International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Survey on Ciphertext Policy Attribute-Based Encryption Scheme based Cloud E- Healthcare Secure Framework

Gurupriya K. G.[1] & Dr. A. S. Aneeshkumar[2]

Submitted: 02/05/2024 **Revised**: 15/06/2024 **Accepted**: 22/06/2024

Abstract: The cloud computing has the potential to completely transform healthcare by lowering costs, increasing accessibility, and improving user experience. Healthcare practitioners required to efficiently and reliably communicate data at any time, from anywhere, in order to appropriately monitor patients and make choices on their requirements. When it comes to cloud-based data interchange and outsourcing, patients' electronic health records' security and confidentiality are top priorities. In the medical field, maintaining patient privacy is crucial, even if it is standard procedure to give patient information to other parties.

To address this security gap and offer secured access to medical and healthcare information, this study suggests a secure healthcare framework that runs in the cloud. This article specifically enhances the Ciphertext Policy Attribute Based Encryption (CP-ABE) technique by adding two more modules that work to provide both fine-grained access control and data privacy and integrity. Encryption and hashing systems are made easier by it. We compare the proposed framework to those that have utilized the CP-ABE approach before. It demonstrates the product's enhanced security capabilities for protecting medical records. It is important to consider data security requirements such as privacy, integrity, and fine-grained access control when proposing solutions for ensuring data sharing in the cloud.

Keywords*: Cloud Computing, Healthcare, Cipher text Policy Attribute Based Encryption,*

Introduction

A new way to effectively supply IT services is via the use of cloud computing, which offers revolutionary computing capabilities. Cloud computing has the potential to improve Quality Of Service (QoS) in several industries, including healthcare and medicine. Electronic health records (EHRs) have essentially revolutionized the healthcare industry by facilitating better data storage, accessibility, sharing, and cooperation among medical professionals. Everything from a patient's medical history to their test results, prescriptions, diagnostic procedures, and physical examinations are all part of the electronic health record. The Health Insurance Portability and Accountability Act (HIPAA) has made the recommendation to secure and preserve the data and documents since the majority of these records are vital and private. As previously said, there are several unnecessary advantages to hospitals and medical organizations that may be realized by using cloud computing for healthcare services.

The utilization of distributed computing in medical services can possibly improve service delivery by lowering execution costs. Healthcare services are also easier to maintain thanks to cloud computing, which allows for excellent monitoring of resource management and system administration (infrastructure). Despite the many benefits, cloud computing faces a significant security risk. Especially susceptible to several security flaws are the frameworks that have been utilized by medical services specialists or end-clients. It is because the irresponsible entity's disclosure of sensitive medical information is intolerable. In addition, consumers may feel a loss of control over their data if it is kept in the Cloud, which may live anywhere and outside territorial boundaries ([1,2]). Another problem with security is the need for healthcare and medical organizations to have a transparent agreement with their CSP, which should address all security concerns. Methods for controlling access and ensuring security are part of this. Cloud service providers (CSPs) often fail to adequately inform their customers about the security risks and requirements associated with renting cloud computing resources. As a result, improving security services for Cloud users and CSP requires data integrity and privacy mechanisms that enable fine-grained access control [3,4].

Healthcare and Medical in Cloud

Healthcare providers and medical practitioners, including physicians and hospitals, are now able to provide their patients more economical and high-quality services because to the fast growth of cloud computing. The company's demands to lower costs and improve the quality of treatment are the two main drivers of this change. To offset the rising infrastructural, administrative,

[1]*Research Scholar, Research Department of Computer Science , AJK College of Arts and Science, Coimbatore, Tamilnadu-641105, India*
Email: gurupriyasarath8@gmail.com
[2]*Research Supervisor and Head, Research Department of Computer Science and Applications, AJK College of Arts and Science, Coimbatore, Tamilnadu-641105, India*
Email: aneeshkumar.alpha@gmail.com

and pharmaceutical costs, providers might reduce operating expenditures from a business perspective. At the same time, they need to address government requirements to improve healthcare quality and implement a unified operational standard for healthcare [15].

