Analysis of Privacy and Security Challenges in e-Health Clouds

Reem Alanazi
Faculty of Engineering and Information Technology
University of Technology Sydney, Australia

***Abstract*—Electronic Health Records (EHR) techniques are being used at an increasingly faster rate to store the patient data making it easier to retrieve, share and utilize it efficiently. This data can be used for research purposes, clinical trials and for studying epidemiology to come up with strategies for epidemic control. With a huge global inflation, the increasing costs of healthcare and the shortage of medicine, it becomes convenient for the healthcare organizations to migrate from the traditional healthcare system to a more sophisticated, cost effective and efficient cloud-based e-Health model. To optimize the full potential of an ICT-based e-Health system, it is imperative for the existing healthcare systems to be implemented in a full-fledged cloud environment. However, with numerous benefits of technology, it might pose some privacy and security threats as well. Therefore, the security and access control of such information is of vital significance. Nonetheless, with the increasing interest of healthcare organizations to migrate from the conventional healthcare systems to the modern cloud-based e-Health systems, not much care is being taken to address security and privacy issues effectively towards the protection of sensitive data.**

Keywords*—*HER; e-health; security; privacy; cloud

I. Introduction

With the advancements in Information and Technology, services all across the globe have improved, in all fields in general, and around healthcare in particular, all due to several provisions like flexible processes and low-cost treatments. When healthcare is integrated with the internet it is termed as e-Health [1] [2]. This e-Health is the biggest innovation of technology and its implementation in a cloud-based environment is necessary to maximize the benefits. Despite all the benefits that e-health has been providing, it nevertheless still gets affected by certain challenges of privacy and security [1]. Since its conception, cloud computing has garnered enough popularity around the health sector. The cloud-based e-health makes the sharing of this health data with its stakeholders easier [3]. Although the internet by making use of technologies like cloud computing has made the concept of centralized healthcare possible, it has however brought in with it certain bugs and loopholes in the system. There are certain issues concerning security and privacy that remain unaddressed and unresolved even today [3].

The services that the e-health cloud offers are preventive care, keeping an account of patient satisfaction, a continuous vigil and AI supported detection. All these services are prone to privacy breach, and it needs to be taken care while rules regarding privacy measures are implemented. With the growth of use of technology among people, the awareness regarding privacy of their medical data has grown as well. Patients fear leak of their private medical history that they might be embarrassed of, to social media. It's important to maintain the trust of patients in health services providers, thus the e-health cloud needs to be highly secured [2] [9]. The centralization and digitization of the data in the health sector has made the sharing of medical data easy. However, this sharing might lead to data attacks and cause loss of confidential data. To tackle this, several government bodies have taken initiatives to ensure better security and proper privacy of data. Instances from the US healthcare industry show the progress that's been made in securing the e-health systems. The Health Insurance Portability and Accountability Act (HIPAA), which had guidelines set for security and privacy requirements of US healthcare, ensured proper utilization of e-health [1]. A secure e-health system ensures the system has these attributes; Authenticity, Integrity, Availability, Access control, Anonymity [4].

II. Literature Review

Several articles have been written and read about e-Health and its merits and demerits. The research has been done about what challenges are being faced in the pursuit of better security and maintaining privacy of data, and how these drawbacks can be addressed. Security models developed in relation with healthcare applications, targeted the information loss and ways to combat it. A security model, Role Based Access Control (RBAC) was deployed to find solutions for the already identified security challenges in electronic health [31]. An extended version of RBAC known as u-healthcare, was designed to carry out four vital functions: what meal should the patient take, exchange of information related to health, management of the same health information on smart devices that the records are accessed through. These studies however concluded not much could be resolved about these security issues. The model had several drawbacks, and it was not suitable for disturbed environment. The solution offered had limited application. It was not scalable to any number of users.

