Advancement of Cloud Computing and Big Data Analytics in Healthcare Sector Security

AKSHAT GAURAV[1], KWOK TAI CHUI[2]
[1]Ronin Institute, Montclair, New Jersey 07043, U.S.(e-mail: akshat.gaurav@ronininstitute.org)
[2]Hong Kong Metropolitan University (HKMU) , Hong Kong(e-mail: jktchui@hkmu.edu.hk)

ABSTRACT Professionals and health policymakers have recently placed a premium on patient safety and healthcare. Because of the breadth and depth of its service offerings, healthcare creates a mountain of data that can only be processed by enterprise-level software. In light of this, the core of healthcare operations is in the functions of big data application. When combined with big data applications, cloud computing's on-demand nature makes it an invaluable tool in the healthcare industry. In this study, we examine how healthcare might benefit from the combination of big data and cloud computing.

KEYWORDS Big Data, Cloud Computing, Healthcare, Security

I. INTRODUCTION

A large amount of data generated by different sources in the healthcare sector has always been the concern of researchers and the industrial sector, due to which researchers proposed to use the concept of big data analytics and cloud computing to solve the issued of the healthcare sector. The use of big data and cloud computing is presented in **??** Therefore, due to its low cost and massive data storage capacities, big data and cloud computing in healthcare services is receiving widespread attention throughout the globe. Similarly, as more and more smart cities are being built, academics and governments are becoming more interested in smart healthcare. However, due to the use of cloud computing and big data analytics, the smart healthcare sector becomes vulnerable to different types of cyber-attacks. As the smart devices used in the smart healthcare sector are heterogeneous in nature therefore traditional attack detection techniques are not applicable in the smart healthcare sector. Therefore, there is a need for the development of new tools and techniques for attack detection in the smart healthcare sector. In this context, this article review attack detection techniques in the healthcare sector.

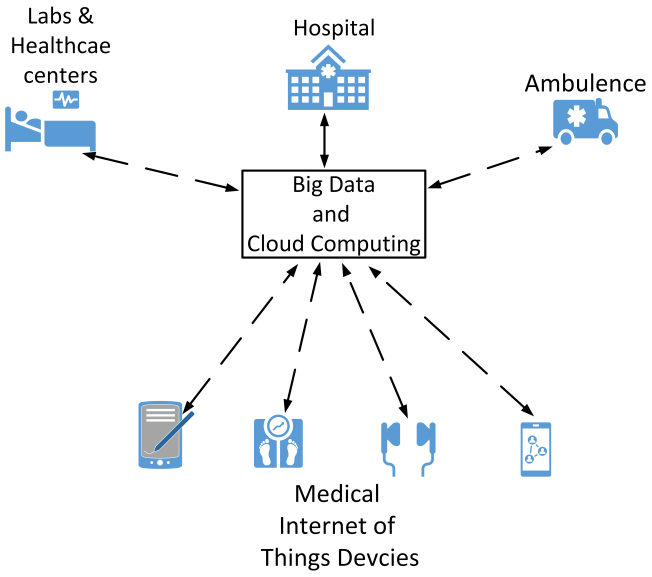


FIGURE 1: Big data and Cloud computing in Healthcare sector

II. LITERATURE SURVEY

Authors in [1] proposed joint computation offloading and task caching for multi-user and multi-task MEC systems. Authors in [2] proposed a secure timestamp-based mutual authentication protocol for IoT devices using RFID tags. Author in [3] proposed a trust infrastructure-based authentication method for clustered vehicular ad hoc networks. Author in [4] presented detection, avoidance, and attack pattern mechanisms in modern web applications. Authors in [5] proposed an enhanced CBF packet filtering method to detect DDoS attack in cloud computing environments. Authors in [6] proposed hadoop based defense solution to handle distributed denial of service (DDoS) attacks. Authors in [7] proposed a a novel solution to handle DDOS attack in MANET. Authors in [8] present a technique for accelerating 3D medical volume segmentation using GPUs. Authors in [9] presented an accelerating compute-intensive medical imaging segmentation algorithm using a hybrid CPU-GPU. Authors in [10] proposed a prototype method to discover

