Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

Cloud Computing in Healthcare - Investigation of Threats, Vulnerabilities, Future Challenges and Counter Measure

Sara Asif[1], Mushk Ambreen[2], Zia Muhammad[3], Hameed ur Rahman[4]
[1]Department of Cybersecurity, Air University Islamabad-Pakistan (sara.asif@mail.au.edu.pk)
[2]Department of Information Security, MCS-NUST, Pakistan (mushkhumera@yahoo.com)
[3]Department of Cybersecurity, Air University Islamabad-Pakistan (zia.muhamma@mail.au.edu.pk)
[4]Department of Creative Technologies, Air University Islamabad-Pakistan (rhameedur@gmail.com)

DOI: 10.5281/zenodo.6547289

ABSTRACT

The use of cloud computing has gradually increased over the last decade. Healthcare provision has become more scalable, efficient, and effective through the cloud-based healthcare paradigm. This flexibility of emerging computing services has opened many possibilities for health organizations that did not exist before. But with that, security and privacy concerns have also increased. With this massive rise and adoption of cloud architecture in healthcare, it's unclear how this paradigm shift is affecting the smart healthcare industry, which is varied, complicated, and distinctive. There is a need for auditing and evaluation of cloud services evolving in the health sector. In this paper, we explored the contemporary state and trends of healthcare by conducting a comprehensive survey to identify potential risks, vulnerabilities, and threats associated with the cloud computing platform. Moreover, cloud platforms like Secure G-Cloud, Pixel Conversion, tiers-based Cloud, and Cloud-of-Things have been discussed. Finally, threats have been classified and mitigation, possible alternatives, and counter-stones have been proposed in order to eliminate identified threats.

Keywords: Cloud Computing, Cloud Security, Healthcare, Fog Computing, Edge Computing, Telehealth, Cloud in Healthcare.

Cite as: Sara Asif, Mushk Ambreen, Zia Muhammad, Hameed ur Rahman, SZ Iqbal5. (2022). Cloud Computing in Healthcare - Investigation of Threats, Vulnerabilities, Future Challenges and Counter Measure. LC International Journal of STEM (ISSN: 2708-7123), 3(1), 63–74. https://doi.org/10.5281/zenodo.6547289

INTRODUCTION

The Healthcare system has changed widely with the use of the present information technology in both developed and underdeveloped countries across the globe. For the past few years, cloud computing has been serving as a paradigm of computing with a centralized body to control and govern network and end devices. In the healthcare industry, cloud computing has brought smart transformations and has changed the conventional healthcare system. Smart healthcare systems (SHS) have provided control to healthcare providers and patients control over their health records via smart devices [1]. Over time many solutions with different implementation models in the cloud have been introduced for secure smart healthcare [2].

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

Cloud computing was a great architecture till the end devices were not much powerful. Now end devices possess a great amount of storage and processing capabilities.
Rapid advancement in technology and agile growth of networks has brought some serious challenges to cloud computing, for which cloud computing was never made to be faced. Therefore, cloud computing architecture felt a bit lacking in the methodology.

Cloud is implemented as a centralized body to maintain control but it is also a single point of failure if comprised all the devices are unable to access resources [3]. The edge devices are more computationally powerful than ever before which makes the cloud even more vulnerable to DOS and DDOS attacks [4]. Since the health records come under the domain of sensitive data, breach of privacy and confidentiality can be a big concern in CC. Cloud computing architecture is usually secured using IDS, NIDS, and SIEM solutions [5]. These security solutions are signature-based which means they have to compare all the incoming traffic with the saved signatures in the database. Cloud computing has three different service models: Software as a service (Saas), Platform as a service (PaaS), and Infrastructure as a service (IaaS) [6]. A quick overview of models is visualized in Fig. 1.