On the other hand, patients want services, particularly from online merchants and financial institutions, to be available around the clock, therefore it's imperative that providers meet this expectation by providing services that are both quick and of high quality. At the moment, people are eager to take an active role in their healthcare management, which has increased the requirement for a framework that can give conclusion, data, and therapies. By way of illustration, patients would greatly benefit from a web-based service that allows them to have continuous two-way communication with their healthcare practitioners, particularly in the lead-up to, during, and after any medical operation [6].

Given the current situation, in order to fulfill the needs of their patients as well as a dynamic commercial climate, healthcare providers must immediately start the process of migrating their IT infrastructure from on-premises systems to the cloud. Although it may first seem like a fantastic concept, using cloud computing in healthcare really causes a lot of issues. Though worries over the security and privacy of sensitive data kept in the cloud have grown in recent years, cloud computing is becoming more and more popular as a way to enhance healthcare. Numerous factors, such as data loss or leakage, phishing, account or service hijacking, and an unknown risk profile, put cloud data privacy and integrity at risk [7]. Protecting Cloud-Based Medical Records and Healthcare Information Enabling end users to manage access to data stored on the cloud servers with encryption techniques is a practical approach for medical and health organizations to prevent data leaks, ensure secure transfer, and guard against other security risks.

Users are able to encrypt data using the encryption technique, which guarantees that only the owner of the key can decipher it ([8,47,48]). However, this standard encryption solution is unable to provide one-to-many encryption, which is essential in a cloud sharing scenario. One-to-many encryption allows several users who have the decryption key to decode the data after only one encryption by the data owner. To solve this issue and prevent unauthorized users from accessing the Cloud, a control access mechanism that permits one-to-many encryption should be implemented. The suggested method [9] by the author allows for one-to-many encryption and is based on attribute-based encryption (ABE). The foundation of this plan is an innovative patient-centered architecture for managing who has access to PHRs kept on semi-trusted cloud servers.

Applications in E-Health record on Cloud systems

The expression "e-wellbeing distributed computing" portrays the utilization of distributed computing to work on quiet consideration; this sort of distributed computing gives chances to defeat specific deficiencies of clinic data frameworks. Healthcare services may be greatly enhanced if patients have 24/7 access to their medical records. Medical records may be accessed using cloud computing, which helps enhance healthcare facilities. Data breaches, assaults, and thefts may happen more easily on the cloud because of the shared and open nature of the environment in which cloud computing is often run. The healthcare business is hesitant to use cloud computing technologies due to security concerns. Because of the potential for hackers to get access to patient medical information, healthcare professionals are wary about cloud computing. People do have legitimate worries about security and privacy [10,46].

If healthcare providers and consumers are to have more faith in cloud computing, the companies providing the service need resolve security issues. It has been shown in research that an increasing number of healthcare administrations are planning to use cloud computing services. Nonetheless, as shown earlier, the healthcare business has found many uses for cloud computing, especially in the realm of administration. Because of the functional difficulties of conveying clinical benefits, the medical care business is extremely confounded [11].

Dissimilar stakeholders with diverse interests and sector-specific traits comprise the healthcare business. Consequently, there are many facets to cloud computing as it pertains to healthcare, and its implementation via healthcare institutions can only be guaranteed under certain conditions. Many important issues related to these situations should be thought about before putting distributed computing frameworks right into it. Settling on an execution decision without cautiously thinking about the components that will determine it might cause complications and impede the healthcare industry's efficient use of cloud computing. An enormous UK hospital, for instance, lost £8.6 million and temporarily interrupted medical services due to an ill-informed choice to implement cloud computing [12].