workflow violation and XSS vulnerabilities in PHP web applications. Authors in [11] proposed an ISP level solution to combat DDoS attacks using a combined statistical-based approach. Authots in [12] proposed cross-site scripting (XSS) abuse and defense technique. Authors in [13] presents a a comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques. Authors in [14] present a URL features-based phishing detection system using machine learning. Author in [15] proposed an statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic. Author in [16] proposed coverless information hiding based technique. Authors in [17] proposed a decentralised control-based interaction framework for secure data transmission in internet of automated vehicles. Authors in [18] propsed a dynamic policy attribute based encryption and its application in generic construction of multi-keyword search. Authors in [19] review security issues and challenges in online social networks. Authors in [20] review recent advances in fog and mobile edge computing. Authors in [21] review different honeypot techniques. Authors in [22] proposed a novel approach for DDoS attack detection in COVID-19 scenario for small entrepreneurs. Author in [23] proposed Ddos attack detection in vehicular ad-hoc network for 5g networks. Author in [24] proposed Identity-based authentication mechanism for secure information sharing in the maritime transport system. Authors in [25] proposed phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email. Author in [26] proposed an MRI scans-based Alzheimer's disease detection via convolutional neural network and transfer learning.

III. BIBLOMETRIC ANALYSIS

In this research paper, we try to understand the importance of big data and cloud computing in the healthcare sector. As there is a large number of available articles, we limit our analysis to the Scopus database. The combined analysis of the literature is presented in Figure 2. The annual production of articles is presented in Figure 2a and in Figure 2a it is clear that the number of articles published in the field of healthcare sector increases over the years. This is proof that researchers are constantly working to find new techniques and protocols for the development of the healthcare sector. Therefore, if a new researcher wants to work in this field, he or she can start his work. The type of publication is also a good criterion that may help young researchers find relevant papers. From Figure 2b, it is clear that the majority of work in the field of the healthcare sector is published in international conferences. In addition to the type of publication, the subject area is also a good factor in the analysis of the research field. The topic distribution is presented in Figure 2c. From Figure 2c it is clear that most researchers in the computer science domain work in the healthcare sector.

The distribution of countries is also a good factor to analyze the distribution of researchers. The distribution of researchers is presented in Figure 2d and from the figure it is clear that researchers from *India* and *US* are working in the field of healthcare. Finally, Figure 2e and Figure 2f present the distribution of the research field according to the authors and affiliations.