Similarly, cloud infrastructure has three main actors having access to data. There exist some evaluation schemes for the security assessment of Cloud products [7]. Among all, these actors include users of the system (patients, healthcare providers, system administrators), cloud service providers, and third-party owners (insurance companies). A smart healthcare system associated with data under surveillance is divided into seven sub-assets that are associated with medical records [8]. Details of these assets are as follows:

1. Users' Personal Data (Critical and Noncritical)
2. Patient Health Record (Medical History)
3. Real-time Service Delivery (Availability)
4. Intellectual Property (Sole ownership)
5. Access Control/Authorization Credentials
6. Network (Connection, Networks, API)
7. Physical (Hardware, Software, Backup server)
8. CSP management (Cloud Service Platform)

We spend our time and efforts on critical analysis of cloud computing and its rapid adoption in healthcare.

In this regard, we thoroughly reviewed the working of the cloud network with health sectors and explored its trend in the past and present. This is done by conducting a comprehensive survey of vulnerabilities, risks, and threats associated with the cloud infrastructure. Moreover, competitive analysis is added to possible alternative technology of cloud computing like Fog and edge. Afterward, after a detailed analysis, we provided counter-stones and mitigation techniques that can be used to eliminate identified threats that are directly applicable to smart healthcare.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

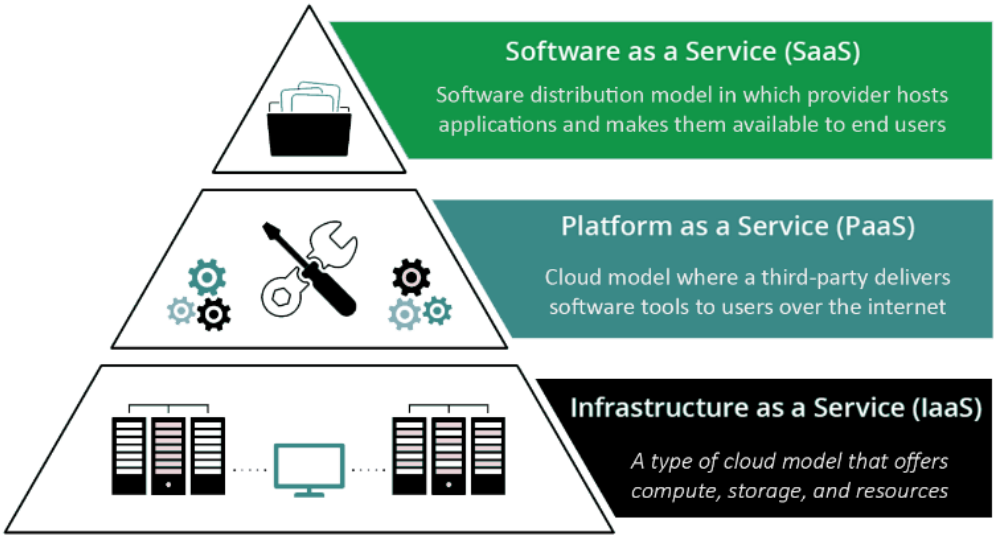

Figure 1: Models of Cloud Computing

Organization of the Paper

The paper is organized in the following sections as Section II contains a comparative study of existing literature associated with the selected domain. Section III provides a list of healthcare considerations before the actual implementation of the cloud in healthcare. Section IV covers hazards associated with cloud architecture. Section V provides details about counter-stones and a mitigation technique that can be used to eliminate potential threats. Finally, the conclusion and future work has been added.

LITERATURE REVIEW

Due to the novelty of our domain, we found comparatively less literature associated with our work. Major contribution in recent years has been discussed. The section provides a reference to past work that has been done in the field of cloud and the smart healthcare system. Moreover, in ensuring paragraphs we added true advantages and shortcomings of past efforts. The main requirements when developing security and privacy for Smart Healthcare System (SHS) include satisfying data semantic standards without unauthorized tampering, 24/7 availability of data to users, authorized use of data, and secure data transmission. Devi and Manju [9] proposed a framework that can recognize patients' privacy for health records in CC.