Another model developed by [32] demonstrated the working of a comparatively lightweight framework that was based on Transport Layer Security/Secure Sockets Layer (TLS/SSL) to secure the data shared between the server and client. This framework was called Secure Health and it had many security features like proper authentication, and authorization for the transmitted and stored data. It protected the system from unidentified and unauthorized access minimizing alien access to confidential health data. It also

helped the administrator in identifying wrongly stored information [33]. Despite all the benefits that the system offered, some challenges remained unresolved, the main one being its platform dependency and no or less scalability. In cloud computing, scalability is the most sought feature. The systems based on cloud should have provision for an expansion in future. In the need to minimize the cost of maintaining the health data and for keeping it available but secure, another security mechanism with a different concept of hierarchy was given by Barua, et al. This model adopted the theory of Attribute Based Encryption (ABE). It had provision for access control, which was framed at the central level. However, even this approach failed at addressing a large number of requests from the client side because of the centralized manner in which the health data was stored in [34]. In case of many users accessing the system at once, the requests needed to be sorted out depending on their priorities. To overcome the challenges caused due to the centralization of data, other attributes like collaborative and distributive nature of the e-health systems were taken in consideration by Guo et al. [35]. They brought about a change in the way requests were being addressed and servers being accessed. They suggested authorization from both the patients and the doctors, and not from the centralized server itself. Clients were given access only on the basis of priorities concealing their identities and characteristics. Hamid et al. worked on the confidentiality of patient's multimedia data in the cloud. They proposed a bilinear pairing cryptography based triparty one-round authenticated key agreement protocol. This protocol helps in secure communication by generating a session key. Also, a decoy technique with a fog computing facility has been implemented so that the private healthcare data can be accessed and secured securely. This approach induces computational expenses in communication for strong security [10-15]. Marwan et al. proposed a new method to enhance the reliability of cloud storage and used Shamir's Secret Share Scheme (SSS) and multi cloud concept. This was done to meet security requirements, avoid data loss, and prevent unauthorized access and privacy disclosure. To prevent medical records from getting leaked and revealed, this technique allows division of the data into small shares. Also, data is spread among various cloud storage systems. Medical Data is encrypted using SSS technique and split into shares to ensure confidentiality and privacy. This article has not discussed any aspect of the optimal number of shares aroused to tradeoff between efficiency and security [16, 17]. Galletta et al. have proposed a system developed at Instituto di Ricovero e Cura a Carattere Scientifico (IRCCS) claiming to address security and privacy of patient's data [18]. This system works on two software parts: the splitter and anonymizer. The anonymizer collects anonymized clinical data and the splitter obscures and stores health data in multiple cloud storage providers. This data can be accessed by only authorized clinical operators. Moreover, the performance of the system has been assessed by magnetic resonance imaging (MRI) data. Alexander et al. proposed anonymization techniques and privacy-aware systems in order to publish data on the cloud. This system used Advanced Encryption Standard (AES) and k-anonymity [19-21]. Smithamol et al. proposed a novel architecture to address data confidentiality. This model constructed the group-based access structure and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) by making use of the partially ordered set, thereby providing medical records access control. This approach reduced overall encryption time and computational overhead [22] [23]. Ibrahim et al. provided a solution to access securely the privacy-sensitive EHR data through: 1) a cryptographic role-based technique for the distribution of session keys with the help of Kerberos protocol, 2) location and biometrics-based process for user authorization, and 3) a wavelet-based steganographic technique for embedding EHR data securely. This approach showed resilience to man in the middle attack and replay attacks. However, it did not show resilience to other security threats and did not analyze its scalability [24]. Shah and Prasad deployed a novel structure with cloud-based privacy-aware role-based access control (CPRBAC) model. This model presented a list of different methods of encryption and various privacy, and security challenges were addressed. Its goal was to minimize computational complexity. However, no qualitative analysis was carried out to check the efficiency of the approach [25]. Supriya and Padaki surveyed various lapses in health care security particularly concerned with non-repudiation, CIA model. They studied and discussed some already proven operational strategies and methodologies related to risk management. This way they were able to perceive what the health industry must follow to reduce security and privacy threats [26]. Lohr et al. tried to establish privacy domains in e-health infrastructures by presenting a security architecture based on Trusted Virtual Domains (TVDs). This architecture, however, did not address other research challenges like anonymity, non-repudiation, incapacity of the patient to authenticate [27, 28]. Kumar et al. proposed a model based on encryption technique called Attribute Based Encryption (ABE). All the users have been divided into two domains: personal and public. This is done to control key management complexity. In the personal domain, a user can encrypt data that is allocated to him whereas in the public domain, a user can adopt and utilize multi-authority ABE. Scalability and flexibility are the two challenges associated with this approach as integrating ABE into the EHR system gives rise to serious and key management challenges [29]. Zhu et al. proposed a model that utilized re-encryption and Attribute Based Encryption (ABE) with proxy encryption which is enabled by Rivest Shamir and Adleman (RSA). The whole purpose of using proxy encryption was to induce a separation mechanism to validate the patient's data. Write privilege keys were given to professionals whereas read privilege keys were given to patients. Using this model, computation overhead was minimized. The healthcare worker can be easily stopped from getting the read keys and this does not need to be approved from both ends. Moreover, this framework can be accessed by only a few users [30].

