A Review of Security and Privacy of Cloud Based E-Healthcare Systems

Faiza Nawaz, Jawwad Ibrahim, and Maida Junaid
faizanawaz42@gmail.com, maidajunaid765@gmail.com,
†Faculty of Computer Science & IT, University of Lahore, Gujrat Campus, 50700 Gujrat
†† Faculty of Computer Science & IT, University of Lahore, Gujrat Campus, 50700 Gujrat

Abstract
Information technology plays an important role in healthcare. The cloud has several applications in the fields of education, social media and medicine. But the advantage of the cloud for medical reasons is very appropriate, especially given the large volume of data generated by healthcare organizations. As in increasingly health organizations adopting towards electronic health records in the cloud which can be accessed around the world for various health issues regarding references, healthcare educational research and etc. Cloud computing has many advantages, such as "flexibility, cost and energy savings, resource sharing and rapid deployment". However, despite the significant benefits of using the cloud computing for health IT, data security, privacy, reliability, integration and portability are some of the main challenges and obstacles for its implementation. Health data are highly confidential records that should not be made available to unauthorized persons to protect the security of patient information. In this paper, we discuss the privacy and security requirement of EHS as well as privacy and security issues of EHS and also focus on a comprehensive review of the current and existing literature on Electronic health that uses a variety of approaches and procedures to handle security and privacy issues. The strengths and weaknesses of some of these methods were mentioned. The significance of security issues in the cloud computing environment is a challenge.

Keywords:
Cloud Computing, Electronic Healthcare System, Security, Privacy Health Information Technology

1. Introduction

Today, the healthcare industry demands to generate an environment that minimizes long term efforts and other expensive processes, to acquire the patient's entire medical record and consistently assimilate this diverse assortment of medical information for delivery to the health system [1]. In operational experience, technologies are rarely used in such industries, limiting the medical fields. There are still some medical areas where paper records remain. Similarly, they have computerized their data in the health fields. The adoption of technology will facilitate collaboration across the essential health sector to distribute

data to victims, doctors, physicians, psychiatrists and health researchers. To transform and rebuild the healthcare sector, cloud computing is universally accepted. The medical organization is transitioning to a paradigm that helps support and match medical data and workflows. Between authorized users and hospitals, cloud computing facilitates the loading of large amounts of information and allows the distribution of data as well as increased data analysis or monitoring functionalities. It will help to improve the capacity of doctors and provide good treatment to patients, as well as at a reasonable cost to improve the benchmark of an investigator's data [2].

Cloud computing services offer the required framework at lower and better prices. Cloud computing, when utilized in the healthcare industry, "reduces storage, processing and updating costs, with increased efficiency and quality". Internally, it can ease the load of framework and the quantity of individuals included, and allow institutions to focus on their core competencies. In synergy, cloud computing and intelligent elements help patients, clinics and insurers to obtain patient health records when required. So, the improvement of intelligent health innovations, Like "mobile health care, wireless sensors and cloud computing", reduces the need to visit medical services and practices, which can be met remotely and reduce the manpower requirements, and provide high quality treatment to the patient by making remote consultation and treatment feasible and achievable. However, the implementation of these technologies presents many challenges, such as "security and confidentiality issues, technological constraints or management and governance challenges" [3]. The electronic health record (EHR) is made up of highly confidential patient record images. EHRs in healthcare comprise "scan images, DNA reports, x-rays", which are viewed as a patient's private information. Security is required for huge volumes of high efficiency information. Health cloud data is encrypted. This information is very essential and constitutes an appealing objective for cyber criminals. Many researchers have offered a framework to protect the healthcare cloud and numerous procedures have been studied to secure information in the cloud [1].In the cloud-based health information system (HIS), privacy and security ought to be a top need from the right first moment.