In this process of recognition, the patients were asked to encrypt the data by themselves via encryption schemes. Similarly, researcher Divya [10] proposed a system to improve the efficiency of the treatment of patients by providing an environment where the patients' records are stored in a place that is referenced by the doctors. The system was designed to handle the patient's history across the country by storing their records in a single shared place. Glasper [11] claimed that high companies such as Apple, Amazon, and IBM have started entering the medical space and partnering with healthcare providers to offer medical solutions for the modern patient C.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

Wang et al [12] explored secure outsourcing for widespread large-scale systems of linear equations, which happen to be the most known computational tool and algorithm in engineering, used for the optimization of present systems. Jin li et al [13] proposed a Fuzzy keyword search for encryption of data over cloud computing. Craig Gentry et al [14] in their paper have proposed a fully Homomorphic scheme that practices the processing of data without giving access. Ming Li et al [15] have proposed a patient-centric framework for controlling data access to personal health records stored in trusted servers.

A. Secure G-Cloud Based Framework

Sana and Nidal in their paper introduced a framework that aimed to provide health facilities and services from government to citizens by benefiting from the electronic government cloud-based project Yasser [16]. The proposed system ensured the privacy and security of data in the cloud. In order to provide so, access control policies were enforced by multi-authority CP-ABE. With that multifactor user, authentication ensured no computational overhead on the system. A high level of interoperability and integration of data and services among healthcare providers was achieved in the proposed system.

B. Pixel Conversion based Framework

R. Aiswarya et al. in their paper proposed a framework based on the pixel conversion method. In an application scenario of healthcare with cloud computing, the framework seemed appropriate because it securely harnessed the cloud for big-scale problems. Results and security analysis demonstrated the practicality and validity of the framework in cloud-based healthcare. In order to provide security in the system asymmetric cryptosystems of homomorphic encryption i-e, Paillier Cryptosystem is used [17].

C. Three Tiers-Based Cloud Framework

Sumon and et al in their paper proposed a framework based on a three-tier with a data mining approach to make the e-health-based systems better [18]. The system consisted of a Logic layer, SimpleDB sensor, and client based on the rich internet application. The user connects with the system via a rich internet application, then a cloud server i-e SimpleDB by amazon, which will provide a platform for user parties to integrate. The logic layer is the one that will implement rules for the system; it will reside between user and server. Rules of application and transaction logic, web service, data query, and data security are maintained and implemented by this layer.

D. Cloud-of-Things Based Framework

Ahead et al in their paper proposed a framework that integrated cloud computing and the internet of things thus named Cloud of Things [19]. The paper widely discussed the new platform and its implementation in healthcare. Energy efficiency and quality of service in CoT in healthcare were enlightened by the proposed framework.

HEALTHCARE CONSIDERATIONS IN CLOUD INFRASTRUCTURE

This section provides a list of the key requirement that must be filled before compliance with cloud computing in smart healthcare systems. To full fill the requirements of the Health Insurance Portability and Accountability Act (HIPAA) it is required to comply with CIA traits i.e. Confidentiality, Integrity, and availability of medical records. Fig. 2 provides a quick overview of associated terminologies. Confidentiality implies to ethical principle or legal right of a physician or other health practitioner to keep all information about a patient confidential until the patient consents to dissemination.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

The key aspects that reside in this domain are as follows:

- Confidentiality of medical records.
- The anonymity of patients and healthcare providers.
- Need to know the base rule for medical health records.
- Ownership of medical health records.
- Suspension of access to records when not needed.
- Unlinkability i-e no link between identities, users, and records for unauthorized users.
- No access to authorization/ authentication/admin credentials/encryption keys of the system.

Integrity in healthcare can be defined as honesty in maintaining one's medical records, and continuously adhering to professional standards, especially when it is difficult to do so. The key points indulge in integrity are as follows:

- The integrity of medical health records of the patient.
- Detection and prevention against data tampering attacks and violations of system.
- The system should validate and authenticate the user on every login request made by a legitimate person or attacker.
- Ensure non-repudiation i.e, access to the system by the user cannot be denied in any case.
- Ensure intellectual property rights.