III. WHAT IS E-HEALTH

The concept of conventional healthcare has been narrowed down to virtual healthcare. The integration of technology with healthcare has emerged as a new concept termed as e-health. In an era like today time management is the need of the hour. Going to doctors for consultations and waiting in queues for hours is an obsolete scene now. With the internet and

technology being used in all walks of life, people prefer a virtual way of seeking medical treatment. The process of having consultations online, using desktops and laptops is e-Health [5]. This cloud-based e-health system can be created specifically according to the needs of the patient. Also, healthcare accessed via mobile phones is m-health which is mostly for self-management of chronic diseases. The e-Health systems have been of great help in dealing with patients who had prolonged diseases and needed to be kept constant vigil. These e-Health systems keep a track of health-related information and provide help with symptom checking, finding a suitable doctor, managing financial records, self-monitoring, and filling prescriptions. This information is available and accessed by a large population [5]. E-health has now become a vital part of the healthcare system due to its efficient services and accurate results, and error free unlike the traditional healthcare systems. In a traditional way of treatment, a patient could get a particular dose of medicine twice due to manual handling of records. This is not the case with health where electronic medical records are maintained, which store all the information about the patient's treatment and medicines given, thus avoiding any errors with the medication of the patient [6]. A country's success of e-Health is derived from many factors like what type of management and infrastructure is being used, how much is the user involvement, if the system is scalable to adapt to as many users as possible or not. The medical data in the cloud is of importance to its healthcare professionals, patients, entrepreneurs, and businesses which deal with health insurances or such policies. E-health strategies like norms, laws and regulations must be created to implement cloud technology in healthcare effectively. It is not just another progress in the field of technology, it is a way of thinking, state of mind, to increase the reach of healthcare, improving local, regional and global healthcare by making use of ICT (Information and Communication Technology).

As the name suggests the e-Health uses electronics which can be mobile phones or computers along with cloud technology for storage purposes. The eHealth is mainly of two types: Personal Health records (P-HR) and Electronic Health Records (E-HR). The P_HR is used by patients to update their health records themselves and for seeking consultations online by using mobile phones. Whereas E-HR is of use to healthcare professionals. This E-HR is very beneficial in providing the right treatment to the patient and for secure sharing medical records or patient medical history, medicine details and prescriptions. E-health provides an effective and real time treatment for the patient.

IV. Cloud based e-health Models

1) Private cloud: Model given in Fig. 1 is the most secured model. It is usually operated and managed by the same organization that uses it, making it highly secured and hence security issues are limited. It is located on premises, over the intranet and behind the firewall. In this, the public internet is completely restricted. Only recognized personnel from the healthcare institution are able to access the electronic medical record (EMR). Only these personnel are considered to be trustworthy and reliable. A good example is VMware [1] [4].