By making available to users innovative protocols that were previously unimaginable, e-health cloud computing platforms are radically altering the healthcare sector. The innovative foundation of contemporary health systems will be e-health cloud computing solutions. One study that looked at healthcare security was that of Ambarkar and Shekokar [13]. The benefits of utilizing e-wellbeing distributed computing stages to further develop diagnostics in various applications were discussed by Farahani et al. [14]. In order to facilitate a more efficient

recovery, doctors may use data-driven treatment regimens made possible by cloud computing equipment. In order to power e-health distributed computing frameworks, individual wellbeing the board, and information disclosure, Abouelmehdi et al. [15] utilized enormous information.

They looked at the pros and cons of privacy and security technology in relation to e-health cloud computing platforms. When assessing healthcare cloud computing systems, factors such as cloud software, cloud service delivery, and healthcare cloud administration could play a role. To solve healthcare problems, they advocated using a cloud computing strategy. A comprehensive analysis of the existing research on healthcare data privacy and security issues[16]. The limits of healthcare designs were also studied by Semantha et al. [17], who reviewed the existing literature on privacy design in healthcare and categorised them. In addition, they highlighted vital research paths for future progress.

The Factors Influencing the Cloud Computing System Adoption

I)Cloud Management

Management considerations, such as the need to integrate and share data as well as keep costs down, are a key factor in the rise of cloud computing. When it comes to software as a service, for example, businesses typically buy adaptation updates and pay month to month programming charges in light of the quantity of clients, in this way diminishing data innovation costs and data mix.. This is just one example of how implementing a cloud computing system can lead to significant savings. The more money a system saves with cloud computing, the more effective the system is. Consequently, healthcare organisations may avoid the hazards of product redundancy and the constraints of conventional software licencing models by paying licence costs on a monthly basis, allowing them to prolong the product lifespan of software [44].

In addition, service providers provide limitless, pay-as-you-go client services that may be adjusted on the fly by constructing virtual resource pools for maintenance, adoption, design, and integration of customisation infrastructures, all while saving customers money. You won't have to spend money on data storage devices, administration, maintenance, easy information exchange, or any other gear when you use the cloud services. Clients would be tasked with resolving these management issues in the absence of cloud services. Consequently, while evaluating cloud the board capabilities for e-health distributed computing frameworks, it is urgent to consider data incorporation, simple data trade, and cost adequacy [18].

II) Cloud Service Delivery

Reliable services are produced by cloud computing systems that consistently maintain high quality. In addition, system security is closely linked to programming innovative work, testing and troubleshooting, and framework dependability since framework engineers underscore that data security is connected with the probability of accomplishing information stockpiling security and framework solidness. Distributed computing administration frameworks in medical care are susceptible to hackers, viruses, and data theft since they rely on network architectures. As a result, e-health cloud computing system evaluations must take testing and debugging, software R&D, and system stability extremely seriously [49].

III)Cloud Security

Data integrity, access control, and confidentiality were our primary concerns. The data breach risk increases when data is delegated to the cloud since many parties will have access to the data. The potential for data breach grows in proportion to the proliferation of connected devices, apps, and stakeholders. Ensuring the consistency and accuracy of health data given to or acquired by a system is crucial for maintaining integrity. No modifications should be made to this data in any way. A highly reliable e-health cloud is essential. No mistakes should be made in the e-health cloud data or services. Only a designated medical professional or a third party with proper authorization will be able to access a patient's medical records according to this policy. Concerns about access and control security have prompted a plethora of proposed solutions. The majority of healthcare cloud computing solutions use attribute-based or role-based access restrictions [19,45].

IV)Cloud Software

An e-health cloud computing system's software mechanism is the center of whatever service it offers. The healthcare sector places great importance on software scalability, cloud-based medical image exchange, and user-friendly interfaces. High user satisfaction can be achieved by healthcare cloud computing systems when the following requirements are met: software should be easily configurable and scalable; Patients and healthcare professionals should be able to manage system operations; and all software should be designed with the healthcare environment in mind. As this feature could centre on urgent care, cloud-based medical picture interchange is essential. As a result, health information systems should have structures that allow for the fast and accurate transfer of medical records and the categorization of crucial patients' medical data or photos, so that personnel can effectively identify and treat crises [20,21].