The term "availability" refers to a sufficient restricted and adequate providence of required information to health workers with the necessary competencies and skills according to international standards for the population's health requirements. In this regard, competencies, abilities, knowledge, and behavior of the health workforce must be measured by professional norms and as seen by users.

- Real-time service delivery is something that is most valued when it comes to the requirement for the working of the system regardless of system failures.
- Up to date data/system should be readily available.
- Restoration and recoverability of stored data in case of any system failure, system crash, or natural disaster.
- The efficiency and usability of the system is a must.
- Secure transmission of data on communication channel.

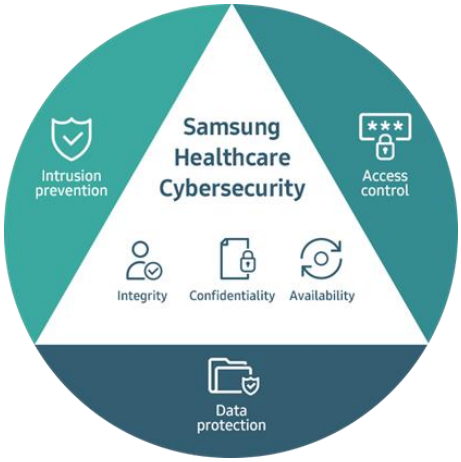

Figure 2: CIA Traits for Smart Healthcare

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

To ensure patient record safety, this should be compulsory for smart healthcare organizations to must comply with dis- cussed three triads i.e. confidentiality, integrity, and availability of data before the actual adoption of cloud.

HAZARDS ASSOCIATED WITH CLOUD ARCHITECTURE

This section provides details about challenges faced by cloud platforms including privacy, scalability, usability, and Data ownership. Moreover, a huge list of threats and vulnerabilities identified in the entire research phase has been added.

A. Challenges of Cloud Infrastructure

Security and Privacy: The SHS involves multiple stakeholders and actors in order to function. Threats are associated o every asset which we will discuss in detail in the paper. Treatment and elimination of the risk associated with every asset to secure the CIA triad is a challenge.

Data Management and Scalability: A good deal of structured and non-structured data will keep on adding to the cloud database, so data backups need to be located at geographical distances for better access and higher availability. In order to cater to the high traffic jams SHS should be able to scale itself without any delay or failure [20].

Usability: Acceptable user experience and usability of SHS have to be thoroughly considered to entirely exploit the potential of smart healthcare applications along with catering to the aspects of technical feasibility. [21]

Quality of Service and Inter-operability: QoS needs to be on point since no margin of error exists in SHS regarding operation and services. Easy data migration and interoperability is required between primary and secondary cloud service providers i-e multi-tenancy.
Availability: Confidentiality Integrity Availability Cloud Security CC resources and services must be drafted and designed for quick restoration and reliability. In order to provide error-free services and fast restoration, perfect testing models need to be implemented in SHS. 24/7 365 days is goal.

Data ownership and Legislation: Medical records are the absolute property of the patient, healthcare provider, hospital, and insurance body. An area of concern that has to be addressed is compliance with data privacy laws and the cross-border flow of information. In clouds, infrastructure needs to be fully imposed obligations based on patients' confidentiality and consent agreements between them and healthcare providers. Data classification and sharing among different parties arise challenges. If standards like HIPPA are not implemented the integrity of SHS cannot be fully assured.