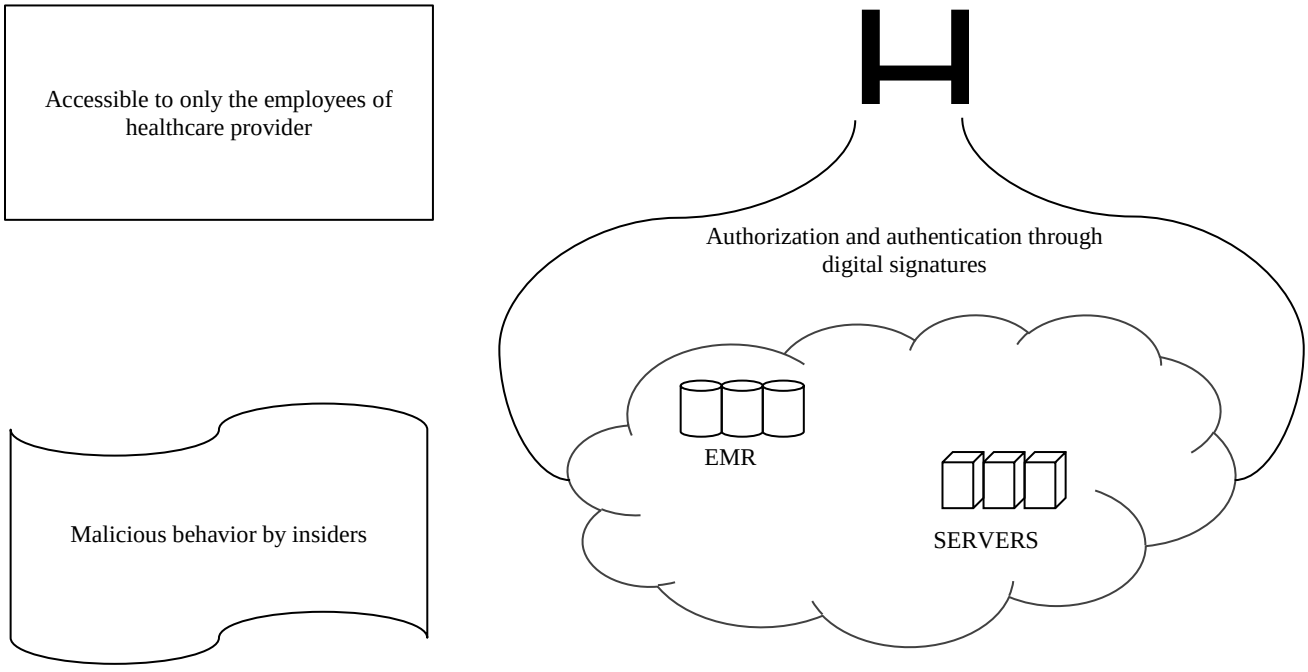

Fig. 1. Private Cloud.

2) Public cloud: This model given in Fig. 2 is totally in control of the third-party provider as the services of the cloud system are provided by them only. They are known as cloud service providers (CSPs). It is located off premises, over the internet controlled by CSPs. In this, EHRs are held between various organizations and these EHRs are highly vulnerable to malicious attacks. It has many security challenges associated with it and to avoid them, efficient cryptographic mechanisms and fine-grained access control frameworks need to be applied. It is considered less secure than the private cloud. Some good examples are Dropbox, Amazon EC2, Microsoft Azure [1] [4].

3) Hybrid cloud: Model given in Fig. 3 is a combination of public and private cloud servers where both works individually but unitedly. The deployment of this model combines the benefits of both the models and multiple cloud services can be used. This model is highly advantageous to e-health and plays an important role in integration, composition and organizational impact and housing big medical data. Health care providers that have restricted and limited resources can easily deploy this model which makes use of third-party services. There is a huge importance of hybrid cloud in health care but at the same time there is a need of effectively implementing hybrid cloud in e-health as it has trust and confidentiality issues because of the public part. An important example is Rackspace [1] [7].