IV. CYBER ATTACKS ON HEALTHCARE SYSTEMS

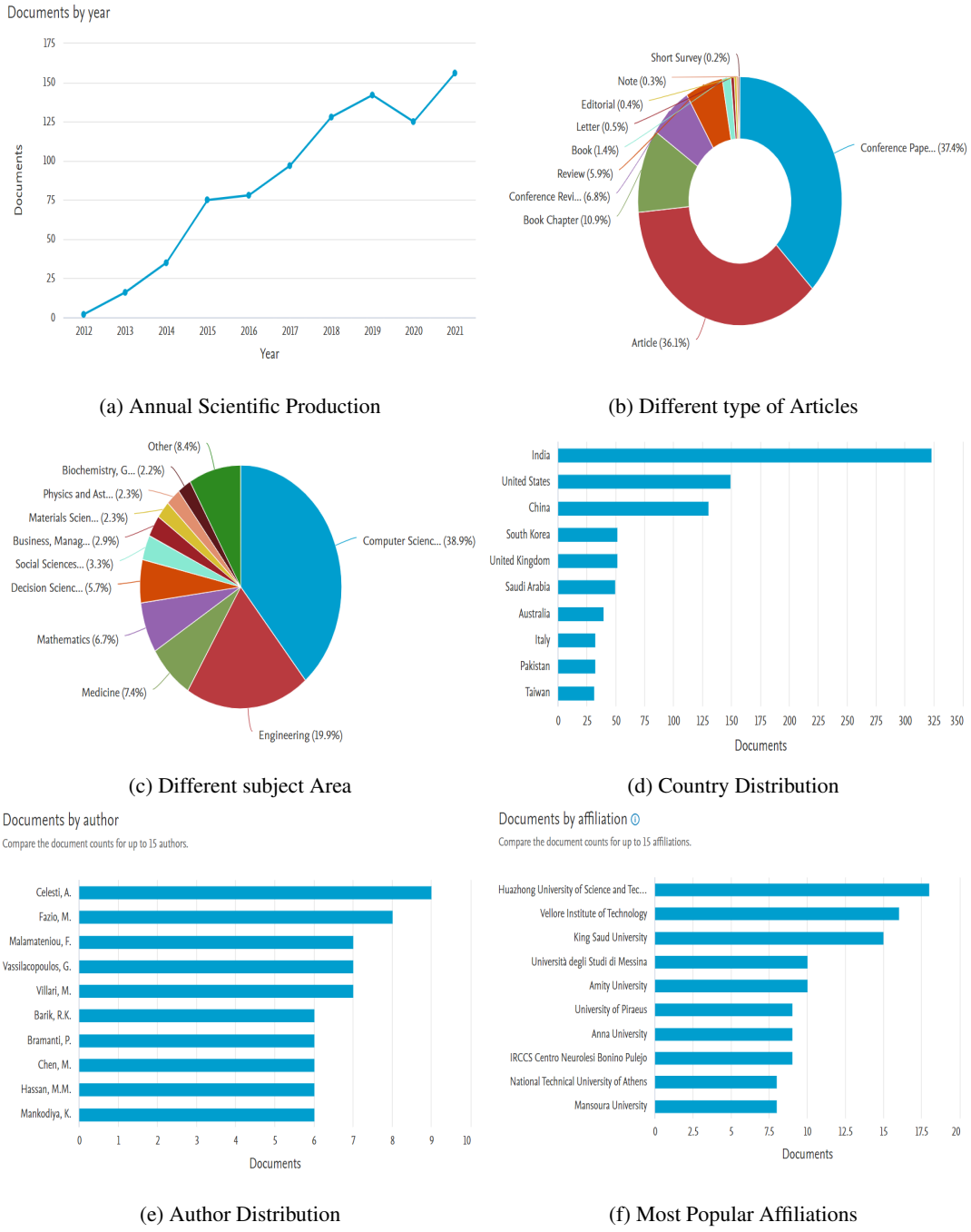
The healthcare sector majority depend upon digitally stored data. The data collected from different sources are processed and the outcome is used to predict the epidemic. However, due to the presence of a large amount of digital data security and privacy becomes the major concern of the healthcare sector. Attackers always attack the healthcare sector and try to steal confidential data, some of the major attacks on healthcare systems are represented in Table 1.

At Becker hospital in 1979, the first ransomware attack occurs, due to which 20000 floppy disks were affected. It was the earliest version of the Wanna cry worm [27]. In 2009, an identity theft attack named "HealthNet" occurs, which steals 531,400 patient data from the hospital database. Lincoln Medical and Mental Health Center was attacked in 2010 and the confidential information of 180,111 patients was stolen by the attackers. A similar type of attack occurred in 2011 in which attackers stole the confidential information of Memorial healthcare systems. In 2012, hackers hacked into the system of US Medicaid and stole 780,000 users' personal information. Advocate Medical Group is also affected by a confidentiality breach attack in 2013, in which its 4,000,000 users' data were stolen. 4,500,000 user data of Community Health Systems were stolen by the attackers in 2014. In 2015, Anthem Inc, CareFirst BlueCross Blue Shield-Maryland, Medical Informatics Engineering, Premera, and Santa Monica were targeted by the attackers and confidential information was stolen by the attackers. In 2016, 21st Century Oncology, Apple Health Medicaid, Inuvik hospital, and Banner health records were hacked and personal records of the patients were stolen. Grozio Chirurgija was attacked by an attacker in 2017 and, in 2018 Centers for Medicare and Medicaid Services' system was hacked by the attackers. Health Sciences Authority (Singapore) data was leaked due to zero-day vulnerability in 2019. Unit pint health also suffered two data breaches in 2019. In March 2019, attackers stole confidential data from Life Bridge Healthcare systems by installing malware on their system.