B. Threats and Vulnerabilities

Threats and Vulnerabilities associated with Cloud Infrastructure and Smart Healthcare systems are identified against each asset. There are four major categories of identified threats i.e, data threats, network threats, cloud-specific threats, and other miscellaneous threats. Table. 1 provides details of these 4 categories along with their subcategories. Moreover, seven sub-assets associated with medical records are also mapped and in fourth column.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

Table 1: CLASSIFICATION OF THREATS ON CLOUD INFRASTRUCTURE

Threats	Threat No	Type	Details/ Affected Asset	Category	Vul. No	Vulnerability Associated
Data Threats	T1.1	Data Breach	Unauthorized access to sensitive information due to poor access control and security control. (A1,A2,A5) [22-25]	I,E	V1	- Insufficient access control - Weak/poor credentials - Weak encryptions
Data Threats	T1.2	Data Loss	Loss of data due to theft, power failure, ransom/malware attack/phishing attack. (A5,A1,A5) [26-28]	D, E, I	V2	- Poor backup mechanisms - Poor user training - Malicious Users - Weak Data protection
Data Threats	T1.3	Data Tamper	Damage, change or misuse of data. (A1,A2,A3,A5.A4)	T	V3	- Insider Threats -Weak authentication Mechanisms
Network Threats	T2.1	DOS	Unavailability of the system to users. (A3)	D	V4	- No whitelist/blacklist implementation - No tracking of connections - Weak Rate limiting
Network Threats	T2.2	Malware/ Ransomware/ Phishing Attack	Compromise of the system leading to any damage to CIA of system. (A1,A2,A3,A4,A5) [29-31]	S, T, D	V5	- No Web and email Filers - Weak security Infrastructure - No or less security Awareness
Network Threats	T2.3	Insecure connection/ API / Interface	Any insecure gateway (at user end or CSP) leading to loss, unauthorized or unavailability of system. (A1,A2,A3,A5,A6) [32-34]	S, D	V6	- Poorly constructed SLA - Cloud service provider lock in - Internet availability
Cloud Specific Threats	T3.1	Misuse of CSP	Unauthorized access or use of cloud due to poor infrastructure or poorly deployed security mechanisms. (A1,A2,A3,A5,A6,A7,A8)	S, T,I,D, E	V7	- No audits of CSP - Shared access - Poor or no encryption mechanism
Cloud Specific Threats	T3.2	Insufficient Spot and Check	Not enough cloud and security experts by user organization leading to security problems. (A3.A5,A6,A7,A8)	S, T, R, I, D, E	V8	- Insufficient security staff
Cloud Specific Threats	T3.3	Third party attacks	If Cloud has outsourced a part of the system with improper or insufficient security controls and access mechanisms with legal paperwork, might lead to bad shared access and damage to system and data. (A1,A2,A3,A5,A6,A7,A8)	T, R, I, D	V9	- Poor SLA with multiple vendors - Unevaluated business risk
Other Miscellaneous Threat	T4.1	Power Failure	Power failure leading to unavailability of system. (A3)	D	V10	- Poor backups
Other Miscellaneous Threat	T4.2	Natural Disaster	Any unanticipated disaster leading to loss of system or even back up system. (A3,A7)	D	V11	- Poor backups

DISCUSSION ON CORNERSTONE, MITIGATION, AND POST ALTERNATIVE TECHNIQUES

This section proposes a solution to counter the existing threat model and propose some possible alternative to cloud computing along with their advantages and limitations.

A. Cornerstone and Mitigation Techniques

As above we have mentioned our assets, threat classes, and vulnerabilities associated with them. Our first class was data threats which discussed data loss, data temper, and data breaches. In order to mitigate such attacks, we need strong encryption schemes for critical data. Using Anonymity of users and data can prevent exploitation of a vulnerability. Two-factor authentication, identity management, and a strict access control list for the system are a must. As we are discussing the privacy of data, compliance with a standard will add more reliability to the architecture of the system.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

For SHS, HIPPA and ENIST can be used. Our next threat class is comprised of network threats. Malware/Phishing/Ransom attacks and insecure connection/API/interface were discussed in T-class. Such attacks can be prevented with the use of intrusion detection systems, intrusion prevention systems, blacklisting/whitelisting of requests generated, use of web /email filters at the end of healthcare providers/ cloud service administration, and security awareness training should be conducted. Implementation of network access control, secure routing algorithms, and APIs is a must in order to avoid these threats. A well-constructed SLA between CSP and healthcare management comprising all security and privacy policies should be the start of this healthcare service. If there is a multi-tenancy in the system then that should be added to the respective SLA.