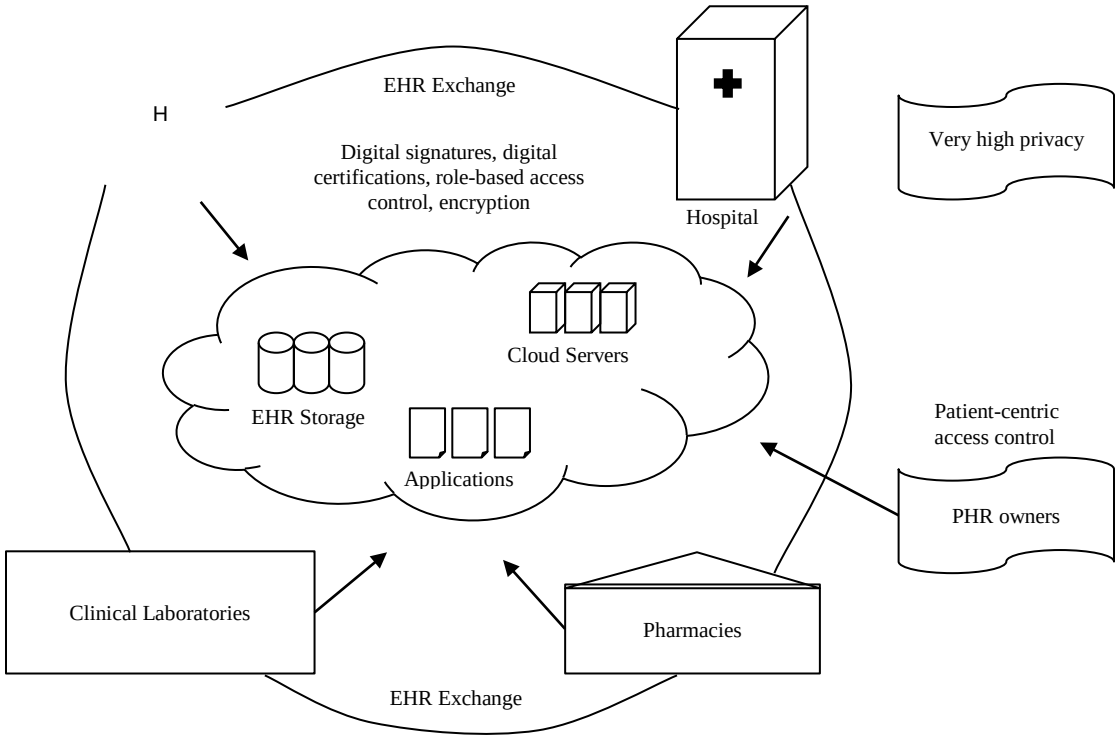

Fig. 2. Public Cloud.

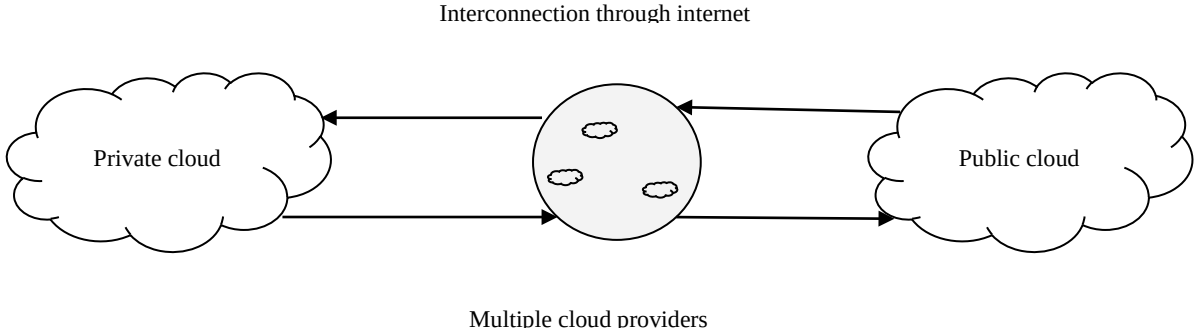

Fig. 3. Hybrid Cloud.