Manuscript received June 5, 2024
Manuscript revised June 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.6.18

Patient information must be secured with comprehensive "physical security, data encryption, user authentication and application security", just as the most recent security practices and certificates that set standards and protect end-to-end data repetition aimed at data backup. These security issues have been widely studied for cloud computing generally. The main problem to the healthcare cloud is the security fears, such as, “interference or leakage of confidential patient data to the cloud, loss of confidentiality of patient information and unauthorized use of that information". Therefore, cloud computing systems for healthcare must meet various security requirements [4]. The enduring part of the document is prepared as follows: Section 2 contains the cloud computing architecture and health framework services. The third section presents a brief electronic structure of the modern health care framework. The security and privacy needs of EHS in cloud computing are discussed in section 4. The issues of categorizing security and privacy of EHS are detailed in section 5. The comparative study of literature is introduced in section 6. After analysis, we have open problems and challenges, debated in section 7. Lastly, the conclusion is introduced in section 8.

2. Cloud Computing

Cloud computing is the extent of IT services like "servers, storage, databases, networks, software, machines and more devices on the Internet", called "the cloud". Cloud computing is a technique utilized by the "Internet and remote central servers to store data and other applications". Cloud computing enables clients and businesses to upload their files to and from any computer over the Internet, and use the applications. This innovation provides efficient computing thanks to "central storage, processing and data volume".

2.1 Cloud Architecture

Cloud Computer architecture can be separated into two sections. These are called the "front and back ends". The front end contains the customer's PC and the applications expected to get to and do the operation proceeding the cloud computing framework. Not all Cloud Computing frameworks need to have a similar UI as appeared in Figure 1 [5].

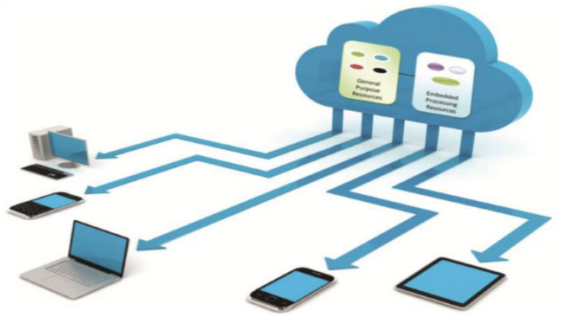

Fig.1 Cloud Architecture [5]

At the back of the system there are many systems, "servers, and data storage systems" that are the cloud of IT services. Theoretically, a cloud computing framework can be any PC program, from information preparing toward video games. Each application has its own server. A main server manages the "system, monitors traffic, and makes sure everything is working properly". It keeps a lot of rules named as "protocols" and utilize a specific type of software called "middleware". Middleware enables networked computers to interconnect with one another [6].

2.2 Cloud Deployment Models

The cloud deployment models below are mainly used to provide cloud services for healthcare. **Private cloud:** Institutions usually manage and maintain it. For specific e-Health the cloud architecture, like, "storage and processing units", is maintained through hospitals or any assigned outsider. Though, because to the limited availability of "public Internet access, electronic medical records (EMRs)" kept in the "private cloud" are considered safer than other deployment models. This happens in the light of a fact that EMR employees merely access EMRs in a private cloud atmosphere, which is generally considered reliable (with a few exceptions). **Public cloud:** The public cloud is a shared physical framework handled by external providers. Establishments using cloud facilities receive the facilities through the cloud "service providers (CSP)". In a public online health cloud, electronic medical records (EHR) can be divided among many participating organizations like, "clinics, hospitals, insurance companies, pharmacies and clinical laboratories". In addition, EHRs kept on external servers handled by CSP. As a result, EHRs are profoundly unsafe to pernicious assaults and tries to falsify internal and external assets. Therefore, methods are needed to reduce privacy issues and make sure privacy through strong "cryptographic techniques, patient-centered access control and effective signature verification schemes" [7]. **Hybrid clouds:** Hybrid clouds are a mixture of at least two or more cloud providers "public or private", so they work independently, but they connect with standard technology. The hybrid cloud deployment model is very useful for medical facilities, where medical professionals with restricted physical assets who want to use legacy structures can access third-party amenities to save a large

scale clinical and medical records. Though, one of the main limitations of this model is that it needs a number of security measures to protect your privacy [8].