The next t-class mentioned threats related directly to the cloud. Cloud resource monitoring is required by CSP to avoid such threats. CSP itself needs to be audited to maintain the security image. The technical security staff should be well trained and sufficient in number. CSP should have evaluated the business risks and treated them accordingly. Again, if there is a third-party cloud, proper SLA should be maintained. Other threats are power failure for which proper backups must be maintained. And to avoid delays and latency cloud servers should be geographically located evenly. The system should be readily available if any natural disaster or unforeseen calamity happens.

B. Post Alternative Techniques

Fog Computing in Smart Health Care system: To fix the issues and uphold the challenges being faced in cloud computing, Fog computing is introduced. As a new standard of computing, it is still not taken as a full concept in society. It is an expansion of cloud computing at the edge of the network, which is a virtualized staging of resources providing storage, networking, and computation services to the users more efficiently. The architecture of Fog computing would consist of the device layer, fog layer, and cloud layer. In recent years SHS has been shifting to fog computing. Ahmad and et al proposed a framework called Healthfog which primarily focused on the improvement of privacy problems regarding medical records and system security by adding cloud-based security software [35].

In [36] Rahmani et.al performed an analysis on fog computing in healthcare by introducing a medium layer that received unprocessed information from the sensor devices and then stored it on cloud devices. A comparison on basis of characteristics of fog and cloud-based computing is as follows.

Table 1: Characteristics Comparison Of Cloud, Fog, And Edge Computing.

Char.	Cloud	Fog	Edge
Data Storage	Enormous	Limited	Limited
Data Transmis-sion	Device to cloud	Device to Device	Faster
Latency	High	Low	Low
Distribution	Centralized	Distributed	Distributed
No of nodes	low	High	High
Aggregation of data	Entirely at Cloud	Partially to cloud	Partial to edges and cloud
Scalability	Very Adaptive	Limited adaptive	Limited adaptive
Security	Not user de-fined but CSP	User-defined	User-defined
Mobility	Limited	Supported	Supported
Real-time Delivery	Supported	Supported	Supported

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

Edge Computing in Smart Health Care System: Edge computing is an emerging distributed technology architecture that aims to empower end devices [37 - 38]. Cloud computing was the best solution as long as the cloud itself had more processing power and resources than end devices. In recent decades, end devices had great technological advancements. Rapid evolution in technology has enhanced the capabilities of end devices.

The end devices are more capable in terms of computation power, storage, and communication than ever before. Soraira et al in their research proposed a framework that highlighted improvements in resource utilization and patient length by use of edge computing. A comparison on basis of characteristics of edge and cloud-based computing is as follows.

CONCLUSION

The security and privacy of the healthcare system is an ongoing challenge. Maintaining the system, and securing it physically and logically with maximum efficiency is the goal. After a thorough study, we can conclude that data security and privacy measures will evolve with time in the smart healthcare system. Although we have summarized security attacks in along with their mitigation techniques, this threat paradigm is continuously increasing. There are open research challenges, some of them are discussed, as well as directions for future research can be derived from this thought analysis of multiple cloud infrastructures and services. The research invites professionals to the design and implementation of best practices for slow and smooth adoption of the cloud.

REFERENCES

[1] Nidhya, R., Kumar, M., Maheswar, R. and Pavithra, D., 2022. Security and Privacy Issues in Smart Healthcare System Using Internet of Things. IoT - Enabled Smart Healthcare Systems, Services and Applications, pp.63-85.