After reviewing the literature, consulting with experts, and having extensive conversations with healthcare industry administrators and researchers, we were able to separate the security and cloud computing features of e-health cloud records into four primary categories: cloud software, cloud administration, cloud service provisioning and cloud security. Three factors influence cloud management: cost-effectiveness, ease of information interchange, and knowledge integration. Three factors affect the delivery of cloud services: system stability, software development and research, and testing and debugging. Transparency, data integrity, and access control are the three pillars upon which cloud security rests. Software scalability, software ease of use, and cloud computing for medical image interchange are the three aspects that influence cloud software. This research aimed to shed light on the aspects that matter most in achieving the targeted financial and commercial performance by examining the interrelationships between different components and estimating their relative importance [22, 23].

Setup Algorithm

A. **Input** to the setup procedure is a security parameter, and outputs are a master key and a public parameter key. An algorithm for generating keys will use both of these as inputs. The setup technique uses Bilinear Pairing to obtain a public key, which is then utilized by Attribute Authority.

B. **Key Generation** The Duty to Generate Keys is Carried Out by the Attribute Authority. An operation will be performed on the inputs of user characteristics, public parameters, and master key in order to construct a secret key. As time goes by, the data user will utilize this secret key to decipher the encrypted message.

C. **Hashing** The SecHC module that was just added is this one. Using a mathematical function, the hashing method produced a hash value from the user's input. It was used to check whether a file was intact after being transmitted. By using the MD5 method, this module will hash the access policy characteristics [31,32]. In comparison to other algorithms, MD5 is very efficient and runs quickly (as stated in reference 33). Soon after the hashing operation is completed, the ciphertext and hashed value are sent to the cloud.

D. **Data Encoding** Here, the algorithm accepts the Data Owner's inputs and generates ciphertext. An method for encrypting data into an unintelligible form is the Advanced Encryption Standard (AES). The data owner will provide the ciphertext and hashed value to a cloud service so that other users may access them [34,50].

E. **Covert Access Policy** By default, Cloud storage for ciphertext also includes the access policy in a readable format, according to conventional CP-ABE. So, policy privacy is compromised since anybody may decipher the ciphertext and discover the access policy. Therefore, an access policy concealing scheme that is created and put into place in Secure Health record to provide fully disguised access policies is a solution to this issue. In this module, attributes' names and values are converted into abstract notions using the Logical Connective Operator. Then, this worthless value will be sent to the cloud together with the hashed value and ciphertext. [35].

F. **Uncovering Secret Access Policy Data** A user can't access or download a file from the cloud unless they first extract the concealed access policy. This section will carry out the opposite operation of the previous one, transforming the concealed access policy from an empty string of values back into an actual access policy. Hashing verification will be carried out once the access policy has been extracted.

G. **Validation of Hashing** To verify the authenticity of the ciphertext and access policy, a hashing verification approach can be employed. Ensuring the integrity of the sent ciphertext is the responsibility of this module. This section requires the user to execute an algorithm (a hashing verification method) in order to get access to the policy [36]. After downloading from the cloud, if the hash value of the access policy is the same as before, then the file is an exact replica. The next step is for the user to access the decryption module. On the other hand, the procedure will terminate if the values differ.

H. **Deciphering** Once the hashing verification procedure has generated a genuine hashing value, the decryption module may begin. Decryption schemes generate messages by taking ciphertext, a public parameter, and a secret key as inputs [37,38].

Data Security Requirement Analysis of e Health care record

Concerns about data privacy, secrecy, and integrity have arisen as a result of organizations exchanging patient records on the cloud, which is a major concern in the healthcare industry. Based on this need, the Sec HC framework was created to address and fulfil Cloud security requirements [39]. This is how the security requirements analysis is laid out.