V. SECURITY REQUIREMENTS OF HEALTHCARE BIG DATA

In the era of healthcare 4.0, the healthcare industry is responsible for the generation, storing, and processing of a large amount of data. To handle this large amount of data, the healthcare industry adopts big data technologies and tools, but along with the benefits, there are some limitations of big data that create new security challenges for the healthcare industry like data privacy and data security.

The security and privacy of healthcare big data depend upon many factors like the type of device which collects the data, type of data storage technology, the type of users who



(a) Annual Scientific Production

(b) Different type of Articles

(c) Different subject Area

(d) Country Distribution

(e) Author Distribution

(f) Most Popular Affiliations

FIGURE 2: Statistical Analysis contribution of Big data and Cloud computing in Healthcare sector

are accessing the data, etc. The challenges in the field of big data security are classified as follows:

- The sharing of data among the hospitals is most important to get the most benefit from the health care big data. However, there is no single rule for storing the data, some hospitals are saving the data on their private servers, some are using public cloud servers, some are using the combination of both private and public cloud. Each of the storing environments has its own security rules, hence the sharing of data among different sources is a challenging task.
- In different countries, there are different laws by which data is collected, processed, and accessed, so the health care big data has to follow these rules set by the government. But as in cloud computing, data is not stored in one place, so it is difficult to apply the government rules to data theft cases.
- Unauthorized access to healthcare big data is a major

TABLE 1: Timeline of cyber attacks on healthcare sector

1979	Attack on Becker's Hospital
2009	Attack on HealthNet
2010	Attack on Lincoln Medical and Mental
2011	Attack on Memorial Healthcare System
2012	Attack on US Medicaid at the South Carolina Government
2013	Attack on Advocate Medical Group and Crescent Health Inc. and Walgreens
2014	Attack on Community Health Systems
2015	Attack on Anthem Inc., CareFirst BlueCross Blue Shield-Maryland, and Medical Informatics Engineering
2016	Attack on 21st Century Oncology, Apple Health Medicaid, Inuvik hospital, and Banner health
2017	Attack on Grozio Chirurgija
2018	Attack on Centers for Medicare and Medicaid Services
2019	Attack on Health Sciences Authority (Singapore), Life Bridge Healthcare, Unit pint health, and Health Sciences Authority

security issue. As in the medical database, there is personal information about the patients, so if an unauthorized person gets access to this data and he uses it for illegal activities like insurance fraud, then it leads to a bigger problem.

– Privacy is also a security issue in healthcare big data if the information present in the database is leaked, then sometimes it creates an unwanted social issue.

VI. CONCLUSION

In this article, we looked at some of the concerns around the privacy and security of healthcare big data. We all know that there are two sides to every story, and the use of big data and cloud computing in healthcare opens the door to a variety of cyberattacks. Therefore, in order to preserve the confidentiality of healthcare, we examine the various security measures provided by the researchers.or.

REFERENCES

[1] I. A. Elgendy and et al., "Joint computation offloading and task caching for multi-user and multi-task mec systems: reinforcement learning-based algorithms," Wireless Networks, vol. 27, no. 3, pp. 2023–2038, 2021.

[2] A. Tewari and et al., "Secure timestamp-based mutual authentication protocol for iot devices using rfid tags," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 16, no. 3, pp. 20–34, 2020.

[3] F. Mirsadeghi and et al., "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," Peer-to-Peer Networking and Applications, vol. 14, no. 4, pp. 2537–2553, 2021.