2.3 Cloud Service Models

Those involved in the field, such as doctors, physicians, researchers, and many others, could compete with three key cloud service solutions that could meet their professional requirements. Service models allow "software access as a service (SaaS), service infrastructure (IaaS), and platform as a service (PaaS) ". For each of the three services, **SaaS** is the payment method that is the most cost-effective choice, particularly for small hospitals or clinics. SaaS does not need an always IT professional and it also minimizes capital investment needed for "hardware, software and operating systems". **PaaS** is a comprehensive cloud-based development and deployment platform that allows you to offer everything from simple "cloud based apps to sophisticated, cloud-enabled healthcare applications" [9]. The hospital must buy the cloud service source according to the payment method and use it for a secure Internet connection. The **IaaS** is able to work in the health department with a more scalable infrastructure. Because IaaS is low cost, it puts a strain on security, flexibility, data protection and backups [10].

3. Electronic Healthcare System

Electronic health is a developing area at the intersection of "medical informatics, public health and business, referring to health services and data provided" or enhanced via an Internet and related innovations. From a more extensive perspective, "the term characterizes not only technical development, but also a state of mind, a way of thinking, behavior and a commitment to thinking of global networking, to enhance health care at the local level, regional and global by using information and communication technology"[11]. Today, healthcare facilities need a framework that minimizes long and high cost operations to acquire a complete patient medical record and integrates a seamless medical data collection for delivery to healthcare professionals. Electronic health records so that information about health care, insurance companies and patients can generate, control and acquire medical data in all cases. Each health industry must manage more demands with the resources available. The main purpose of the entire medical institution is to expand the quantity of individuals receiving medical services. To improve service quality, "as the amount of data that needs to be stored, processed, and updated increases exponentially", the healthcare industry needs more computing power. The cloud computing atmosphere ensures patient care and meets the needs of the healthcare industry by giving better, quicker, safer and more versatile facilities at a lower price. Therefore, healthcare workers are all the more ready to migrate their frameworks to the cloud to eliminate the barrier of geographic distance between healthcare workers and patients. With cloud computing, some specialists can get to a patient's health proceedings regardless of whether they are miles separated. These doctors can transfer their medical records without direct communication. These can be accessed from the cloud [12].The types of e-health cloud structure may be "public, private, hybrid and community" based on the information kept. Since the EHR information is firmly "confidential, containing sensitive patient information and located on third-party servers, access control techniques" are necessary. "Access control" is a security hindrance that ensures information protection by limiting processes and access to health documents in the healthcare framework. The basic techniques of "Access Control" in health frameworks are "Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Identity Based Access Control (IBAC)". The "Role-Based" System assigns users a role to access data. ABAC uses encryption and non-encryption technologies, but "IBAC" utilizes an identity-based encryption mechanism that uses client uniqueness for data encryption. Data share is a characteristic of electronic medical frameworks. It may be shared between different stakeholders like "healthcare providers, hospitals, healthcare organizations", etc. Research is an important alternative function of electronic medical systems. "Proxy encryption and public key encryption" are commonly utilized as an encryption mechanism for information retrieval [13]. The following figure shows the structure of electronic health data in the cloud.

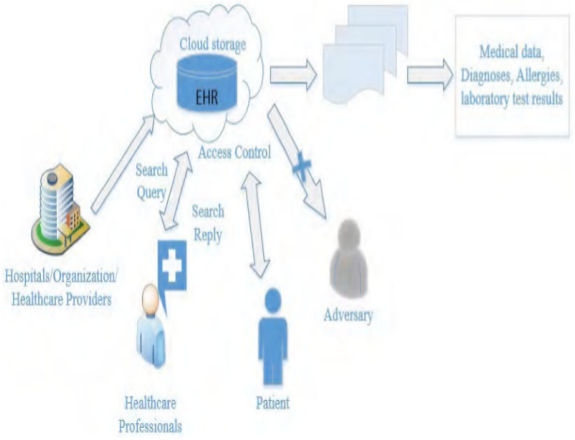

Fig. 2 Architecture of electronic health data in the cloud [13].

4. Privacy and Security Requirements of EHS

The advancement of electronic health solutions has placed more accentuation on the security and confidentiality of users' health facts, as various attacks, "such as tampering of data, information disclosure, denial

of service and insider attack ", can lead to digitization and outsourcing [14]. A lot of essential security and protection prerequisites that must be kept up in electronic health solutions are distinguished and condensed in Table 1.