[2] Hameed, Y Rana, B., 2022. Blockchain-Based Model for Secure IoT Communication in Smart Healthcare. In Emerging Technologies for Computing, Communication and Smart Cities (pp. 715-730). Springer, Singapore..

[3] Alhayani, B., Kwekha-Rashid, A.S., Mahajan, H.B., Ilhan, H., Uke, N., Alkhayyat, A. and Mohammed, H.J., 2022. 5G standards for the Industry 4.0 enabled communication systems using artificial intelligence: perspective of smart healthcare system. Applied Nanoscience, pp.1-11.

[4] Ambarkar, S.S 2021. Critical and Comparative Analysis of DoS and Version Number Attack in Healthcare IoT System. In Proceeding of First Doctoral Symposium on Natural Computing Research (pp. 301-312). Springer, Singapore.

[5] Somasundaram, R. and Thirugnanam, M., 2021. Review of security challenges in healthcare internet of things. Wireless Networks, 27(8), pp.5503-5509.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

[6] Saraswat, M. and Tripathi, R.C., 2020, December. Cloud Computing: Analysis of Top 5 CSPs in SaaS, PaaS and IaaS Platforms. In 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) (pp. 300-305). IEEE.

[7] Fatima, M., Abbas, H., Yaqoob, T., Shafqat, N., Ahmad, Z., Zeeshan, R., Muhammad, Z., Rana, T. and Mussiraliyeva, S., 2021. A survey on common criteria (CC) evaluating schemes for security assessment of IT products. PeerJ Computer Science, 7, p.e701.

[8] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S. and Wang, G., 2018. Data processing and text mining technologies on electronic medical records: a review. Journal of healthcare engineering, 2018.

[9] A. Algarni, "A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems", IEEE Access, vol. 7, pp. 101879-101894, 2019. Available: 10.1109/access.2019.2930962. A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems

[10] A. "ENHANCING SECURITY FEATURES IN CLOUD COMPUTING FOR HEALTHCARE USING CIPHER AND INTER CLOUD", International Journal of Research in Engineering and Technology, vol. 03, no. 03, pp. 200-203, 2014. Available: 10.15623/ijret.2014.0303036.

[11] D. Raval and S. Jangale, "Cloud based Information Security and Privacy in Healthcare", International Journal of Computer Applications, vol. 150, no. 4, pp. 11-15, 2016. Available: 10.5120/ijca2016911483. [4] Glasper, A. (2019). A long-term plan for embracing digital healthcare technology. British Journal of Nursing..

[12] C. Wang, K. Ren, J. Wang and Q. Wang, "Harnessing the Cloud for Securely Outsourcing Large-Scale Systems of Linear Equations", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1172-1181, 2013.

[13] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou,"Fuzzy keyword search over encrypted data in cloud computing", International Journal of Recent Trends in Engineering and Research, vol. 4, no. 1, pp. 375-379, 2018.

[14] T. Plantard, W. Susilo and Z. Zhang, "Fully Homomorphic Encryption Using Hidden Ideal Lattice", IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2127-2137, 2013.

[15] Ming Li, Shucheng Yu, Yao Zheng Kui Ren and, Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption.

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

[17] Varatharajan, R., Manogaran, G. and Priyan, M.K., 2018. A big data classification approach using LDA with an enhanced SVM method for ECG signals in cloud computing. Multimedia Tools and Applications, 77(8), pp.10195-10215.

[18] Yin, J., Tang, Y., Deng, S., Zheng, B. and Zomaya, A.Y., 2020. MUSE: a multi-tierd and SLA-driven deduplication framework for cloud storage systems. IEEE Transactions on Computers, 70(5), pp.759-774.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

[19] Ahmad, M.; Hussain, S.; Kang, B.H.; Cheong, T.; Lee, S. Health Fog: A novel framework for health and wellness applications. J. Supercomput. 2016, 72, 3677–3695

[20] Rahmani, A.M.; 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. Comput. Syst. 2018, 78, 641–658

[21] Oueida, S., Kotb, M., Jararweh, Y. and Baker, T., 2018. An Edge Computing Based Smart Healthcare Framework for Resource Management. Sensors, 18(12), p.4307.