Data Privacy

Entire privacy is safeguarded by the suggested architecture. By using the encryption technique, it safeguards users' privacy. The proposed architecture made use of the encryption algorithm of the CPABE scheme to provide data privacy in a secure health Cloud. Users may ensure the confidentiality of their electronic health records by storing them in the cloud in an encrypted format with a concealed policy. Part B: Ensuring the Originality of Data The suggested system employs the hashing method to safeguard data integrity against tampering, deletion, or fabrication[40]. Accurate data storage on the cloud

requires only reliable information, and consistent results are possible with outsourced data that has not been altered, destroyed, or otherwise interfered with. The system will encrypt all health records and medical information, and it will hash all policies pertaining to access. The purpose of this hashing procedure is to verify that the ciphertext kept in the cloud has not been altered in any way. The decryption operation will fail if the ciphertext is altered in any way. Performing this procedure validates that the suggested architecture provides a means to safeguard information in a protected health Cloud environment [41].

Access Control

No two people using a healthcare cloud will ever have the same level of access to patients' data. The level of involvement or specialization of the user determines the extent to which this permission is granted. As a result, the architecture guarantees that each user will have unique access rights established by the policy and enforced by the attribute authority. This framework's usage of the CP-ABE scheme allows for very granular control over who has access to what. This implies that in order to get the necessary information, all the characteristics need to be compatible with the help of user access policy framework [42,43].

Conclusion

In an era where data breaches are occurring more often, cloud computing has to offer a security solution to protect sensitive data and transactions. Data transfers are shielded with this technique from data modification and eavesdropping. Here, we create the secure healthcare framework by refining the Ciphertext Based Encryption technique.

Both consumers and suppliers in healthcare and medical organizations may benefit from this, since it enhances the security and privacy of the Cloud. By providing a granular approach to access control, the secure healthcare framework ensures that sensitive medical and healthcare data remains private and uncompromised. The CP-ABE scheme, which combines old and modern parts, is responsible for providing it.

Fast decryption and a completely concealed access policy are features of such components. This framework satisfies the criteria for safeguarding the availability and confidentiality of medical records, according to the study of security requirements. Real medical and healthcare data will soon be able to be managed in a cloud environment via the proposed framework.

References

[1] O. Ali, A. Shrestha, and S. Fosso, International Journal of Information Management, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," vol. 43, no. April, pp. 146–158, 2018.

[2] F. Shiferaw and M. Zolfo, "The role of information communication technology (ICT) towards universal health coverage: the first steps of a telemedicine project in Ethiopia," Global health action, 5(1), 15638, no. June 2014, pp. 0–8, 2012.

[3] J. J. Yang, J. Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future. Gener. Computer. Syst., vol. 43–44, pp. 74–86, 2015.

[4] A. Jemai, R. Attia, N. Kaaniche, S. Belguith, and M. Laurent, "PHOABE: Securely outsourcing multi-authority attribute-based encryption with policy hidden for cloud assisted IoT," Computer. Networks, vol. 133, pp. 141–156, 2018.

[5] N. Sultan, "International Journal of Information Management Making use of cloud computing for healthcare provision: Opportunities and challenges," Int. J. Inf. Manage., vol. 34, no. 2, pp. 177–184, 2014.

[6] N. Y. Lee and B. H. Wu, "Privacy Protection Technology and Access Control Mechanism for Medical Big Data," Proc. - 2017 6th IIAI Int. Congr. Adv. Appl. Informatics, IIAI-AAI 2017, pp. 424–429, 2017.

[7] L. Ibraimi, M. Asim, and M. Petko, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," Proc. 6th Int. Work. Wearable, Micro, Nano Technol. Pers. Heal., pp. 71–74.

[8] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," IEEE Access, pp. 22313–22328, 2017.

[9] T. Kajiyama, M. Jennex, and T. Addo, "To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions," Inf. Comput. Secur., pp. 00–00, 2017.

[10] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attributebased data access control in mobile cloud computing: Taxonomy and open issues," Futur. Gener. Comput. Syst., vol. 72, pp. 273–287, 2017.