Table 1: Security and privacy requirements of EHS

Requirements	Description
Patient's understanding	Expresses patients reserve the option to see how their private data is held and used by caregivers.
Patient's control	It is up to the patient to know who can control their health information.
Confidentiality	Patient health information should be maintained confidential for any party who is not entitled to retrieve the information.
Data integrity	This makes the unauthorized "omission, tampering and destruction of health records" mandatory. Therefore, the integrity information exchanged with an organization must be the genuine portrayal of the planned data without any kind of change.
Consent exception	The confidentiality regulations stipulate that the patient's health data can be consulted without the patient's approval, except in the event of a crisis or in the event of death and as determined by the patient.

5. Privacy and Security Issues of EHS

In this section, we have discussed many privacy and EHS security issues. The following figure provides a summary of EHS privacy and security issues.

Healthcare data and services issues: "sharing, integrity, confidentiality, delegation, heterogeneity and availability of data and services" are basic issues that require greater concern. Patient anonymity is one way to ensure the confidentiality of information exchange. However, we require a solution to ensure confidentiality, where patient identifiers and clinical proceedings are disclosed to an unapproved party [15]. Today, medical data comes from an assortment of sources. The kind of the data is diverse. Therefore, this data is unsuited and in unreliable formats. Therefore individuals need a basic stage where a different kind of information is presented in an acceptable structured format. A delegation is a procedure through which a person grants their own entrance to another client. Subsequently, the delegated user can execute all procedures on behalf of this user. In the EHS, the delegation is utilized when the patient is unable to make a conclusion. A solid set of rules should allow safe delegation [16].

Trust management: Trust management is also a major concern in the EHS, particularly when there is a disseminated structure in the EHS. All data and services are placed and managed remotely by third parties in EHS. Then, utilizing trust, an individual can handle and protect their information and facilities against unreliable clients [17]. Trust can affect not only users, but as well the "applications, services, storage devices, and security mechanisms" utilized to give safety.

Anonymity: EHS is an important issue of patient data security. The anonymity of health information is one of the solutions to ensure confidentiality and secure information against breaches of privacy [18]. It is a mechanism where communication segments cannot be identified with one another. This should be possible by "data anonymity, user anonymity, communication anonymity, disconnection ability and differential confidentiality" [19].

Access control issues: this is a mechanism that checks all requests to recognize the access decision. "Attribute-based (ABAC) and identity-based (IBAC)" techniques are normal access control methods utilized in EHS [20]. Because of a wide assortment of data and health facilities, this access control model does not fully meet EHS safety needs.

Authentication issues: Not only does an external attacker commit an authentication violation, but intruder can also pose a serious validation problem. Sometimes, to access various facilities, the client's needs a dissimilar login and credentials. To tackle this issue, Google gives a basic stage depends on XML authentication mechanism, provides authentication in various apps devoid of re-authentication. However, the proposed method can replace and imply the idea of system attacks [21].