[22] Kamaruddin, N. S., Kamsin, A., Por, L. Y., & Rahman, H. (2018). A review of text watermarking: theory, methods, and applications. IEEE Access, 6, 8011-8028.

[23] Rahman, H., Arshad, H., Mahmud, R., & Mahayuddin, Z. R. (2017, October). A framework for breast cancer visualization using augmented reality x-ray vision technique in mobile technology. In AIP Conference Proceedings (Vol. 1891, No. 1, p. 020116). AIP Publishing LLC.

[24] Rahman, H., Arshad, Mahayuddin, Z. R., & Obeidy, W. K. (2017). A Framework to Visualize 3D Breast Tumor Using X-Ray Vision Technique in Mobile Augmented Reality. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(2-11), 145-149.

[25] Salleh, S., Mahmud, R., Rahman, H., & Yasiran, S. S. (2017). Speed up Robust Features (SURF) with Principal Component Analysis-Support Vector Machine (PCA-SVM) for benign and malignant classifications. Journal of Fundamental and Applied Sciences, 9(5S), 624-643.

[26] Obeidy, W. K., Arshad, H., Tan, S. Y., & Rahman, H. (2015, November). Developmental analysis of a markerless hybrid tracking technique for mobile augmented reality systems. In International Visual Informatics Conference (pp. 99-110). Springer, Cham.

[27] Awan, D., & Rehman, H. U. (2015). Grid Load Balancing Using Parallel Genetic Algorithm.

[28] Lashkari, A.H. (2010, April). Widget Based Position System (WBPS) An innovative mobile Application. In 2010 2nd International Conference on Computer Engineering and Technology (Vol. 2, pp. V2-615). IEEE. .

[29] Zia, Z. U. R., Rahman, (2020). Technical Challenges in Achieving Ultra-Reliable & Low Latency Communication in 5G Cellular-V2X Systems. LC International Journal of STEM (ISSN: 2708-7123), 1(3), 89-95.

[30] Abbas, M., Arshad, M., & Rahman, H. (2020). Detection of Breast Cancer Using Neural Networks. LC International Journal of STEM (ISSN: 2708-7123), 1(3), 75-88.

Tasleem, S., Bano, P., & Rahman, H. (2020). Students Attendance Management System Based On Face Recognition. LC International Journal of STEM (ISSN: 2708-7123).

[31] Ahmad, R., Khalid, A., & Rahman, H. (2020). Brain Tumor Detection Using Image Segmentation and Classification. LC International Journal of STEM (ISSN: 2708-7123), 1(3), 59-65.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-03 | Issue-01 | March-2022

[32] Sameen, D, I., & Rahman, H. (2020). Skin Cancer Disease Detection Using Image Processing. LC International Journal of STEM (ISSN: 2708-7123), 1(3), 50-58.

[33] Tariq, T., Hassan, M., Rahman, H., & Shah, A. (2020). Predictive Model for Lung Cancer Detection. LC International Journal of STEM (ISSN: 2708-7123), 1(2), 61-74.

[34] Bano, R., & Rahman, H. (2020). Detection of Anthracnose Disease in Chili Using IOT and Field Data. LC International Journal of STEM (ISSN: 2708-7123)75-82.

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

[36] Oueida, S., Kotb, Y, and Baker, T., 2018. An Edge Computing Based Smart Healthcare Framework for Resource Management. Sensors, 18(12), p.4307.

[37] Mirza, S., 2021, A Malware Evasion Technique for Auditing Android Anti-Malware Solutions. In 2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) (pp. 125-130). IEEE.

[38] Muhammad, Z, A Systematic Evaluation of Android Anti-Malware Tools for Detection of Contemporary Malware. In 2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 117-124). IEEE.

BIOGRAPHY