[11] Satar, S.D., Hussin, M., Hanapi, Z., & Mohamed, M.A. (2018). Data Privacy and Integrity Issues Scheme in Cloud Computing: A Survey. International journal of engineering and technology, 7, 102.

[12] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, and D. S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption," Multimedia Tools and Applications, 74(10), 3441-3458.2014.

[13] Ambarkar S.S., Shekokar N. Internet of Things, Smart Computing and Technology: A Roadmap Ahead. Springer; Cham, Switzerland: 2020. Toward Smart and Secure IoT Based Healthcare System; pp. 283–303.

[14] Farahani B., Firouzi F., Chang V., Badaroglu M., Constant N., Mankodiya K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Gener. Comput. Syst. 2018;78:659–676. doi: 10.1016/j.future.2017.04.036.

[15] Abouelmehdi K., Beni-Hssane A., Khaloufi H., Saadi M. Big data security and privacy in healthcare: A Review. Procedia Comput. Sci. 2017;113:73–80. doi: 10.1016/j.procs.2017.08.292.

[16] K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen, "An Efficient and Fine-Grained Big Data Access Control Scheme with PrivacyPreserving Policy," IEEE Internet Things J., vol. 4, no. 2, pp. 563–571, 2017.

[17] Semantha F.H., Azam S., Yeo K.C., Shanmugam B. A Systematic Literature Review on Privacy by Design in the Healthcare Sector. Electronics. 2020;9:452. Doi: 10.3390/electronics9030452.

[18] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[19] S. Sabitha and M. S. Rajasree, "Access control based privacy preserving secure data sharing with hidden access policies in cloud," J. Syst. Archit., vol. 75, pp. 50–58, 2017.

[20] H. Wang, X. Dong, and Z. Cao, "Multi-value-Independent CiphertextPolicy Attribute Based Encryption with Fast Keyword Search," IEEE Transactions on Services Computing vol. 1374, no. c, 2017.

[21] L. Zhang, Y. Cui, Y. Mu, and S. Member, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," IEEE Systems Journa, pp. 1–11, 2019.

[22] Q. Han, Y. Zhang, and H. Li, "Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things," Future. Gener. Comput. Syst., vol. 83, pp. 269–277, 2018.

[23] Abd Hamid, N., Ahmad, R. and Selamat, S.R., 2017. Recent Trends in Role Mining Algorithms for Role-Based Access Control: A Systematic Review. World Applied Sciences Journal, 35(7), pp.1054-1058.

[24] F. Deng, Y. Wang, L. I. Peng, H. U. Xiong, and Z. Qin, "CiphertextPolicy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records," IEEE Access, vol. 6, pp. 39473–39486, 2018.

[25] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System," IEEE Access, vol. 3536, no. c, pp. 1–1, 2019.

[26] D. Slamanig and C. Stingl, "Privacy Aspects of eHealth," pp. 1228– 1235, 2008.

[27] Z. Ying, L. U. Wei, Q. I. Li, X. Liu, and J. I. E. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," vol. 6, 2018.

[28] N. Muhammad, J. M. Zain, and M. Mohamad, "Current Issues in Ciphertext Policy-Attribute Based Scheme for Cloud Computing : A Survey," International Journal of Engineering & Technology, vol. 7, pp. 64–67, 2018.

[29] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," Proc. - 2010 IEEE 3rd Int. Conf. Cloud Comput. CLOUD 2010, pp. 268–275, 2010.

[30] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health : Efficient Access Control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, 2018.

[31] Rachmawati, D., Tarigan, J. T., & Ginting, A. B. C. (2018, March). A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. In Journal of Physics: Conference Series (Vol. 978, No. 1, p. 012116).

[32] S. Sharaf and N. F. Shilbayeh, "A Secure G-Cloud-Based Framework for Government Healthcare Services," IEEE Access, vol. 7, pp. 37876– 37882, 2019.