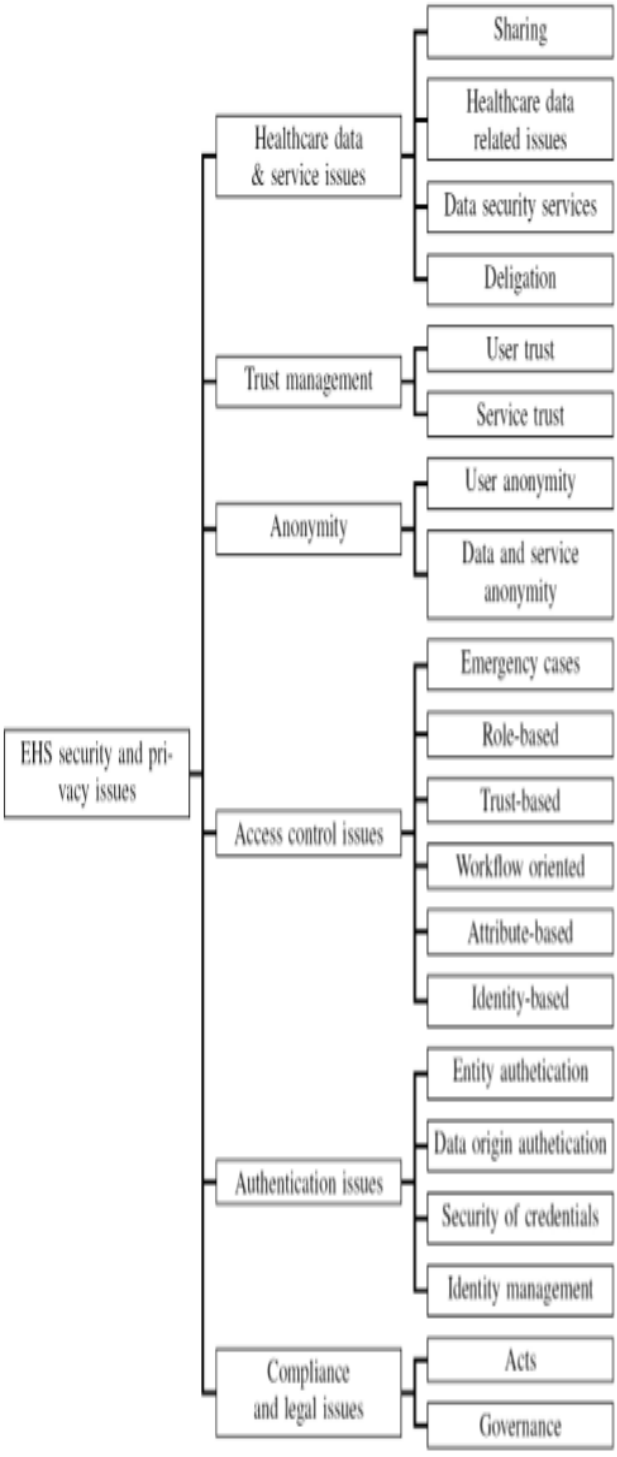

Fig.3 Security and privacy issues of EHS

Compliance and legal issues:

Both parties agreed and signed the terms and conditions of the services. In the EHS, cyber laws, forensic technology and the actions used do not ensure complete safety and confidentiality of patient data [22]. Interoperability issues, the issue of data format, the quality and the price of the business service are some of the basic questions that remain for the EHS government.

6. A Comparative Study of Literature Survey

The comparative study of privacy and security issues in EHS given in Table 2.

Table 2: A comparative study of literature survey

No.	Discussed Technique	Solution	Strength	Weakness	Reference
1	"Revocable-storage identity-based encryption (RS-IBE) "	Supports blocking of the identity and the update of the encrypted the text at the same time.	A practical and inexpensive data exchange system is possible. It also Offers forward and backward security.	Data Duplication	[23]
2	"Privacy preserving biometric identification scheme"	It can withstand a collusion attack propelled by clients and the cloud.	It is safe "even If attackers can fake identification requests and alliance with the cloud".	Need to trust the cloud service provider, Centralized data storage, computationally expensive for a real scale problem.	[24]
3	"Robust and efficient heterogeneous framework with single CA(Central Authority) and multiple AAs (Attribute Authorities) For public cloud storage"	Evacuate the problem of a single point execution bottleneck.	A monitoring mechanism that the system can use to track AA errors to verify the user's legitimacy. The bulky burden of checking user legitimacy shared by numerous AAs.	For the key generation and distribution must trust CA.	[25]
4	Attribute based encryption	Protects the confidentiality of data on storage servers. Enables fine-grained access control, Dynamic user management.	Maintains the name and detectability of the data provider.	The owner of the data for each public key requires that each authenticated user encrypt the data.	[26]
5	"Hybrid technique which includes query set size restriction and k-anonymity"	Inference control, Secures data from "inference attacks, linking attacks".	Hybrid solution is more profitable.	Need large dataset for experimental work.	[27]
6	"Context and Trust Aware Work flow Oriented Access Control model"	It highlighting on inter-component relationship to avoid performance bottleneck.	The Quality of context and trust with specific work flows for access control.	Access level is undefined.	[28]
7	End to end encryption technique	It improved the security when compared to the other methods by the handshake message and OTP based authentication process.	Enhanced the confidentiality and data integrity.	Difficult to handle large communication	[29]
8	Data perturbation based privacy technique	Secures sensitive information from inference attacks. The control of the data view protects against spoofing attacks.	It is secure and efficient for healthcare information.	Data view control restricts the users.	[30]
9	"homomorphic encryption and proxy re-encryption technique"	Address the subcontracted computation setup in the healthcare framework.	Proficient for computing encrypted data under various keys.	Needed cloud server with unlimited capacity and powerful computation functions.	[31]
10	"Privacy preserving disease prediction scheme (PPDP)"	Enables the cloud server to analyze patient infections without disclosing confidential data.	A Highly efficient technique for disease prediction and High level of privacy.	Computation complexity, communication cost increase with the increase in EHRs.	[32]