V. Privacy and Security Requirements

It is a known fact that transition of conventional health care systems to e-health care has brought with it a lot of benefits and has made health care systems easier and affordable but there are a lot of challenges associated with it like confidentiality, privacy and security of patients' records. Cloud computing is highly acceptable in digital technology which is being used in the healthcare industry extensively [8]. In order to increase the confidence of patients and organizations, the cloud service providers and other government organizations have formulated a range of security measures and guidelines. Cloud servers have been broadly classified into three categories: trusted, semi-trusted, and untrusted. A trusted server can be defined as the one that can be trusted completely. It doesn't lead to any information leak and threats to the health data. Semi trusted servers are those that are considered to be honest but curious servers. They conspire with malicious users to acquire health data. Untrusted servers cannot be trusted and are highly vulnerable to attacks.

In e-health system there is a need of security and privacy in the following ways:

1) Data integrity: It is a mechanism which ensures health data is not being altered by an unauthorized entity.

2) Data confidentiality: It is a mechanism which ensures that the sensitive health information does not reach unauthorized users. Data confidentiality is achieved by data encryption.

3) Authenticity: It is a mechanism that ensures sensitive health data is accessed by only authorized and authentic authority.

4) Accountability: It is a mechanism to justify the actions and decisions of organizations and individuals.

5) Audit: It keeps the track of any kind of activity on the health data and is continuously monitored and protected. It also ensures data privacy and security.

6) Non-repudiation: It refers to the sender and receiver's non denial of authenticity. It means, neither patients nor doctors can repudiate health data after its theft.

7) Anonymity: It is a mechanism which keeps the identity of the users anonymous so that the cloud servers are unable to access the stored health data.

VI. Conclusion

The security and privacy of patient data in e-Health systems is quite a demanding task. Researcher is being carried out internationally to provide and protect the Electronic Health Records (EHR) data. To mitigate the hurdles of security and privacy challenges, it is essential for health organizations to migrate from the traditional e-Health systems to the advanced cloud-based e-Health systems. While migration towards the cloud-based infrastructure protects the patient data in EHRs to a larger extent, it, however, does not guarantee the full-proof security and protection against data theft and other type of threats and vulnerabilities. An in-depth analysis has been done in this perspective. Firstly, an attempt has been made to understand the requirement of shifting from traditional e-Health systems to cloud-based infrastructure. A survey has been carried out to highlight the privacy and security considerations prevalent in the cloud-based e-Health systems [8]. More than 30 research papers were analyzed to highlight the underlying security and privacy issues in various cloud-based e-Health systems across the globe. Some security techniques with their pros and cons have also been presented. Finally, some recommendations have been made for enhanced privacy and protection in the cloud-based e-Healthcare infrastructure. For the future research, we are looking forward to exploring the state-of-the-art techniques for preserving privacy especially in terms of EHR data in the cloud infrastructure scenarios.

VII. Future Directions

There has been a tremendous development and progress in security and privacy in e-health clouds. Still, there is a need to enhance and enforce certain security and privacy measures in the e-health system. This can be done by enhancing and maintaining efficiency of all the initiatives regarding security and privacy.

Some of the strategies for security purpose in e-health are mentioned below:

1) Auditing is the first thing in assuring security and privacy in e-health. This approach greatly helps in locating and identifying any kind of wrongdoing in the e-health system. Hence, auditing can be regarded as a new research direction for e-health.