[33] H. Xiong, Y. Zhao, L. Peng, H. Zhang, and K. Yeh, "Partially policyhidden attribute-based broadcast encryption with secure delegation in edge computing," Futur. Gener. Comput. Syst., vol. 97, pp. 453–461, 2019

[34] Gao F., Sunyaev A. Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. Int. J. Inf. Manag. 2019;48:120–138. Doi: 10.1016/j.ijinfomgt.2019.02.002.

[35] Chen C., Watanabe C., Griffy-Brown C. The co-evolution process of technological innovation—An empirical study of mobile phone vendors and telecommunication service operators in Japan. Technol. Soc. 2007;29:1–22. Doi: 10.1016/j.techsoc.2006.10.008.

[36] Buyya R., Yeo C.S., Venugopal S. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities;

Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications; Dalian, China. 25–27 September 2008; pp. 5–13.

[37] Vaquero L.M., Rodero-Merino L., Caceres J., Lindner M. A break in the clouds: Towards a cloud definition. ACM SIGCOMM Comp. Commun. Rev. 2008;39:50–55. Doi: 10.1145/1496091.1496100.

[38] Hathaliya J.J., Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput. Commun. 2020;153:311–335. doi: 10.1016/j.comcom.2020.02.018.

[39] Liao W.-H., Qiu W.-L. Applying analytic hierarchy process to assess healthcare-oriented cloud computing service systems. SpringerPlus. 2016;5:1–9. doi: 10.1186/s40064-016-2686-3.

[40] Butpheng C., Yeh K.H., Xiong H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. Symmetry. 2020;12:1191. doi: 10.3390/sym12071191.

[41] Botta A., De Donato W., Persico V., Pescapé A. Integration of Cloud computing and Internet of Things: A survey. Future Gener. Comput. Syst. 2016;56:684–700. doi: 10.1016/j.future.2015.09.021.

[42] Azeez N.A., van der Vyver C. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egypt. Inform. J. 2019;93:237–255. doi: 10.1016/j.eij.2018.12.001.

[43] Singh S., Wachter R. Perspectives on medical outsourcing and telemedicine: Rough edges in a flat world? N. Engl. J. Med. 2008;358:1622–1627. Doi: 10.1056/NEJMhle0707298.

[44] Standing S., Standing C. Mobile technology and healthcare: The adoption issues and systemic problems. Int. J. Electron. Health. 2008;4:221–235. Doi: 10.1504/IJEH.2008.022661.

[45] Rahmani A.M., Gia T.N., Negash B., Anzanpour A., Azimi I., Jiang M., Liljeberg P. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Gener. Computer. Syst. 2018;78:641–658. Doi: 10.1016/j.future.2017.02.014.

[46] Shewale A.D., Sankpal S.V. IOT & Raspberry Pi based Smart and Secure Health Care System using BSN. Int. J. Res. Appl. Sci. Eng. Technol. 2020;8:506–510.

[47] Dang L.M., Piran J., Han D., Min K., Moon H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics. 2019;8:768. Doi: 10.3390/electronics8070768.

[48] Wu J., Tian X., Tan Y. Hospital evaluation mechanism based on mobile health for IoT system in social networks. Computer. Biol. Med. 2019;109:138–147. Doi: 10.1016/j.compbiomed.2019.04.021.

[49] Tuli S., Basumatary N., Gill S.S., Kahani M., Arya R.C., Wander G.S., Buyya R. HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. Future Gener. Comput. Syst. 2020;104:187–200. Doi: 10.1016/j.future.2019.10.043.

[50] J. Sen, "Security and Privacy Issues in Cloud Computing," J. Netw. Comput. Appl., vol. 71, no. iv, pp. 11–29, Mar. 2013.

[51] Rakesh K K, Dr.A .S Aneeshkumar, "Optimization of Fuzzy Logic-Based Genetic Algorithm Techniques in Wireless Sensor Networks Protocols". VOL. 12 NO. 14S (2024)