7. Open issues and challenges

Security issues and solutions are described in the previous section. This clearly shows that many security and privacy issues remain and more research is needed in this area. Cloud computing provides opportunities and challenges. Like all IT applications, the cloud has security issues. It typically operates in an open and shared atmosphere, which can lead to "data loss, theft, and malicious attacks". Poor cloud security is one of the key issues preventing the healthcare industry from fully embracing the cloud. There are many reasons why health professionals do not depend the cloud. For instance, you cannot manage medical records. Cloud providers typically collect their information from multiple data centers positioned in various geographic locations. This is an obvious benefit, "since data storage in the cloud will be excessive and, in the event of force majeure, multiple data centers will assist in disaster recovery". Then again, this can be a single benefit security challenge as there will be a higher risk of "theft and loss" of secure data in different locations. Over-all, using the cloud poses many security risks, such as "lack of segmentation of virtual users, identity theft, abuse of privileges, and poor encryption of certain security concerns". All the points discussed are the future improvement of EHS to deliver an entirely safe atmosphere.

8. Conclusion

Today, EHS is a more promising research area. Traditional technologies, in addition to new ones in EHS, attract users to adapt modern EHS. However, this can generate numerous security and privacy concerns. Realization of these threats to privacy and security will help for the extension of EHS. In this article, we discussed the architecture and services of cloud computing, as well as the structure of the modern healthcare framework. Next, we outlined EHS privacy and security requirements. The document then explores the discussion of security and privacy issues depend on the problem of "data and health services, trust management, anonymity, access control problem, authentication problem and legal and compliance problem". Finally, the document discussed a series of open issues and challenges, which will be useful for the researcher and the academy to emphasis on the matter.

References

[1] Altowaijri, S. M. (2020). An Architecture to Improve the Security of Cloud Computing in the Healthcare Sector. In *Smart Infrastructure and Applications* (pp. 249-266). Springer, Cham.

[2] Raju, G. D., Chandrakala, A., Kumar, A. P., & Reddy, M. P. R. R. (2017). END TO END ENCRYPTION BASED PRIVACY FOR MENTAL HEALTH CARE DATA TRANSACTION IN THE CLOUD. *International Journal of Engineering, Science and*, *6*, 1029-1034.

[3] Stantchev, V., Barnawi, A., Ghulam, S., Schubert, J., & Tamm, G. (2015). Smart items, fog and cloud computing as enablers of servitization in healthcare. *Sensors & Transducers*, *185*(2), 121.

[4] Youssef, A. E. (2014). A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments. *Int J Ambient Syst Appl*, *2*(2), 1-11.

[5] Mahalakshmi, M. V., & Shrivakshan, G. T. (2017). An Efficient Cloud Computing Security in Healthcare Management System. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(8), 185-192.

[6] Kumar, B. V., Ramaswami, M., & Swathika, P. (2017). Data security on patient monitoring for future healthcare application. *International Journal of Computer Applications*, *163*(6), 20-23.

[7] Abbas, A., & Khan, S. U. (2015). E-Health cloud: privacy concerns and mitigation strategies. In *Medical Data Privacy Handbook* (pp. 389-421). Springer, Cham.