2) Encryption schemes can also help in achieving security and privacy. Encrypting information that has the data regarding e-health users will in no way lead to insecurity of data. This is an excellent procedure as the other parts of information remain unencrypted.

3) RBAC is a model that has been put into use in order to address the issues of security and privacy in e-health. Also, Attribute Based Access Control (ABAC) model is widely used to ensure remarkable scalability and flexibility for authorizations and authentications.

4) Attribute Based Encryption (ABE) is an exceptional way to ensure privacy in e-health. But the performance is affected while decrypting data because of bi-linear pairing operations. These bi-linear operations require a solution to strengthen the efficiency of ABE.

5) General enforcement needs to be adopted to ensure privacy. Privacy must be incorporated in e-health that benefits all the parties. Also, research must be done to know about the security and privacy violations.

6) Most of the solutions adopted RBAC, MAC, and DAC. These models can ensure better results of security and privacy when applied collectively or hybridized into a single model.

REFERENCES

[1] N. A. Azeez, & C. V. der Vyver, (2018). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal. doi:10.1016/j.eij.2018.12.001.

[2] C. B. Pheng, K.H. Yeh, & H. Xiong, (2020). Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. Symmetry, 12(7), 1191. doi:10.3390/sym12071191 XX.

[3] S. Aqeel et.al(2021).A Review of the State of the Art in Privacy and Security in the eHealth Cloud, Doi:/10.1109/ACCESS.2021.3098708,IEEE Access.

[4] Y. Al-Issa, M. A. Ottom, & A. Tamrawi, (2019). eHealth Cloud Security Challenges: A Survey. Journal of Healthcare Engineering, 2019, 1–15. doi:10.1155/2019/7516035.

[5] L. Leung, & C. Chen, (2019). E-health/m-health adoption and lifestyle improvements: Exploring the roles of technology readiness, the expectation-confirmation model, and health-related information activities. Telecommunications Policy. doi:10.1016/j.telpol.2019.01.005.

[6] M. H. da Fonseca, (2021). E-Health Practices and Technologies: A Systematic Review from 2014 to 2019 ,doi:. https://doi.org/10.3390/ healthcare9091192.

[7] H. Kunwal, B. H. Malik, A. Saeed, H. Mushtaq, H. B. Cheema, F. Mehmood, (2017). "Medicloud: Hybrid Cloud Computing Framework to Optimize E-Health Activities", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 9, 2017.

[8] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker (2019), "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing", IEEE, 2019.

[9] D. K. Yadav, S. Behera, (2020). "A Survey on Secure Cloud-Based E-Health Systems",: doi: 10.4108/eai.13-7-2018.163308.

[10] 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, vol. 5, 2017.

[11] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," Cryptography and Coding, vol. 3796, pp. 13–36, 2005.

[12] J. Voris, J. Jermyn, A. D. Keromytis, and S. J. Stolfo, "Bait and snitch: defending computer systems with decoys," in Proceedings of the Cyber Infrastructure Protection Conference, Strategic Studies Institute, Arlington, VA, USA, September 2013.

[13] S. P. Karekar and S. M. Vaidya, "Perspective of decoy technique using mobile fog computing with effect to wireless environment," International Journal of Scientific Engineering and Technology Research, vol. 4, no. 14, pp. 2620–2626, 2015.

[14] J. Shropshire, "Extending the cloud with fog: security challenges & opportunities," in Proceedings of the Americas Conference on Information Systems, AMCIS 2014, Savannah, GA, USA, August 2014.

[15] K. Manreet and B. Monika, "Fog computing providing data security: a review," International Journal of Computer Science and Software Engineering, vol. 4, no. 6, pp. 832–834, 2014.

[16] M. Marwan, A. Kartit, and H. Ouahmane, "Protecting medical data in cloud storage using fault-tolerance mechanism," in Proceedings of the 2017 International Conference on Smart Digital Environment, pp. 214–219, Rabat, Morocco, July 2017.

