random value x by using $\boldsymbol{A = g^x \, mod \, n}$
- Sender send to this value to receiver
- Receiver select another number y calculated by using $\boldsymbol{B = g^y \, mod \, n}$
- Receiver send y value to sender
- Sender calculates their secret key value K1 by $\boldsymbol{K1 = B^x \, mod \, n}$
- Receiver calculates their secret key K2 by using $\boldsymbol{K2 = A^y \, mod \, n}$
- K1=K2(Key Exchange over)

IV RESULT AND DISCUSSION

Every organization is generating a large amount of data in their day to day activities. A cloud-based system produces a better solution to store and handle a high amount of data. But adequately securing data is a significant task. Most healthcare organizations also transfer the data from the traditional storage system to a cloud-based system. In healthcare system contains various data, including patient sensitive data. Typically, different types of security concepts are used. In this proposed framework, AES,GDP, DES, and Diffie- Hellman techniques are used to protect the PHR information. Table 1 shows the PHR data encryption

performance value of AES, GDP, DES, and Diffie - Hellmam techniques based on the file size.

Table 1 PHR Data Encryption Performance of AES and GDP Techniques

File Size(in MB.)	AES(in Minutes)	GDP(in minutes)	DES (in minutes	Diffie-Hellman (in minutes)
64	1.4	1.7	1.9	2.2
128	2.3	3.0	3.2	3.5
256	2.8	3.5	3.7	9
512	7.5	8.2	4.0	10.9

Values are logged, and the outcome is represented pictorial as exposed in Fig 3. This figure demonstrates the time taken for encryption by AES and GDP approach.

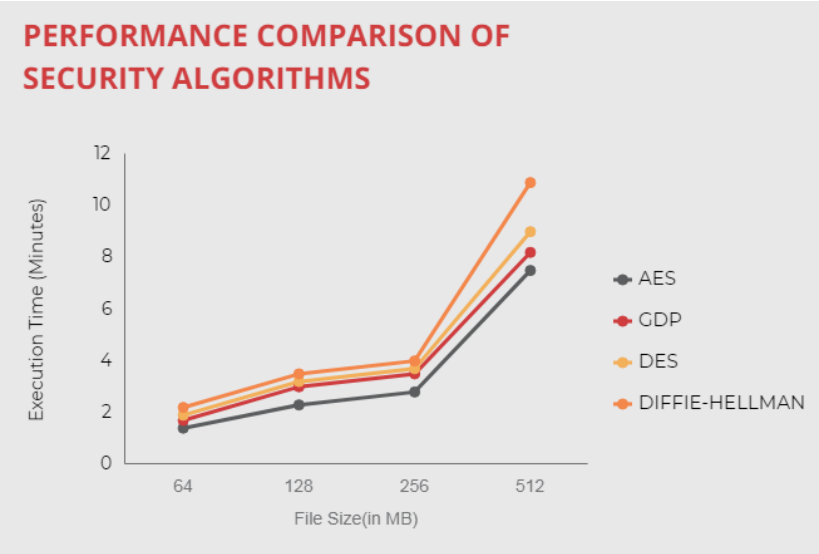

Fig 3 Performance Comparison of AES , GDP, DES and Diffie - Hellman.

Compared to the AES encryption method with the GDP, DES, and Diffie-Hellman technique, AES takes less time for data encryption.

V CONCLUSION

A cloud-based system contains a large amount of information. Due to the flexibility, storage space, and demand for service features, most institutions replace their traditional design with the cloud-based system. But, people are expected to store their data securely. Various approaches are used to solve data security issues of PHR data. Retrieving data from a cloud

system is a challenging task based on user needs. Here the patient's data will be stored on the cloud server after the encryption process. From the cloud-based server, the healthcare staff members are retrieved desired decrypted information. This research paper's primary objective is to analyze AES, GDP, DES, and Diffie-Hellman techniques during the encryption time-based on the size of the file. From the outcome of this system, AES consider as the best encryption method.

REFERENCES

[1] [1] Emmanuel Kusi Achampong & Clement Dzidonu(2015), "Attribute-based Encryption for Electronic Health Records in a Cloud Computing Environment", *International Journal of Cloud-Computing and Super-Computing*, Vol.2, No.2, pp.1-6.

[2] [2] Rojitha Abdulla, Anupriya Vysala(2013), "Secure Personal Health Records in Clouds: A Hierarchical Attribute-Based Solution", *International Journal of Computer Science and Mobile Computing*, ISSN 2320–088X, pp. 44-49.

[3] Ming Li, Shucheng Yu, Kui Ren & Wenjing Lou(2010), "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings", Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol 50. Springer.

[4] Hao Wang & Yujiao Song (2018), "Secure Cloud-Based E.H.R. System Using Attribute-Based Cryptosystem and Blockchain ", *Journal of Medical Systems*, Vo**l.** 42, Article number: 152.

[5] Maithilee Joshi, Karuna P. Joshi & Tim Finin(2018), "Attribute-Based Encryption for Secure Access to Cloud-Based E.H.R. Systems", Proceedings of the IEEE CLOUD Conference.

[6] Nirmala Sugirtha Rajini, S(2015)," Access Control in Healthcare Information Management Systems Using Biometric Authentication", *International Journal of applied environment sciences(IJAES)*, vol. 10 no.1, pp.143-148, ISSN: 0973-6077.

[7] S. Balasubramaniam & V. Kavitha(2015), "Geometric Data Perturbation-Based Personal Health Record Transactions in Cloud Computing", *The Scientific World Journal*, Volume 2015, Article ID 927867.

[8] Md. Irfan & Sayeed Yasin(2010), "A Novel Framework for Securing Medical Records in Cloud Computing", *International Journal of Modern Engineering Research (IJMER)*, Vol. 3, No. 5, pp-2695-2697 ISSN: 2249-6645.

[9] KSS.Trinadh Samudrala, Potluri Sindhu Phani Sree, Chennupati Karthik & Divya Vadlamudi(2019), "An Efficient Data Integrity using Attribute-Based Encryption for Cloud Computing System", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, ISSN: 2278-3075, Vol. 9, No 2, pp. 2186-2190.

[10] Nureni Ayofe, AzeezCharles & Van der Vyver(2019), "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis", *Egyptian Informatics Journal*, Vol. 20, No 2, pp. 97-108.

[11] Yujiao Song, Hao Wang, Xiaochao Wei & Lei Wu(2019), " Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud," *Hindawi Security and Communication Networks*, Vol. 2019, Article ID 3249726, pp. 1-9.

[12] Magesh, S., et al. (2020) "Concepts and Contributions of Edge Computing in Internet of Things (IoT): A Survey." 146 – 156. DOI: 10.22247/ijcna/2020/203914

[13] Rammohan, S. R., Jayashri, N., Bivi, M. A., Nayak, C. K., & Niveditha, V. R. (2020). High performance hardware design of compressor adder in DA based FIR filters for hearing aids. International Journal of Speech Technology, 1-8.

[14] Natrayan, L. P. Sakthi shunmuga sundaram.J. Elumalai.(2019) “Analyzing the Uterine physiological With MMG Signals using SVM”, International journal of Pharmaceutical research 11.2 (2019): 165-170.

[15] Magesh, S., et al. (2020) "Pervasive computing in the context of COVID-19 prediction with AI-based algorithms." International Journal of Pervasive Computing and Communications, 15(5); 477-487.

[16] Sundaram, P. S. S., Basker, N. H., & Natrayan, L. (2019). Smart Clothes with Bio-sensors for ECG Monitoring. International Journal of Innovative Technology and Exploring Engineering, 8(4), 298-301.