[4] S. Gupta and et al., "Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 3, pp. 1–43, 2017.

[5] P. Negi and et al., "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment," arXiv preprint arXiv:1304.7073, 2013.

[6] S. Tripathi and et al., "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," 2013.

[7] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.

[8] M. Al-Ayyoub and et al., "Accelerating 3d medical volume segmentation using gpus," Multimedia Tools and Applications, vol. 77, no. 4, pp. 4939–4958, 2018.

[9] M. A. Alsmirat and et al., "Accelerating compute intensive medical imaging segmentation algorithms using hybrid cpu-gpu implementations," Multimedia Tools and Applications, vol. 76, no. 3, pp. 3537–3555, 2017.

[10] S. Gupta and et al., "Php-sensor: a prototype method to discover workflow violation and xss vulnerabilities in php web applications," in Proceedings of the 12th ACM international conference on computing frontiers, 2015, pp. 1–8.

[11] B. B. Gupta and et al., "An isp level solution to combat ddos attacks using combined statistical based approach," arXiv preprint arXiv:1203.2400, 2012.

[12] B. Gupta and et al., "Cross-site scripting (xss) abuse and defense: exploitation on several testing bed environments and its defense," Journal of Information Privacy and Security, vol. 11, no. 2, pp. 118–136, 2015.

[13] A. Mishra and et al., "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in 2011 European Intelligence and Security Informatics Conference. IEEE, 2011, pp. 286–289.

[14] A. K. Jain and et al., "Phish-safe: Url features-based phishing detection system using machine learning," in Cyber Security. Springer, 2018, pp. 467–474.

[15] Z. Zhou and et al., "A statistical approach to secure health care services from ddos attacks during covid-19 pandemic," Neural Computing and Applications, pp. 1–14, 2021.

[16] Z. Zhou and et al., "Coverless information hiding based on probability graph learning for secure communication in iot environment," IEEE Internet of Things Journal, 2021.

[17] B. B. Gupta and M. Quamara, "Decentralised control-based interaction framework for secure data transmission in internet of automated vehicles," International Journal of Embedded Systems, vol. 12, no. 4, pp. 414–423, 2020.

[18] B. B. Gupta and S. T. Ali, "Dynamic policy attribute based encryption and its application in generic construction of multi-keyword search," International Journal of E-Services and Mobile Applications (IJESMA), vol. 11, no. 4, pp. 16–38, 2019.

[19] S. R. Sahoo and et al., "Security issues and challenges in online social networks (osns) based on user perspective," Computer and cyber security, pp. 591–606, 2018.

[20] E. Ahmed and et al., "Recent advances in fog and mobile edge computing," p. e3307, 2018.

[21] B. B. Gupta and A. Gupta, "Assessment of honeypots: Issues, challenges and future directions," International Journal of Cloud Applications and Computing (IJCAC), vol. 8, no. 1, pp. 21–54, 2018.

[22] A. Gaurav and et al., "A novel approach for ddos attacks detection in covid-19 scenario for small entrepreneurs," Technological Forecasting and Social Change, vol. 177, p. 121554, 2022.

[23] A. Gaurav and et al., "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," in Security and Privacy Preserving for IoT and 5G Networks. Springer, 2022, pp. 263–278.

[24] B. B. Gupta and et al., "Identity-based authentication mechanism for secure information sharing in the maritime transport system," IEEE Transactions on Intelligent Transportation Systems, 2021.

[25] A. Almomani and et al., "Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email," arXiv preprint arXiv:1302.0629, 2013.

[26] K. T. Chui and et al., "An mri scans-based alzheimer's disease detection via convolutional neural network and transfer learning," Diagnostics, vol. 12, no. 7, p. 1531, 2022.

[27] M. Akbanov and et al., "Ransomware detection and mitigation using software-defined networking: The case of wannacry," Computers & Electrical Engineering, vol. 76, pp. 111–121, 2019.