[17] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[18] A. Galletta, L. Bonanno, A. Celesti, S. Marino, P. Bramanti, and M. Villari, "An approach to share MRI data over the Cloud preserving patients' privacy," in Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC 2017), pp. 94–99, Heraklion, Greece, July 2017.

[19] E. Alexander and Sathyalakshmi, "Privacy-aware set-valued data publishing on cloud for personal healthcare records," in Artificial Intelligence and Evolutionary Computations in Engineering Systems, pp. 323–334, Springer, Berlin, Germany, 2017.

[20] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 571–588, 2002.

[21] M. Terrovitis, N. Mamoulis, and P. Kalnis, "Privacy-preserving anonymization of set-valued data," Proceedings of the VLDB Endowment, vol. 1, no. 1, pp. 115–125, 2008.

[22] M. B. Smithamol and S. Rajeswari, "Hybrid solution for privacy-preserving access control for healthcare data," Advances in Electrical and Computer Engineering, vol. 17, no. 2, pp. 31–38, 2017.

[23] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributebased encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98, Alexandria, VA, USA, October 2006.

[24] B. Dhivya, S. P. S. Ibrahim, and R. Kirubakaran, "Hybrid cryptographic access control for cloud based electronic health records systems," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 2, 2017.

[25] K. Shah and V. Prasad, "Security for healthcare data on cloud," International Journal on Computer Science and Engineering (IJCSE), vol. 9, no. 5, 2017.

[26] S. Supriya and S. Padaki, "Data security and privacy challenges in adopting solutions for IOT," in Proceedings of the 2016 IEEE International Conference on Internet of Cings (iCings) and IEEE green Computing and communications (GreenCom) and IEEE cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 410–415, Chengdu, China, 2016.

[27] H. Lohr, A.-R. Sadeghi, and M. Winandy, "Securing the ¨ e-health cloud," in Proceedings of the ACM international conference on Health informatics—IHI'10, pp. 220–229, Arlington, VA, USA, November 2010.

[28] J. L. Griffin, T. Jaeger, R. Perez, R. Sailer, L. Van Doorn, and R. Caceres, "Trusted virtual domains: toward secure dis- ´ tributed services," in Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability (HotDep'05), pp. 12–17, Yokohama, Japan, June 2005.

[29] M. Kumar, M. Fathima, M. Mahendran, 2013, "Personal health data storage protection on cloud using MA-ABE", Int J Comput Appl 2013;75(8):11–6.

[30] H. Zhu, R. Huang, X. Liu, H. Li, SPEMR: A new secure personal electronic medical record scheme with privilege separation. In: 2014 IEEE International Conference on Communications Workshops (ICC), Sydney, NSW, Australia, 2014, pp. 700–705.

[31] M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, & S. P. Jeong, (2015). Constructing RBAC Based Security Model in u-Healthcare Service Platform. The Scientific World Journal, 2015, 1–13. doi:10.1155/2015/937914.

[32] N. A. Azeez, A. A. Lasisi, 2016. Empirical and statistical evaluation of the effectiveness of four lossless data compression algorithms. Nigerian J Technol Dev 2016;13 (2):64–73.

[33] M. Simplicio, L. Iwaya, B. Barros, T. Carvalho, M. Naslund, 2015, SecourHealth: a delay tolerant security framework for mobile health data collection. IEEE J Biomed Health Inform 2015;19(2):761–72.

[34] M. Barua, R. Lu, X. Liang, X. Shen, 2011. PEACE: An Efficient and Secure Patient Centric Access Control Scheme for eHealth Care System. In: The First International Workshop on Security in Computers, Networking and Communications, Shanghai, China, 2011, pp. 970–975.

[35] L. Guo, C. Zhang, J. Sun, Y. Fang, 2012. PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks. In: 2012 32nd IEEE International Conference on Distributed Computing Systems,Macau, China, 2012, pp. 224–233.