[8] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

[9] Meena, S., & Gayathri, V. (2017). AN APPROACH TO SECURE MENTAL HEALTH DATA IN THE CLOUD USING END-TO-END ENCRYPTION TECHNIQUE. *Journal of Computer Engineering & Technology*, *8*(5), 87-98.

[10] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.

[11] Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal*, *20*(2), 97-108.

[12] Mahalakshmi, M. V., & Shrivakshan, G. T. (2017). An Efficient Cloud Computing Security in Healthcare Management System. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(8), 185-192.

[13] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-Health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.

[14] Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current

solutions. *Computers & Electrical Engineering*, *59*, 126-140.

[15] Yang, J. J., Li, J. Q., & Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation computer systems*, *43*, 74-86.

[16] Moon, J. K., Song, Y. J., & Kim, J. M. (2016). A Delegation Model of Healthcare System Based of AB-PRE in Fog Computing Environment. *Advanced Science Letters*, *22*(11), 3432-3436.

[17] Birkhäuer, J., Gaab, J., Kossowsky, J., Hasler, S., Krummenacher, P., Werner, C., & Gerger, H. (2017). Trust in the health care professional and health outcome: a meta-analysis. *PloS one*, *12*(2).

[18] Baek, S., Seo, S. H., & Kim, S. (2016). Preserving Patient's Anonymity for Mobile Healthcare System in IoT Environment. *International Journal of Distributed Sensor Networks*, *12*(7), 2171642.

[19] Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Kumar, N. (2018). A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Generation Computer Systems*, *80*, 483-495.

[20] Servos, D., & Osborn, S. L. (2017). Current research and open problems in attribute-based access control. *ACM Computing Surveys (CSUR)*, *49*(4), 1-45.

[21] Singh, A., & Chatterjee, K. (2019). Security and privacy issues of electronic healthcare system: A survey. *Journal of Information and Optimization Sciences*, *40*(8), 1709-1729.

[22] Berbée, R. G., Gemmel, P., Droesbeke, B., Casteleyn, H., & Vandaele, D. (2009). Evaluation of hospital service level agreements. *International journal of health care quality assurance*.

[23] Wei, J., Liu, W., & Hu, X. (2016). Secure data sharing in cloud computing using revocable-storage identity-based encryption. *IEEE Transactions on Cloud Computing*, *6*(4), 1136-1148.

[24] Zhu, L., Zhang, C., Xu, C., Liu, X., & Huang, C. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. *IEEE Access*, *6*, 19025-19033.

[25] Xue, K., Xue, Y., Hong, J., Li, W., Yue, H., Wei, D. S., & Hong, P. (2017). RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage. *IEEE Transactions on Information Forensics and Security*, *12*(4), 953-967.

[26] Cui, H., Deng, R. H., & Li, Y. (2018). Attribute-based cloud storage with secure provenance over encrypted data. *Future Generation Computer Systems*, *79*, 461-472.

[27] Kundalwal, M. K., Chatterjee, K., & Singh, A. (2019). An improved privacy preservation technique in health-cloud. *ICT Express*, *5*(3), 167-172.

[28] Bhattasali, T., Chaki, R., Chaki, N., & Saeed, K. (2018). An adaptation of context and trust aware workflow oriented access control for remote healthcare. *International Journal of Software Engineering and Knowledge Engineering*, *28*(06), 781-810.

[29] Raju, G. D., Chandrakala, A., Kumar, A. P., & Reddy, M. P. R. R. (2017). END TO END ENCRYPTION BASED PRIVACY FOR MENTAL HEALTH CARE DATA TRANSACTION IN THE CLOUD. *International Journal of Engineering, Science and*, *6*, 1029-1034.

[30] Kundalwal, M. K., Singh, A., & Chatterjee, K. (2018, October). A Privacy Framework in Cloud Computing for Healthcare Data. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 58-63). IEEE.

[31] Wang, Q., Zhou, D., Yang, S., Li, P., Wang, C., & Guan, Q. (2019, July). Privacy Preserving Computations over Healthcare Data. In *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 635-640). IEEE.

[32] Zhang, C., Zhu, L., Xu, C., & Lu, R. (2018). PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system. *Future Generation Computer Systems*, *79*, 16-25.